Rijkswaterstaat
Ministerie van Infrastructuur en Waterstaat

Vraagspecificatie Proces Bijlagen

Vervanging verlichting Schipholtunnel
Zaaknummer: 31212908

Datum: 01-12-2025

Inhoud

Bijlage A Risicolijst 4

Bijlage B Integraal Veiligheidsplan 6

Bijlage C Format Risicobeoordeling 7

Bijlage D Protocol berekenen en aantonen MKI-waarde 8

Bijlage E Kaderrichtlijn Coördinatie uitvoeringsbesluiten op grond van artikel 5.45 lid 2 Omgevingswet 9

Bijlage F Regelingenschema Kabels en Leidingen Derden 10

Bijlage G Verkeersmanagement voor rijkswegen 13

Bijlage H Scheepvaartverkeersmanagement voor rijksvaarwegen 14

Bijlage I Rijkswaterstaat Brede Afspraak Archeologie 15

Bijlage J Programma van Eisen voor uitvoerend archeologisch onderzoek 16

Bijlage K Rijkswaterstaat Brede Afspraak Maatschappelijk Verantwoord Inkopen 17

Bijlage L Minimum eisen emissienormen materieel en energiedragers 18

Bijlage M Levering Areaalgegevens 19

Bijlage N Invulinstructie format LV BRO 28

Bijlage O Melding inzet Zelfstandige Hulppersoon 30

Bijlage P Aanvullende eigen verklaring inzake Russische partijen 31

Bijlage Q Producten en Diensten Catalogus Netwerken CIV 33

Bijlage R Bijlagen Bedrijfsvoering Elektrische Installaties RWS 34

Bijlage S Bijlagen Cybersecurity 35

Bijlage T Procedure Werkvergunningen 36

Bijlage U Leidraad Naamgeving en Codering RWS Tunnelsysteem 37

Bijlage V J-STD-016 38

Bijlage W MIL-STD-1521B (USAF) 4 juni 1985, met Notice 1 19 december 1985; Military Standard Technical reviews and audits for systems, equipments, and computer software 39

Bijlage X Handboek Werk in Uitvoering Landzijde 40

Bijlage Y Coördinatie van voorgeschreven Zelfstandige Hulppersonen 41

Bijlage A Risicolijst

Id	Ongewenste gebeurtenis	Oorzaak	Gevolg
1	Toegewezen slots worden op het laatste moment aangepast	O1. Slots worden op het laatste moment weggegeven (bijv. door calamiteiten, (door prioritering van andere project) O2. Weersomstandigheden maken het niet mogelijk om werkzaamheden uit te voeren O3. Verkeerde planning en communicatie op moment van calamiteit O4. Resource beperkingen (momentopname: kan niet voldoen aan capaciteitsvraagstukken)	G1. Uitvoeringswerkzaamheden lopen vertraging op. Mogelijk min. Jaar vertraging G2. Verhoogde project kosten G3. Imago schade G4. uitval installaties G5. Beperkingen rond de tunnels G6. Nieuwe slots aanvragen
2	Areaalgegevens van de Schipholtunnel zijn niet actueel en/of op orde (PC, ON)	O1.De opdrachtgever is afhankelijk van informatie vanuit TOPII ON, specifiek met betrekking tot vast onderhoud O2. Vertraging in het bijhouden van actuele staat van het onderhoud bij OG O3. De areaalgegevens zijn niet geactualiseerd door ON	G1. Voorspelbaarheid van onderhoud komt in het geding G2. Veiligheidsrisico's voor gebruikers van het areaal/object G3. Kwaliteit: opleverdossier en areaalgegevens niet in lijn met de werkelijkheid
3	Bij werkzaamheden constatering van gevaarlijke stoffen, waaronder Chroom 6, fijnstof, asbest en PFAS.	O1. Onvoldoende inventarisatie van het object omtrent gevaarlijke stoffen O2. Onvoldoende naleving van veiligheidsnormen O3. Ontbrekende gegevens over aanwezigheid van gevaarlijkstoffen vanuit areaalgegevens O4. Bij graafwerkzaamheden constateren we gevaarlijke stoffen (per- en polyfluoralkylstoffen)	G1. Gezondheidsrisico voor medewerkers door blootstelling G2. Milieuvervuiling G3. Vertraging en extra kosten G4. Lange discussies met ON (incl. vtw/afwijkingen proces)
4	Uitvoering duurt langer dan beschikbare Slots	O1. Werkzaamheden duren langer dan vooraf verwacht door onvoorziene tegenvallers O2. De slots zijn ontoereikend tegenover hun eigen planning O3. personele problemen bij opdrachtnemer	G1. De slots kunnen niet worden gehaald G2. Nieuwe slots zijn nodig G3. Vertraging zorgt voor extra kosten G4. Veiligheid: Langer door gaan met bestaande oude verlichting.
5	Bij vervanging van de verlichting, functioneert het bestaande (3B) deel niet meer. (bediening, besturing en bewaking)	O1: Onjuiste aansluiting van de nieuwe verlichting op het bestaande systeem. O2: Incompatibiliteit tussen de nieuwe verlichting en het bestaande 3B-systeem (bediening, besturing en bewaking). O3: Onvoldoende integratie van de nieuwe verlichting in het controle- en bewakingssysteem.	G1. Verlies van bediening over de verlichting. G2. Storingen in het besturingssysteem (bijv. onjuiste schakeling van de verlichting). G3. Onvoldoende bewaking van het verlichtingssysteem (bijv. geen meldingen bij storingen). G4. Verminderde

		O4. ON onbekend met huidige software/platform (specifiek 3b software)	verlichtingsefficiëntie en veiligheid.
6	Levertijden van materiaal zijn langer dan verwacht	O1. Vertragingen bij de leveranciers zelf door productie- of logistieke problemen O2. Het niet goed inschatten van de benodigde tijd voor materiaallevering of de levertijden worden te optimistisch ingeschat O3. Veranderingen in de scope van het project, zoals extra materialen of een versnelde uitvoering O4. Geopolitieke spanningen	G1. Slots voor geplande werkzaamheden worden niet gehaald G2. Materialen niet op tijd beschikbaar voor werkzaamheden
7	Coördinatie en demarcatie van overlappende werkzaamheden in de tunnel tussen ON (NOK) en TOPII is onduidelijk en/of onvoldoende afgestemd.	O1. Huidige aannemer wilt geen nieuwe aannemer in zijn areaal O2. De onderhoudsstaat is niet in orde door toedoen van de aannemer, waardoor deze zich verzet tegen het tonen van het werk aan een andere aannemer.	G1. Storingen door werken aan installaties die met elkaar zijn gesynchroniseerd. G2. De afgesproken Slots wordt niet gehaald G3: De opdrachtnemers lossen de storingen niet op gedurende de ombouw periode
8	Top II aannemer kan het onderhoud niet goed uitvoeren i.v.m. verschillende software in de verschillende buizen.	O1. De slots houden geen rekening met de techniek van 3b O2. Te weinig randvoorwaarden meegeven van techniek aan omgeving op aansturing 3b's O3. De kans op fout om systemen te onderhouden is groot omdat elke buis een ander software heeft.	G1.tijdelijke technische oplossing is nodig om de aansluiting te blijven garanderen.
9	Coördinatie en demarcatie van overlappende werkzaamheden in het netwerk is onduidelijk en/of onvoldoende afgestemd.	O1. Onvoldoende communicatie tussen projectteams zorgt ervoor dat er geen gedeeld overzicht bestaat van de raakvlakken of samenhang O2. Een gebrek aan integrale coördinatie tussen aannemers O3. Onvoldoende betrokkenheid interne stakeholders waaronder andere projectteams O4. Onjuist of niet tijdige documentatie van voortgang en raakvlakken	G1. Meeliften van andere projecten gaat niet door. G2. Wegvak moet meerdere keren afgesloten worden. G3. Imagoschade door negatieve berichten in de media.
10	Garantieperiode: verwachtingen en verantwoordelijkheden niet helder tussen RWS, ON VVS en TOPII aannemer	O1. Onduidelijke contract afspraken betreft garantievoorwaarden O2. Onvoldoende communicatie tussen RWS, ON en TOP II aannemer leidt tot misverstanden O3. Onvoldoende kennis over garantievoorwaarden aannemers	G1. Lang lopend geschil tussen ON en OG G2. Vertraging in het verhelpen van defecten (onderhoudswerkzaamheden) G3. Kostenstijging

Bijlage B Integraal Veiligheidsplan

Rijkswaterstaat
Ministerie van Infrastructuur en Waterstaat

RWS INFORMATIE -

Integraal Veiligheid Plan (IVP) op basis van sjabloon 2.0.7

Bijlage bij Vraagspecificatie Proces

D&C Vervanging Verlichting Schipholtunnel
Zaaknummer: 31212908

Datum	1 december 2025
Status	Definitief

Coördinator Ontwerpfase	*Martijn Heemink*
Coördinator Uitvoeringsfase	*Wordt na de gunning bekendgemaakt*

Colofon

Documentinformatie

Uitgegeven door	*D&C Vervanging Verlichting Schipholtunnel (31212908)*
Technisch manager	*Martijn Heemink*
Telefoon	*06-50197295*
Opgesteld door	*Ralph van Beek*
Versie	*1.0*
Status	*Definitief*

Acceptatie

		Paraaf:	Datum:
Uitgegeven door:			
Opsteller(s)	*Ralph van Beek*		19-11-2025
Vrijgave Technisch manager:	*Martijn Heemink*	Martijn Heemink Digitaal ondertekend door Martijn Heemink DN: cn=Martijn Heemink, o=Rijkswaterstaat, ou=PPO WNN TTM, email=martijn.heemink@rws.nl Datum: 2025.11.19 10:40:31 +01'00'	
Vrijgave V&G-Coördinator	*Rutger van der Kloes*	RK	*19-11-2025*
Vaststelling Project Manager:	*Jeroen Papenhuijzen*	Jeroen Papenhuijzen Digitaal ondertekend door Jeroen Papenhuijzen DN: cn=Jeroen Papenhuijzen, o=Rijkswaterstaat, ou=PPO Portfoliomanagement 5, email=jeroen.papenhuijzen@rws.nl Datum: 2025.11.24 10:15:41 +01'00'	

Versiebeheer

Versie	Datum	Reden van uitgifte/wijzigingen
1.0	*1-12-2025*	*Versie t.b.v. aanbesteding*

Inhoud

Inleiding 7

1 Uitgangspunten en randvoorwaarden 9
1.1 Beleidsverklaring veiligheid Rijkswaterstaat 9
1.2 Ambitie en doelen 10
1.3 Gedragsregels voor projectmedewerkers 10
1.4 Relevante veiligheidsdomeinen 11

2 Het project 12
2.1 Reikwijdte en grenzen project 12
2.2 Betrokken partijen 14
2.3 Coördinator Ontwerpfase, V&G-coördinator en Coördinator Uitvoeringsfase 15
2.4 Planning van de werkzaamheden 17

3 Maatregelen 18
3.1 Arbeidsveiligheid 18
3.2 Verkeersveiligheid 20
3.3 Externe veiligheid 21
3.4 Elektrische veiligheid 21
3.5 Tunnelveiligheid 21
3.6 Constructieve veiligheid 21
3.7 Sociale veiligheid 21
3.8 Brandveiligheid 22
3.9 Integrale beveiliging 22

4 Afspraken 24
4.1 Aanstelling coördinator realisatiefase 24
4.2 Melding Nederlandse Arbeidsinspectie 24
4.3 Actualisatie IVP 24
4.4 Organisatie rond incidentregistratie en -afhandeling 25
4.5 Projectadviseur Integrale Veiligheid 25

5 Wijze van toezicht 26

6 Verantwoording van BTO-keuzen 27

7 Opleiding en instructie 28
7.1 Veiligheidshuisregels Rijkwaterstaat, object specifiek en opdrachtnemer 28
7.2 Aanvragen werkvergunning 28
7.3 PBM’s voor projectmedewerkers van Rijkswaterstaat 28

Bijlage A Definities 30

Bijlage B Ontwerp RI&E 32

Bijlage C BTO-keuzes 33

Bijlage D Calamiteitenbestrijdingsplan RWS WNN 2024 34

Inleiding

Dit IVP is de invulling van het wettelijk vereiste V&G plan voor arbeidsveiligheid, uitgebreid met de overige specifieke veiligheidsdomeinen voor Rijkswaterstaat. Als Opdrachtgever heeft Rijkswaterstaat de verantwoordelijk om tijdens de ontwerpfase dit IVP:

- Op te (laten) stellen en;
- Onderdeel te laten zijn van het contractdossier en;
- Beschikbaar te stellen op de bouwlocatie alvorens de uitvoeringswerkzaamheden van start gaan (= moment dat opdrachtnemers op de bouwlocatie komen").

Als er fysieke werkzaamheden op de bouwlocatie worden uitgevoerd, is de opdrachtnemer vervolgens verantwoordelijk voor het uitvoeren van dit IVP en het actualiseren ervan zodra de uitvoeringswerkzaamheden daartoe aanleiding geven, bijvoorbeeld bij risicovolle werkzaamheden of als via een ander contract een nieuwe partij op de bouwlocatie werkzaamheden gaat verrichten. In deze gevallen zal de Coördinator Uitvoeringsfase namens de opdrachtnemer, in overleg met de Coördinator Ontwerpfase namens de opdrachtgever, moeten zorgen voor de noodzakelijke afstemming en coördinatie.

Dit IVP is als volgt opgebouwd:

- Hoofdstuk 1: een beschrijving van de RWS veiligheidsambitie alsmede de project specifieke veiligheidsdoelstellingen.
- Hoofdstuk 2: een beschrijving van het tot stand te brengen bouwwerk, een overzicht van de betrokken ondernemingen op de bouwlocatie, de naam van de coördinator Ontwerpfase en van de coördinator Uitvoeringsfase;
- Hoofdstuk 3: de maatregelen die volgen uit de risico-inventarisatie en -evaluatie, bedoeld in bijlage B;
- Hoofdstuk 4: de afspraken met betrekking tot de uitvoering van de maatregelen, bedoeld in hoofdstuk 3;
- Hoofdstuk 5: de wijze waarop toezicht op de maatregelen wordt uitgeoefend;
- Hoofdstuk 6: de bouwkundige, technische en organisatorische keuzen die in verband met de veiligheid en gezondheid van de werknemers en zelfstandigen in de uitvoeringsfase worden gemaakt alsmede de onderzoeken en rapporten die de onderbouwing van deze keuzen ondersteunen;
- Hoofdstuk 7: de wijze waarop voorlichting en instructie aan de werknemers op de bouwplaats wordt gegeven.
- Bijlage B: een inventarisatie en evaluatie van de specifieke gevaren voor het betreffende bouwwerk (de objectrisico's) en specifieke gevaren die het gevolg zijn van de gelijktijdige en achtereenvolgende uitvoering van de bouwwerkzaamheden en in voorkomend geval van de wisselwerking met doorgaande exploitatiewerkzaamheden (de samenlooprisico's);
- Bijlage C: zijn de bouwkundige, technische en organisatorische keuzes ten aanzien van veiligheid opgenomen;
- Bijlage D: bevat het vigerende calamiteitenbestrijdingsplan behorende tot het tunnelveiligheidsdossier.

Dit IVP is een coördinatie document dat zal worden aangepast indien wijzigingen in de praktijk daar aanleiding toe geven. Zie hiervoor de tabel "versiebeheer" in de colofon. Voorbeeld: in het IVP voor een vijfjarig onderhoudscontract kan bij de voorbereiding nog niet worden voorzien welke partijen in het vijfde jaar

ingeschakeld gaan worden. Zodra dat wel bekend is, zal het IVP hierop moeten worden aangepast.
Indien volledig ingevuld en correct gebruikt voldoet dit IVP aan de wettelijk vereisten voor een V&G-plan; hierdoor is een separaat V&G-plan niet nodig.

1 Uitgangspunten en randvoorwaarden

1.1 Beleidsverklaring veiligheid Rijkswaterstaat

Met deze beleidsverklaring beloven wij, team Rijkswaterstaat, dat we ons uiterste best gaan doen om onze maatschappelijke taken zo veilig mogelijk uit te voeren over de volle breedte van ons werkgebied, zowel in het fysieke als in het digitale domein.

Het is onze plicht en onze ambitie om ons land te beschermen tegen hoog water. De gebruikers moeten onze wegen en vaarwegen, oppervlaktewateren en objecten veilig kunnen gebruiken. Ook het werken aan de veiligheid van omwonenden van ons werkgebied is onze zorg. Bovendien zorgen we ervoor dat iedereen die bij Rijkswaterstaat of in onze opdracht werkt, zijn of haar werk veilig kan doen.

We streven naar een proactief veiligheidsniveau op de veiligheidscultuurladder. Dit betekent dat we binnen Rijkswaterstaat continu gericht zijn op het voorkomen van veiligheidsrisico's en incidenten en dat blijven doen.

Dat doen we door actief en effectief samen te werken aan veiligheid en goed af te stemmen. Zowel binnen Rijkswaterstaat als met onze maatschappelijke partners en met behoud van ieders verantwoordelijkheid. Wij van Rijkswaterstaat hebben daarin een voorbeeldfunctie en nemen een voortrekkersrol.

Wij werken daaraan volgens een veiligheidsmanagementsysteem dat erop is gericht de veiligheidssituatie van onze objecten en infrastructuur continu te verbeteren. Over de voortgang en de resultaten daarvan leggen we verantwoording af.

Als het gaat om de arbeidsveiligheid streven we naar nul doden en nul ernstig gewonden. Als anderen werken op onze terreinen, zorgen we ervoor dat ook zij voldoen aan de veiligheidseisen en –normen die we aan onze eigen medewerkers stellen.

Wij kennen de belangrijkste veiligheidsrisico's op onze netwerken. We werken continu samen aan het beter beheersen ervan en ontwikkelen het leiderschap, de kennis en het vakmanschap dat daarvoor nodig is.

Bovendien investeren we in een open cultuur die erop gericht is samen continu te verbeteren, te leren en elkaar scherp te houden. Een cultuur waarin we open het gesprek aangaan over risico's, dilemma's, fouten en onveilig gedrag.

Als het nodig is, spelen we veerkrachtig, daadkrachtig en professioneel in op gevaarlijke situaties en incidenten. We communiceren hier eerlijk, open en tijdig over en werken aan goede voorlichting over de veiligheid op en rond onze netwerken.

Ten slotte analyseren we incidenten om daarvan te leren. Opdat we maatregelen kunnen nemen om die incidenten in het vervolg te voorkomen. Daarmee krijgen we een steeds scherper oog voor nieuwe ontwikkelingen die de veiligheid in ons werkgebied bedreigen.

Oktober 2024

Martin Wijnen
Directeur-generaal Rijkswaterstaat

1.2 Ambitie en doelen

Rijkswaterstaat heeft zich gecommitteerd aan een proactieve en integrale aanpak van veiligheidszorg voor:

- Medewerkers en andere betrokkenen;
- Gebruikers van de wegen en de vaarwegen;
- Omwonenden.

Met als streven: nul doden en nul ernstig gewonden.

Deze algemene ambitie is door de opdrachtgever en het projectteam vertaald in de volgende projectspecifieke doelen:

- Veilige werkplek voor opdrachtnemer;
- Veiligheid geborgd in alle projectfases;
- Het projectteam staat voor een proactieve veiligheidscultuur;
- Er wordt bij de uitvoering minimaal eenmaal een Safety Walk uitgevoerd, samen met Opdrachtnemer;
- Alle incidenten, gevaarlijke situaties en bijna ongevallen worden gemeld.

Onze ambitie op het gebied van veiligheid sluit aan bij de ambitie zoals de DG (directeur-generaal) van Rijkswaterstaat deze heeft verwoord in de Beleidsverklaring Veiligheid RWS. We hebben een proactieve houding ten aanzien van veiligheid (trede 4 op de veiligheidscultuurladder).

Het team heeft als motto: 'We kennen de veiligheidsrisico's en nemen daarin verantwoorde keuzes.'

Om onze ambitie te bereiken, is het niet voldoende om alleen bezig te zijn met het Integraal veiligheidsplan en stil te staan bij BTO-keuzes (bouwkundige, technische en organisatorische keuzes). Het Integraal veiligheidsplan dient op verschillende lagen in het projectteam te leven en in onze genen te zitten.

Om dit te bereiken monitoren en/of organiseren we als kernteam:

- De bewustwording van veiligheid in het team;
- Wat noodzakelijk is voor de projectvoortgang.

Veiligheidsbewustzijn vergroten we door veiligheid in verschillende overleggen periodiek te agenderen (safetytopics), themasessies te organiseren en een bezoek aan een soortgelijk project met veiligheid als thema.

1.3 Gedragsregels voor projectmedewerkers

Voor dit project gelden de volgende gedragsregels:

1. Ik heb een voorbeeldfunctie.
2. Ik neem veiligheid altijd mee in mijn werk.
3. Ik zorg voor een veilige werkomgeving.
4. Ik stop elke klus die niet veilig voelt.
5. Ik meld (bijna)ongevallen altijd via 0800-8002 en bespreek deze.
6. Ik zorg voor de juiste persoonlijke bescherming (PBM's).
7. Ik heb respect voor andermans mening en voor de afspraken en richtlijnen inzake veiligheid.

1.4 Relevante veiligheidsdomeinen

Voor dit project zijn de volgende aangekruiste veiligheidsdomeinen relevant:

- ☒ Arbeidsveiligheid (altijd relevant)
- ☒ Verkeersveiligheid
- ☐ Nautische veiligheid
- ☐ Veiligheid tegen overstromen
- ☒ Externe veiligheid
- ☐ Machineveiligheid
- ☒ Elektrische veiligheid
- ☒ Tunnelveiligheid
- ☒ Constructieve veiligheid
- ☒ Sociale veiligheid
- ☒ Brandveiligheid
- ☒ Integrale beveiliging

De definities van bovengenoemde veiligheidsdomeinen kun je terugvinden in Bijlage A.

De aangekruiste veiligheidsdomeinen worden behandeld in dit IVP. *Niet relevante veiligheidsdomeinen voor dit project*

Nautische veiligheid is voor dit object niet van toepassing aangezien in de nabijheid van het object zich geen water bevind.

Veiligheid tegen overstroming is voor dit object niet van toepassing. Het object bevindt zich niet in een dijkring, primaire en/of regionale keringen .

Machineveiligheid is niet van toepassing binnen deze overeenkomst. Het verlichtingssysteem is geen machine.

2 Het project

2.1 Reikwijdte en grenzen project

2.1.1 Omschrijving van het project/bouwwerk

De Schipholtunnel is een belangrijke infrastructuur in Nederland, gelegen in de gemeente Haarlemmermeer, Noord-Holland. Deze tunnel maakt deel uit van de autosnelweg A4 en loopt onder de Buitenveldertbaan van luchthaven Schiphol door.

Met een lengte van 650 meter en een breedte van 103 meter is de Schipholtunnel de breedste tunnel van Nederland. De tunnel bestaat uit acht buizen (vier buizen ten behoeve van de A4) met in totaal 18 rijstroken, waarvan 12 rijstroken onderdeel uitmaken van de A4. Dagelijks maken ruim 170.000 voertuigen gebruik van de tunnel, wat het een cruciale verbinding maakt tussen Noord- en Zuid-Holland.

De Schipholtunnel werd voor het eerst geopend in 1966 en een tweede tunnel werd toegevoegd in 2000. Naast de tunnel voor wegverkeer is er ook een spoorwegtunnel, de Schipholspoortunnel. De tunnel wordt 24/7 bediend en bewaakt vanuit de Verkeerscentrale Noord-West Nederland in Velsen-Zuid.

Werkzaamheden binnen uitvoering overeenkomst

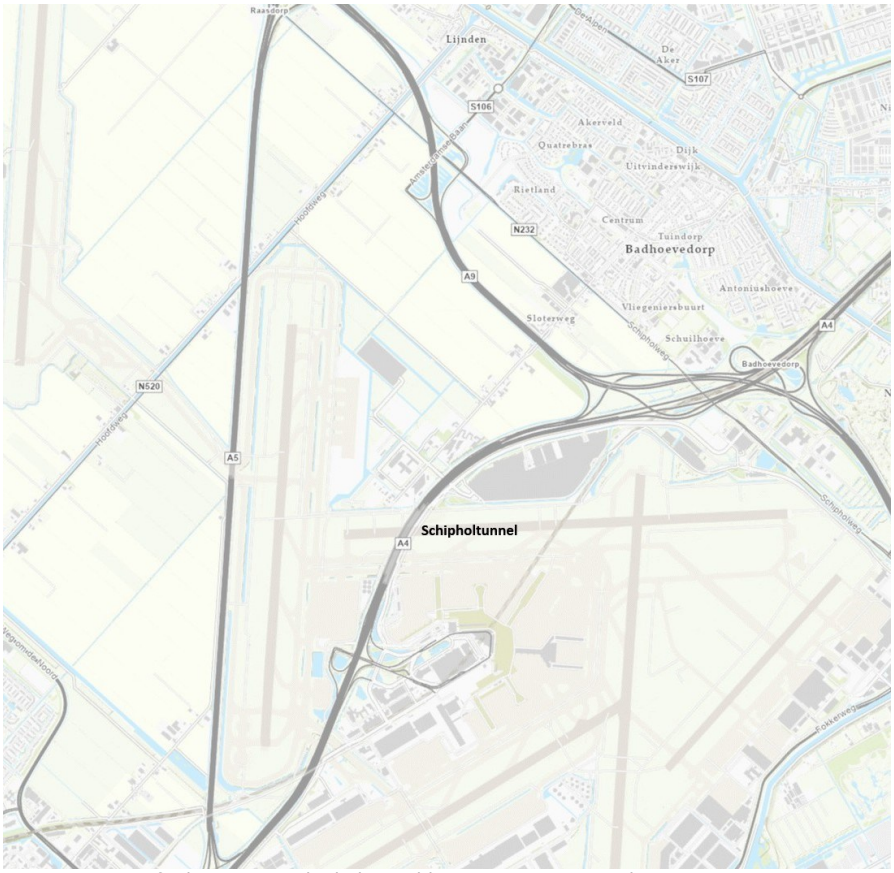
De scope betreft het vervangen van de bestaande tunnelverlichting/openbare verlichting verkeersbuis, inclusief de armaturen aan de wanden van de toeritten. Bestaande uit (niet-limitatief):

- Verwijderen bestaande installatie
    - Verlichtingsarmaturen;
    - Deel van de bekabeling;
    - Ophangconstructie;
    - L2 en L20 sensoren;
    - Besturingskasten oostbuizen;
    - Kritische laagspanningsverdelers vluchtgang westbuizen (inclusief verwijderen gasblusinstallatie en brandwerende beplating)[1].
- Nieuw realiseren
    - Ophangconstructie;
    - Verlichtingsarmaturen;
    - Besturings- en driverkasten;
    - Bekabeling (incl. doorvoeringen);
    - Kritische laagspanningsverdelers vluchtgang westbuizen;
    - Aanpassen laagspanningsverdelers dienstgebouwen en vluchtgang;
    - Aanpassen software SATTline (incl. MMI);
    - L20 Sensoren inclusief masten;
    - Kabelgoten, bevestigingsmaterialen en constructies.

2.1.2 Locatie van het bouwwerk (fysieke grenzen)

Deze Schipholtunnel maakt deel uit van de autosnelweg A4 en loopt onder de Buitenveldertbaan van luchthaven Schiphol door.

[1] Door een incident bij één van de kritische laagspanningsverdelers (regelkasten) van de verlichting in de vluchtgang van de westbuis zijn preventieve maatregelen genomen. De kabelgoten ter hoogte van deze verdelers zijn omkast met brandwerende beplating en de laagspanningsverdelers zijn voorzien van een decentrale gasblusinstallatie. Vanwege het verwijderen van deze verdelers zijn de maatregelen die zijn genomen niet meer noodzakelijk.



Figuur 1 Geografische positie Schipholtunnel bron KernGIS GeoWeb

De fysieke grenzen ten behoeve van het project lopen vanaf ca. hmp 6,6 tot hmp 7,7.



Figuur 2 Grenzen werkterrein

2.2 Betrokken partijen

Deze paragraaf bevat een overzicht van alle betrokken partijen, die belang hebben bij dit IVP.

2.2.1 Opdrachtgever

Organisatie	Ministerie van Infrastructuur en Waterstaat Directoraat Generaal Rijkswaterstaat
Naam	*Jeroen Verburg*
Bezoekadres	*Surinamepad 90*
Postcode en Plaats	*2035 VS, Haarlem*
Telefoonnummer	*06-11 52 63 74*
Emailadres	*Jeroen.verburg@rws.nl*

2.2.2 Opdrachtnemer(s)

Organisatie	*Nader te bepalen*
Naam	*Naam*
Bezoekadres	*Adres*
Postcode en Plaats	*Postcode, Plaats*

Telefoonnummer	*Telefoonnummer*
Emailadres	*Emailadres*

2.2.3 Overige partijen

De volgende partijen spelen binnen de veiligheid van de Schipholtunnel ook een rol.

Onderhoudsaannemer Schipholtunnel (TOPII)

Organisatie	*Equans*
Naam	-
Bezoekadres	*Albert Heijnweg 1*
Postcode en Plaats	*1507 EH, Zaandam*
Telefoonnummer	*+31 88 484 70 00*
Emailadres	*-l*

2.3 Coördinator Ontwerpfase, V&G-coördinator en Coördinator Uitvoeringsfase

2.3.1 Coördinator Ontwerpfase, namens de opdrachtgever

In de Arbowet bedoelt men met 'ontwerpfase', alle werkzaamheden die overeenkomen met activiteiten die bij RWS in de planfase en de start van de realisatiefase plaatsvinden. Ontwerpwerkzaamheden die de ON uitvoert horen ook nog tot de ontwerpfase als bedoeld in de wet.
In het door RWS opgestelde verbeterplan Veiligheid in projecten (opgesteld n.a.v. een aantal dodelijke ongevallen in 2017) worden een aantal verbetermaatregelen gepresenteerd.
De wettelijke Ontwerpfase loopt totdat de uitvoering start en eindigt dus niet na Contractgunning. In voorkomende gevallen kunnen Ontwerpfase en Uitvoeringsfase parallel lopen. (let op VTW's en herontwerp).

Coördinator Ontwerpfase

Organisatie	*Rijkswaterstaat*
Naam	*Martijn Heemink*
Bezoekadres	*Surinamepad 90*
Postcode en Plaats	*2035 VS, Haarlem*
Telefoonnummer	*+31 6 50 19 72 95*
Emailadres	*martijn.heemink@rws.nl*

2.3.2 V&G-Coördinator Opdrachtgever

V&G-Coördinator Opdrachtgever

Organisatie	*Rijkswaterstaat*
Naam	*Rutger van der Kloes*
Bezoekadres	*Surinamepad 90*
Postcode en Plaats	*2035 VS, Haarlem*
Telefoonnummer	*+31 6 501 97 991*
Emailadres	*rutger.vander.kloes@rws.nl*

2.3.3 Coördinator Uitvoeringsfase, namens de Opdrachtnemer

Nader te bepalen: de wettelijke Uitvoeringsfase begint als "start realisatie".
N.B. de wettelijke Uitvoeringsfase begint als "de schop in de grond gaat".

Coördinator Uitvoeringsfase

Organisatie	*Nader te bepalen*
Naam	*Naam*
Bezoekadres	*Adres*
Postcode en Plaats	*Postcode, Plaats*
Telefoonnummer	*Telefoonnummer*
Emailadres	*Emailadres*

2.3.4 Verdeling van overige taken en verantwoordelijkheden

Gedurende de looptijd van de samenwerkingsovereenkomst (SO3), is en blijft de beheerder verantwoordelijk voor zijn areaal. De opdrachtnemer dient in overleg met de beheerder op locatie te gaan.

Beheerder voor object gebonden technische vragen

Organisatie	*Rijkswaterstaat*
Naam	*Mike Peschier*
Bezoekadres	*Surinamepad 90*
Postcode en Plaats	*2035 VS, Haarlem*
Telefoonnummer	*+31 6 501 97 190*
Emailadres	*mike.peschier@rws.nl*

De taken en verantwoordelijkheden voor de RWS IPM-rolhouders zijn beschreven in het RWS Kader Integrale Veiligheid in Projecten (KIViP).

Samenvattend:

Projectmanager
Is eindverantwoordelijk voor de integrale borging van veiligheid binnen zijn project.

Technisch manager
Coördineert de integrale borging van veiligheid binnen zijn project, en is daar operationeel verantwoordelijk voor.

Omgevingsmanager
Inventariseert klanteisen inzake veiligheid, overlegt met de veiligheidsregio betreffende het minimaliseren van veiligheidsrisico's voor de omgeving (verkeer, omwonenden), communiceert en stemt af met omgeving.

Contractmanager
Is verantwoordelijk voor de noodzakelijke contracteisen, voor de juiste uitvoering van het contract en voor een correcte oplevering van de resultaten van het contract.

Manager projectbeheersing
Coördineert interne kwaliteitsborging (IKB), coördineert en faciliteert de beschikbaarheid van de juiste stuurinformatie, waaronder de jaarlijkse beoordeling van het veiligheidsmanagement binnen zijn project aan de hand van en de rapportage daarover aan de opdrachtgever.

V&G-coördinator
De V&G Coördinator (VGC) is "aanjager en waakhond" (luis in de pels) in afstemming met de Technisch manager en ondersteunt de organisatie bij het bewaken en borgen van integrale veiligheid.

Adviseurs en medewerker

Iedere adviseur en medewerker heeft als taak om zijn functie uit te oefenen met in achtneming van de gedragsregels veiligheid en is verantwoordelijk voor zijn of haar eigen veiligheid en die van personen waar hij of zij direct invloed op uitoefent.

2.4 Planning van de werkzaamheden

Beoogde datum aanvang werkzaamheden op bouwlocatie/in areaal	*Juni 2027*
Beoogde datum einde werkzaamheden	Augustus 2027
Beoogde uitvoeringsduur	*Zie contract*
Beoogde meerjarige onderhoudsperiode	*Niet van toepassing*

Ten behoeve van de uitvoering van de werkzaamheden zijn de volgende Slots aangevraagd en toegekend voor deze overeenkomst:

Vervangen verlichting Westbuis 2	*14-06-2027 / 22-06-2027*
Vervangen verlichting Westbuis 1	*26-07-2027 / 02-08-2027*
Vervangen verlichting Oostbuis 2	*03-08-2027 / 09-08-2027*
Vervangen verlichting Oostbuis 1	*10-08-2027 / 17-08-2027*

3 Maatregelen

In dit hoofdstuk worden de maatregelen beschreven waarmee de geïdentificeerde risico's (bijlage B) worden gemitigeerd (gereduceerd). Hoewel het hele IVP een dynamisch document is, en geactualiseerd wordt zodra de werkzaamheden daartoe aanleiding geven, geldt dit zeker voor dit hoofdstuk.

Voor de start van de uitvoering van de werkzaamheden dient de opdrachtnemer conform het Vraagspecificatie Proces ten aanzien van het bijhouden van een integraal veiligheidsdossier en conform eis IV200 ten aanzien van het veilig uitvoeren van de werkzaamheden de werkplek bezocht te hebben en de mogelijke onveilige locaties/situaties in kaart gebracht te hebben en te hebben vastgelegd (in het integraal veiligheidsdossier van het betreffende object). Op basis daarvan dienen adequate beheersmaatregelen toegepast te worden. De relevante documenten, bestaande V&G-dossiers zoals opgenomen het integraal veiligheidsdossier evenals de RI&E zoals opgenomen bij dit plan dienen hierbij als vertrekpunt. De volgende veiligheidsthema's en maatregelen zijn van toepassing bij de uitvoering van het onderhavige contract:

3.1 Arbeidsveiligheid

Arbeidsveiligheid betekent het wegnemen van en/of het preventief beheersen van risico's bij de uitvoering van werkzaamheden door medewerkers van Rijkswaterstaat en door diegenen die voor RWS werken.

3.1.1 Integraal Veiligheidsplan (V&G-plan Ontwerpfase)

Rijkswaterstaat stelt een Integraal Veiligheidsplan (IVP) op. Dit is de wettelijke invulling van het V&G-plan Ontwerpfase (artikel 2.28 Arbeidsomstandighedenbesluit).

De opdrachtnemer moet op basis van dit IVP een V&G-plan Uitvoeringsfase opstellen.

Conform het voorschrift vanuit de Arbo wet en Regeling voor een V&G-plan wordt in dit IVP het volgende beschreven:
- De betrokken partijen, zie hoofdstuk 2;
- De regels en voorschriften, zie hoofdstuk 1;
- De afstemming over V&G-coördinatie, zie hoofdstuk 3.1.3;
- De maatregelen die volgen uit de risico-inventarisatie en -evaluatie, zie hoofdstuk 3;
- De afspraken met betrekking tot de uitvoering van de maatregelen, zie hoofdstuk 4;
- De voorlichting en instructie van medewerkers, zie hoofdstuk 7.

3.1.2 Overdracht V&G-coördinator

Rijkswaterstaat heeft een coördinator ontwerpfase aangesteld, zie paragraaf 2.3.1.

De Opdrachtnemer stelt een V&G-coördinator voor de uitvoeringsfase aan die

de taken en verantwoordelijkheden zoals beschreven in artikel 2.31 van het Arbeidsomstandighedenbesluit op zich neemt. Tussen de V&G-coördinator van de Opdrachtgever en de V&G-coördinator van de Opdrachtnemer vindt een overdrachtsbespreking plaats.

N.B:
Voor dit Werk is nog geen V&G-coördinator aangesteld. De bedoeling is dat tijdens de uitvoering van het project wel een V&G-coördinator is toegewezen aan dit project. Voorlopig zal daarom de technisch manager deze rol waarnemen.

De overdracht van de volgende documenten zal gerealiseerd door deze mee te sturen als bijlage bij de offerteaanvraag:
- V&G-plan 'Ontwerpfase', dit IVP.

Tevens wordt er een warme overdracht-bespreking georganiseerd waarin de OG een toelichting verzorgd op de hierboven opgesomde documenten. De warme overdracht betreft een overleg tussen de OG en de ON.

Verder is, conform het Arbobesluit, afdeling 5 "Bouwproces" (hiermee bedoelt de inspectie), de artikelen 2.23 tot en met 2.35 en de toelichting in de Basisinspectiemodule-Bouwprocesbepalingen, SZW, 2015, het volgende van belang:

A. Bevat dit IVP de juiste specifieke gevaren, de juiste maatregelen om daarmee om te gaan en de "BTO-keuzen" die als gevolg van de exercitie onder A. gemaakt zijn? ("BTO-keuzen" = Bouwkundige, Technische en Organisatorische keuzen (art. 2.28 lid f);
B. Kunnen de coördinatoren hun taken naar behoren vervullen, vervullen ze deze naar behoren en stuurt de Opdrachtgever of uitvoerende partij dit voldoende bij? (gebaseerd op art. 2.29 t/m 2.33).

3.1.3 Risico's Arbeidsveiligheid

De grootste risico's ten aanzien van arbeidsveiligheid zijn:
- Werknemers worden aangereden bij werkzaamheden langs de weg, door onjuist uitgevoerde verkeersmaatregelen of het niet opvolgen van instructies/ procedures;
- Risico's zoals: verstikking of bedwelming, vanwege het uitvoeren van werkzaamheden in besloten ruimten;
- Werknemers vallen van hoogte bij het uitvoeren van werkzaamheden, bijvoorbeeld doordat hoogteverschillen onvoldoende zijn afgeschermd.
- Werknemers worden plotseling blootgesteld aan extreme weersomstandigheden, zoals bliksem, zware regenval, windstoten of extreme hitte/kou.
- Werknemers raken bekneld of komen vast te zitten bij het inspecteren in de buurt van bewegende machinedelen;
- Werknemers worden geëlektrocuteerd bij meetwerkzaamheden in de buurt van onder spanning staande delen;
- Aanrijding doordat werknemers lange afstanden moeten rijden en vermoeid of afgeleid raken onder het rijden.

3.1.4 Samenlooprisico's

Samenlooprisico's ontstaan wanneer er meerdere partijen gelijktijdig op een object aan het werk zijn, of doordat er in de omgeving van het werkterrein gelijktijdige

projecten zijn. Voorbeelden van samenlooprisico's zijn: aanrijding, hoge geluidsniveaus, stofvorming, elektrocutie en/of vallende materialen.

De Opdrachtnemer moet in het V&G plan aangeven bij welke objecten samenlooprisico's te verwachten zijn, op welke wijze hij deze mogelijke risico's gaat beheersen en de samenwerking en afstemming met andere partijen gaat organiseren.

3.1.5 Maatregelen Arbeidsveiligheid

De volgende maatregelen dienen te worden genomen, zodat de Opdrachtnemer de veiligheid kan borgen:

- De OG dient ON periodiek te toetsen ten aanzien van integrale veiligheid;
- De OG dient dit IVP te hebben verstrekt aan ON;
- De ON dient te handelen conform de huisregels van de regionale dienst en huisregels van Rijkswaterstaat;
- De ON voert geen destructieve handelingen uit aan de objecten;
- De ON dient met de objecten om te gaan alsof deze chroom-6 houdend zijn;
- De ON dient met de objectdeskundige (en ter plaatse met de bedienaar) de werkzaamheden af te stemmen. De ON dient voorlichting en instructie te geven voorafgaand aan de werkzaamheden aan iedereen die werkzaamheden verricht;
- De ON dient melding te maken van alle gevaarlijke situaties en ongevallen aan de technisch manager van OG;
- De ON dient de geïnventariseerde risico's te beheersen door adequate veiligheidsmaatregelen te nemen conform de arbeidshygiënische strategie conform de Arbeidsomstandighedenwet artikel 3 lid 1 sub b;
- De ON dient vóór aanvang van de werkzaamheden een werkvergunning aan te vragen bij de objectdeskundige.

3.2 Verkeersveiligheid

Verkeersveiligheid betekent het wegnemen van en/of preventief beheersen van risico's voor verkeersdeelnemers op de weg. Het risico dat werknemers aangereden worden tijdens werkzaamheden, is opgenomen onder hoofdstuk 3.1 Arbeidsveiligheid.

3.2.1 Risico's Verkeersveiligheid

De grootste risico's ten aanzien van verkeersveiligheid zijn:

- Verkeersdeelnemers veroorzaken een verkeersongeval, vanwege het negeren van verkeersmaatregelen;
- Verkeersdeelnemers veroorzaken een verkeersongeval, vanwege onjuiste of onvoldoende verkeersmaatregelen;
- Werknemers veroorzaken een verkeersongeval, door onjuist uitgevoerde verkeersmaatregelen of het niet opvolgen van instructies/ procedures;
- Werknemers veroorzaken een aanrijding, doordat werknemers lange afstanden moeten rijden en vermoeid of afgeleid raken onder het rijden.

3.2.2 Maatregelen Verkeersveiligheid

De Opdrachtgever (OG) heeft de volgende maatregelen genomen, zodat de Opdrachtnemer (ON) de veiligheid kan borgen:

- De ON dient de verkeersmaatregelen aan te vragen bij het bevoegd gezag en dient de OG hierover te informeren;
- De ON dient de verkeersmaatregelen uit te voeren conform de relevante richtlijnen uit de CROW96a en 96b, eventueel aangevuld met specifieke eisen vanuit de beheerder;
- De ON dient de richtlijn reductie aanrijdgevaar op te volgen. Meer informatie over deze richtlijn is te vinden op de website van de Governance Code Veiligheid in de Bouw (GCVB), welke te benaderen is via onderstaande link: https://gc-veiligheid.nl/tools/nieuw-beleid-reductie-aanrijdgevaar.

3.3 Externe veiligheid

Externe veiligheid is de kans dat personen in de omgeving van het hoofdwegennet of hoofdvaarwegennet, als gevolg van transport van vervoer gevaarlijke stoffen of als gevolg van een activiteit waar met gevaarlijke stoffen wordt gewerkt, slachtoffer worden van een ongeval met die stoffen.

3.4 Elektrische veiligheid

Dit betreft het wegnemen van en/of preventief beheersen van risico's van elektrische installaties. Deze moeten zo zijn ontworpen, ingericht, aangelegd, onderhouden en gekenmerkt, dat een veilig gebruik van elektriciteit zo goed mogelijk is gewaarborgd. Hierbij voldoen aan het Arbeidsomstandighedenbesluit en eisen, normen en richtlijnen t.b.v. realisatie, beheer en onder houd elektrische installaties, waaronder NEN 3140, NEN 1010.

3.5 Tunnelveiligheid

Bij tunnelveiligheid is het streven dat door het ontwerp, de bouw en het gebruik van een tunnel, de veiligheid van de tunnel zo optimaal mogelijk is voor de gebruikers en het personeel. Deze regelgeving is vastgelegd in de Tunnelwetgeving en Landelijke Tunnel Standaard van RWS.

3.6 Constructieve veiligheid

Onder constructieve veiligheid wordt verstaan de veiligheid van personen met betrekking tot het bezwijken van of het ontstaan van schade aan constructies zoals damwanden, maar richt zich ook op de stabiliteit van grondlichamen en woningen. Voor dit project geldt specifieke aandacht (verhoogd risico) voor:

- Hijspunten (sterkte, keuring,..);
- Tijdelijke constructies;
- Aanlijnpunten (verankering voor valbeveiliging);
- Opstellen zwaar materiaal op/naast een tunnel (i.v.m. draagkracht);
- Valbeveiligingsconstructies;
- Vaste trappen.

3.7 Sociale veiligheid

Sociale veiligheid betekent het wegnemen van en/of preventief beheersen van risico's voor medewerkers van RWS en gebruikers van onze voorzieningen tegen gevaar dat veroorzaakt wordt door of dreigt van de kant van menselijk handelen in de openbare ruimte.

3.7.1 Risico's Sociale veiligheid

De grootste risico's ten aanzien van sociale veiligheid zijn:
- Verkeersdeelnemers beledigen of bedreigen werknemers, vanwege ontevredenheid over tijdelijke verkeersmaatregelen.

3.7.2 Maatregelen Sociale veiligheid

Er zijn door OG geen maatregelen getroffen ten aanzien van sociale veiligheid. Het risico is onder andere afhankelijk van de tijd en plaats van de werkzaamheden. ON dient dit risico per werklocatie te beoordelen.

3.8 Brandveiligheid

Onder brandveiligheid wordt verstaan de persoonlijke bescherming van mensen tegen (de gevolgen van) brand, het voorkomen en beperken van schade aan het object door brand.

Het domein brandveiligheid heeft ook betrekking op werkzaamheden zoals snijbranden en lassen.

Daarnaast valt te denken aan elektrabranden en het herstellen van brandcompartimenten na werkzaamheden, zoals het doortrekken van kabels en leidingen.

3.9 Integrale beveiliging

Integrale beveiliging betekent het wegnemen van en/of preventief beheersen van risico's van menselijk gedrag (bewust en onbewust, bedoeld en onbedoeld, gewild en ongewild) die de staat, aard en functionaliteit van het areaal van Rijkswaterstaat kunnen aantasten.

Integrale beveiliging is opgedeeld in 4 deelgebieden:
- Fysieke beveiliging
- Informatiebeveiliging (cybersecurity)
- Beveiliging Persoonsgegevens (AVG)
- Integriteit

3.9.1 Fysieke beveiliging

Het wegnemen van en/of preventief beheersen van risico's van fysiek menselijk gedrag (bewust en onbewust, bedoeld en onbedoeld, gewild en ongewild) die de staat, aard en functionaliteit van het areaal van Rijkswaterstaat kunnen aantasten.

3.9.2 Informatiebeveiliging (Cybersecurity)

Het wegnemen van en/of preventief beheersen van risico's van menselijk gedrag in de vorm van indringing in de informatiesystemen (bewust en onbewust, bedoeld en onbedoeld, gewild en ongewild) die de staat, aard en functionaliteit van het areaal van Rijkswaterstaat kunnen aantasten.

3.9.3 Beveiliging persoonsgegevens (AVG)

Het wegnemen van en/of preventief beheersen van risico's van onrechtmatig en/of onrechtvaardig gebruik van persoonsgegevens.

3.9.4 Integriteit

Integriteit gaat niet alleen over goed of fout, maar vooral over de manier waarop wordt omgegaan met morele dilemma's. Bewustwording en het bewust-blijven, vormen de rode draad in elk plan.

Ten aanzien van integriteit zijn er twee parallelle benaderingen.

1. De nalevingsbenadering richt zich op het vermijden van fraude en corruptie. Bijbehorende maatregelen bestaan uit het formuleren van regels, richtlijnen, protocollen en gedragscodes.
2. De stimuleringsbenadering legt de nadruk op het stimuleren van medewerkers om op een zorgvuldige manier om te gaan met de verantwoordelijkheden die samenhangen met hun rol en functie. De nadruk ligt op het vergroten van bewustzijn, inzicht en oordeelsvermogen.

Integriteit zal in de ontwerpfase en uitvoeringsfase de benodigde aandacht vragen en krijgen.

4 Afspraken

4.1 Aanstelling coördinator realisatiefase

De ON dient conform het Arbeidsomstandighedenbesluit een coördinator uitvoeringsfase aan te stellen. De coördinator voor de uitvoeringsfase heeft tot taak om namens de uitvoerende partij:

- Te bewerkstelligen dat de maatregelen die werkgevers en zelfstandigen nemen op de meetlocatie ter bescherming van de veiligheid en gezondheid van werknemers en zelfstandigen op doeltreffende wijze worden toegepast;
- Met het oog op de bescherming van de werknemers en zelfstandigen zeker te stellen dat gelijktijdig of achtereenvolgend aanwezige werkgevers en zelfstandigen op de meetlocaties de werkzaamheden goed op elkaar afstemmen;
- De voorlichting van werknemers op de meetlocatie te bewerkstelligen;
- De nodige maatregelen te nemen opdat alleen bevoegde personen de meetlocaties kunnen betreden;
- Ervoor te zorgen dat het veiligheids- en gezondheidsplan en het dossier worden aangepast indien de voortgang van de werkzaamheden daarvan daartoe aanleiding geven;
- Doeltreffende maatregelen te nemen indien werkgevers of zelfstandigen naar zijn oordeel niet of in onvoldoende mate of op onjuiste wijze uitvoering geven aan een samenhangende toepassing van hun verplichtingen.

4.2 Melding Nederlandse Arbeidsinspectie

Er wordt door de opdrachtnemer een melding gemaakt bij de Nederlandse Arbeidsinspectie indien:

- De melding is verplicht als de geraamde duur van de totstandbrenging van het bouwwerk meer dan 30 werkdagen beslaat en op die bouwplaats meer dan 20 werknemers tegelijkertijd arbeid zullen gaan verrichten, of;
- Met de totstandbrenging van het bouwwerk meer dan 500 mensdagen gemoeid zullen zijn.

4.3 Actualisatie IVP

Dit IVP is opgesteld tijdens de contractvoorbereidingsfase. De opdrachtnemer stelt een IVP op voor de uitvoeringsfase, op basis van voorliggend IVP Ontwerpfase.

Het Integraal Veiligheidsplan (ontwerp- en uitvoeringsfase) van de OG en ON dient geactualiseerd te worden indien de voortgang van het project of onderdelen daarvan daartoe aanleiding geven.

Om de OG aan zijn vergewisplicht te kunnen laten voldoen, zullen dus ook alle wijzigingen via de OG moeten verlopen. Tevens wordt de geactualiseerde versie gedeeld en indien nodig besproken met OG.

4.4 Organisatie rond incidentregistratie en -afhandeling

Er wordt zoveel mogelijk aangesloten bij de standaard (MIR), Meldpunt Incidenten Rijkswaterstaat. Bij een ongeval of incident met (ernstig) letsel aan Opdrachtnemerszijde, zal door Opdrachtnemer een incidenten onderzoek worden uitgevoerd. Integrale veiligheid is vast agendapunt tijdens het reguliere overleg tussen ON en OG. Hierbij zullen de resultaten van het onderzoek worden besproken. Tevens zal tijdens een risicosessie worden bekeken of het risico is onderkend en of de getroffen beheersmaatregel afdoende zijn, een en ander is ook afhankelijk van de uitkomst van het onderzoek.

Indien incidenten/calamiteiten optreden dient Opdrachtnemer tevens in contact te treden met de Technisch manager van dit project. De Technisch manager zal contact leggen binnen Rijkswaterstaat met de Contractmanager en Programma-manager.

Bij incidenten/ongevallen met dodeijke afloop, een ziekenhuisopname van >24 uur of blijvend letsel dient de ON de Nederlandse Arbeidsinspectie in te lichten.

4.5 Projectadviseur Integrale Veiligheid

Binnen het IPM-team van de opdrachtgever is een Projectadviseur Integrale Veiligheid aangesteld, welke zich bezighoudt met het ondersteunen op gebied van de Integrale Veiligheidsthema's. Hij voert onder andere de volgende werkzaamheden uit:

- Het toetsen van veiligheidsdocumentatie van de opdrachtnemer (zoals: werkplannen en het V&G-plan uitvoeringsfase);
- Advisering van OG en ON op het gebied van Integrale Veiligheidsthema's;
- Veiligheids- en waarnemingsrondes tijdens de werkzaamheden;
- Begeleiden van Safety Walks;
- Inventarisering van incidenten inclusief analyse tijdens ieder voortgangsoverleg door het IPM-team. De inventarisatie wordt gedeeld met de projectadviseur integrale veiligheid;
- Bijdrage aan T-rapportages;
- Bijwonen van SCB-toetsingen m.b.t. veiligheid als materiedeskundige;
- Er zijn afspraken gemaakt met de Opdrachtnemer(s) over het melden van onveilige situaties of handelingen (zie paragraaf 4.4). Alle gevaarlijke situaties en incidenten, ongeacht wie de veroorzaker is, dienen gemeld te worden zodat geleerd kan worden en de veiligheid op het project verbeterd wordt.

Projectadviseur Integrale Veiligheid

Organisatie	*Rijkswaterstaat*
Naam	*Hafid Chioue*
Bezoekadres	*Surinamepad 90*
Postcode en Plaats	*2035 VS, Haarlem*
Telefoonnummer	*+31 6 14945411*
Emailadres	*Hafid.chioue@rws.nl*

5 Wijze van toezicht

De formele wijze van toezicht door de OG is als volgt ingericht:

- Safety Walks zijn aangekondigde bezoeken aan de bouwlocatie, waarbij IPM-teamleden van zowel OG als ON aanwezig zijn. Deze bezoeken zijn gericht op het bevorderen van veiligheid en wederzijds inzicht in het werk. ON verleent medewerking aan deze bezoeken en volgt eventuele gezamenlijk vastgestelde verbetermaatregelen op. Uitgegaan dient te worden van twee Safety Walks.
- Een veiligheidsronde is een (on)aangekondigd bezoek aan de projectlocatie met als doel de status van de integrale veiligheid in kaart te brengen en te beoordelen of projectrisico's adequaat beheerst worden. Tijdens de ronde worden de bevindingen vastgelegd en, waar nodig, verbetermaatregelen afgesproken. ON verleent medewerking aan deze rondes en volgt de afgesproken maatregelen op.
- Contractbeheersing binnen RWS richt zich op samenwerking tussen OG en ON, waarbij integrale veiligheid een expliciet aandachtspunt is. Via systeemgerichte SCB wordt getoetst of veiligheidsverplichtingen conform contract worden nageleefd, en wordt de dialoog over risicobeheersing en veiligheidsbewustzijn actief gevoerd.
- Opvolging van incidentmeldingen vindt plaats volgens de door RWS vastgestelde procedure (zogenaamde bulkmeldingen) voor registratie, beoordeling, maatregelen en terugkoppeling. OG vereist dat incidenten aantoonbaar worden afgehandeld in het daartoe bestemde systeem. ON werkt hierin samen met de aangewezen actiehouder en adviseurs en draagt bij aan structurele verbetering van de veiligheid.
- V&G- en werkplannen in de uitvoeringsfase worden door OG beoordeeld, inclusief eventuele V&G-(deel)plannen van onderaannemers. Deze beoordeling valt onder de wettelijke vergewisplicht van OG in het kader van integrale veiligheid. V&G-(deel)plannen dienen via de ON aan OG ter beoordeling te worden aangeboden.

De informele wijze van toezicht door de OG is als volgt ingericht:

- Waarnemingen zijn (on)aangekondigde, informele vormen van toezicht waarbij OG haar bevindingen direct met ON deelt. Van een waarneming wordt niet altijd expliciet verslag opgemaakt. ON verleent medewerking aan deze waarnemingen en volgt eventuele afgesproken maatregelen op.
- Periodiek veiligheidsoverleg vindt plaats tussen OG en ON, met deelname van in elk geval de PIV'er (namens OG), de V&G-coördinator en – indien van toepassing – de veiligheidskundige van ON. In dit overleg wordt de stand van zaken rondom integrale veiligheid besproken en waar nodig worden acties afgestemd.

6 Verantwoording van BTO-keuzen

In dit hoofdstuk worden de bijzondere, technische en organisatorische ontwerpkeuzes toegelicht welke zijn genomen door de OG tijdens de formele 'ontwerpfase'.

Opgemerkt wordt dat er geen formeel 'ontwerp' is gemaakt. Het betreft de contractvoorbereiding voor het uitvoeren van landmeetkundige werkzaamheden ten behoeve van het onderzoeken van de constructieve veiligheid.

Toelichting bouwkundige, technische en organisatorische (BTO-) keuzen die in verband met de veiligheid van de werknemers en zelfstandigen worden gemaakt:

- De Opdrachtgever heeft in het ontwerp de BTO-keuze gemaakt dat per meting een afweging wordt gemaakt om te kijken of het noodzakelijk is in hoeverre een object in gebruik blijft.

Om de meetwerkzaamheden veilig uit te voeren, dient de ON per situatie passende maatregelen te nemen. Dat kan bijvoorbeeld door:

- Het nemen van verkeersmaatregelen;
- Meeliften met een gehele stremming;
- Het afsluiten van een tunnel;
- Of het meten van delen die op dat moment niet in beweging zijn (tussen de bediening door). Hiervoor is nauwe afstemming met de bedienaar noodzakelijk.

Per beheerobject zal de ON in overleg met de OG deze BTO-keuze maken en vastleggen in het (meet)rapport, werkplan of V&G-deelplan.

7 Opleiding en instructie

Alle projectmedewerkers van Rijkswaterstaat hebben de e-learning Integrale Veiligheid gevolgd op het Leerportaal van I&W.
Alle projectmedewerkers van Rijkswaterstaat die op de bouwplaats komen of beslissingen nemen die van invloed kunnen zijn op de omstandigheden tijdens de uitvoering zijn VCA-VOL gecertificeerd.
Alle projectmedewerkers van Rijkswaterstaat die op een bouwplaats komen van een aannemer, die aangesloten is bij de Governance Code Veiligheid in de Bouw, beschikken over een geldige GPI.

Alle medewerkers van de opdrachtnemer die aan dit project werken en buiten werkzaamheden hebben (incl. inspecties), zijn minimaal in het bezit van een persoonscertificaat VCA en hebben een geldige GPI. Nb. Indien de medewerkers een RWS-account hebben volgen zij ook de E-learning IV. Voor personen die een leidinggevende of sturende functie hebben moeten beschikken over VCA-VOL. Voor uitvoerende personen volstaat VCA-basis.

Indien er specifieke onderzoeken/werkzaamheden verricht gaan worden, met verhoogd risico, dan dient men hier aantoonbaar voldoende deskundig voor te zijn.

Medewerkers die specifieke werkzaamheden aan elektrisch installaties gaan verrichten zijn gekwalificeerd volgens de NEN-3140 en/of NEN 3840. Om in spanningsruimten te mogen komen (kijken) eist de beheerder minimaal een VOP-opleiding.

Daarnaast heeft RWS de WiV (Wijzer in Veiligheid) app. De RWS-medewerkers wordt gevraagd hier actief aan deel te nemen.

7.1 Veiligheidshuisregels Rijkwaterstaat, object specifiek en opdrachtnemer

Alle projectmedewerkers van zowel Rijkswaterstaat als de opdrachtnemer hanteren de Veiligheidshuisregels Rijkswaterstaat. Daarnaast gelden de object specifieke huisregels.

Indien de opdrachtnemer nog aanvullende eisen stelt met betrekking bijvoorbeeld PBM’s, regels bij projectbezoeken (zoals aan-/afmelden) dan dient de opdrachtgever hiernaar te vragen en zich hier ook aan moet houden.

7.2 Aanvragen werkvergunning

In de ontwerpfase en tijdens de realisatiefase is de schipholtunnel van de beheerder die het B&O uitbesteed heeft aan de ON. De normale procedure geldt (werkvergunning aanvragen): toestemming voor aanvraag om de tunnel te bezoeken bij de beheerder, deze koppelt je na akkoord aan de ON, die verantwoordelijk is tijdens afsluitingen voor coördinatie van o.a. samenlooprisico’s. Bij bezoek aan de dienstgebouwen, zonder afsluiting, kan evt. de beheerder akkoord geven dit zonder begeleiding ON te doen (wel een Cc).

7.3 PBM’s voor projectmedewerkers van Rijkswaterstaat

We volgen de wetgeving en het beleid ten behoeve van persoonlijke bescherming en zichtbaarheid. We dragen bij bezoek aan het object (langs de weg en in de tunnel (verkeersbuis)) altijd:

- veiligheidsschoenen;
- een helm voorzien van kinbandje;
- een oranje veiligheidsbroek;
- een oranje veiligheidsjas of oranje FLUO-hesje.

Aanvullende PBM’s zijn nodig als specifieke werkzaamheden erom vragen (zoals: gehoorbescherming, veiligheidsbril, handschoenen).

Projectmedewerkers van Rijkswaterstaat kunnen via hun eigen afdeling PBM’s laten bestellen. Ingehuurde medewerkers regelen dat via hun eigen organisatie. Indien er praktische problemen zijn met het organiseren van PBM’s op deze manier, dan zorgen we hier vanuit het project voor. Neem in dat geval contact op met het secretariaat.

Er zijn op diverse Rijkswaterstaat kantoorlocaties een voorraad leen-PBM’s beschikbaar via het servicepunt. Aanvullende PBM’s (indien nodig bij uitvoeringswerkzaamheden, bijvoorbeeld een gelaatsscherm) worden door ON verstrekt.

Bijlage A Definities

Algemene definities	
Veiligheid	Het wegnemen van en/of preventief beheersen van risico's die kunnen leiden tot letsel of economische of milieuschade.
Integrale veiligheid	Alle veiligheidsdomeinen van een systeem in samenhang beschouwd, gedurende de volledige lifecycle van een object of een netwerkschakel.
Risico	Een risico is een onzekere toekomstige gebeurtenis met negatieve consequenties, op het gebied van persoonlijk leed, economische en milieuschade en imagoschade. Onder veiligheidsrisico's worden met name de eerste twee verstaan. Een risico wordt veelal beschreven als product van kans van optreden en gevolg.
Beheersen van Risico's	Indien het risico niet kan worden weggenomen dient het op een voor RWS acceptabel niveau te worden gebracht. Acceptabel is een op basis van de risicomatrix afgewogen risico. Het restrisico moet expliciet afgewogen cf kader VM

Definities veiligheidsdomeinen	
NB Onderstaande veiligheidsdomeinen zijn van toepassing gedurende alle levensfasen van een object (kunstwerk, (vaar)wegvak, machine, installatie, etc.)	
Arbeidsveiligheid	Het wegnemen van en/of het preventief beheersen van risico's bij de uitvoering van werkzaamheden door medewerkers van Rijkswaterstaat en door diegenen die voor RWS werken.
Verkeersveiligheid	Het wegnemen van en/of preventief beheersen van risico's voor verkeersdeelnemers op de weg.
Nautische veiligheid	Het wegnemen van en/of preventief beheersen risico's voor verkeersdeelnemers op de vaarweg en op zee.
Waterveiligheid	Het wegnemen van en/of preventief beheersen van risico's van overstromen, wateroverlast en waterschaarste.
Externe veiligheid	Het wegnemen van en/of preventief beheersen van risico's van incidenten met gevaarlijke stoffen langs transportroutes (weg, water, spoor, buisleiding) of stationaire installatie.
Machineveiligheid	Het wegnemen van en/of preventief beheersen van risico's van machines.
Elektrische veiligheid	Het wegnemen van en/of preventief beheersen van risico's van elektrische installaties.
Tunnelveiligheid	Het wegnemen van en/of preventief beheersen van risico's voor verkeersdeelnemers in tunnels.
Constructieve veiligheid	Het wegnemen van en (proactief) beschermen tegen risico's van bezwijken van een constructie.
Sociale veiligheid	Het wegnemen van en/of preventief beheersen van risico's voor medewerkers van RWS en gebruikers van onze voorzieningen tegen gevaar dat veroorzaakt wordt door of dreigt van de kant van menselijk handelen in de openbare ruimte.
Brandveiligheid	Het wegnemen van en/of preventief beheersen van risico's van brand.
Integrale beveiliging	Het wegnemen van en/of preventief beheersen van risico's van menselijk gedrag (bewust en onbewust, bedoeld en onbedoeld, gewild en ongewild) die de staat, aard en functionaliteit van het areaal van Rijkswaterstaat kunnen aantasten.

Definities binnen Integrale beveiliging	
Fysieke beveiliging	Het wegnemen van en/of preventief beheersen van risico's van fysiek menselijk gedrag (bewust en onbewust, bedoeld en onbedoeld, gewild en ongewild) die de staat, aard en functionaliteit van het areaal van Rijkswaterstaat kunnen aantasten.
Informatiebeveiliging	Het wegnemen van en/of preventief beheersen van risico's van menselijk gedrag in de vorm van indringing in de informatiesystemen (bewust en onbewust, bedoeld en onbedoeld, gewild en ongewild) die de staat, aard en functionaliteit van het areaal van Rijkswaterstaat kunnen aantasten.
Bescherming persoonsgegevens	Het wegnemen van en/of preventief beheersen van risico's van onrechtmatig en/of onrechtvaardig gebruik van persoonsgegevens.

Bijlage B Ontwerp RI&E

Deze bijlage bevat de concrete risico's verbonden aan werkzaamheden binnen de projectscope, te weten object specifieke risico's en samenlooprisico's. Deze vormen de basis voor de maatregelen, afspraken en wijze van toezicht zoals beschreven in dit IVP.

De ontwerp RI&E is als los document bijgevoegd aan het aanbestedigsdossier in excel formaat.

Bijlage C BTO-keuzes

Deze bijlage bevat bouwkundige, technische en organisatorische keuzes die in verband met de veiligheid en gezondheid van de werknemers en zelfstandigen zijn gemaakt.

Rijkswaterstaat
Ministerie van Infrastructuur en Waterstaat

NAAR TOELICHTING

BTO-keuzes

Nr.	Projectfase	Bron	Stap 1: Situatie omschrijving	Stap 2: Dilemma	Stap 3: Keuze		Stap 4: Motivering	Stap 5: Gevolg									
	De projectfase waarin de BTO-keuze gemaakt is.	De herkomst van de BTO-keuze.	Omschrijf de situatie waarover een keuze gemaakt moet worden.	Omschrijf de keuze mogelijkheden.	Omschrijf welke keuze is gemaakt.	in IVP	Omschrijf de afwegingen die tot de betreffende keuze hebben geleid	Omschrijf de gevolgrisico's (de gevolgen van de keuze)									
								Gevolgrisico 1	Risico nummer Ontwerp RIE	Gevolgrisico 2	Risico nummer Ontwerp RIE	Gevolgrisico 3	Risico nummer Ontwerp RIE	Gevolgrisico 4	Risico nummer Ontwerp RIE	Gevolgrisico 5	Risico nummer Ontwerp RIE
1	Contractvoorbereiding	TBO	De verlichting van de Schipholtunnel is einde levensduur. De betrouwbaarheid en beschikbaarheid kan niet gegarandeerd worden tot VAR. Teveel uitval van verlichting (donkere plekken in de tunnel) heeft tot gevolg dat de veiligheid voor de weggebruiker niet gewaarborgd kan worden.	1 - Met vrijkomende materialen uit andere tunnels de installatie in de lucht houden. 2 - Het vervangen van de verlichtingsinstallatie	1 - De verlichtingsinstallatie vervangen.	Nee	Vrijkomende materialen uit andere tunnels zijn niet geschikt gebleken										
2	Contractvoorbereiding	TBO	Voor verlichting kan de keuze gemaakt worden voor Puntverlichting en Lijnverlichting.	1 - Puntverlichting overeenkomstig RTV 2023 2 - Lijnverlichting overeenkomstig RTV 2023 3 - Vrije keuze Opdrachtnemer	2 - Lijnverlichting overeenkomstig RTV 2023	Nee	Lijnverlichting geeft meer comfort naar de weggebruikers. Je hebt geen last van flikkeringen en geeft heel mooi egaal beeld.										
3	Contractvoorbereiding	Ontwerpkeuze beheerder	Arbeidsveiligheid, verkeersveiligheid: Verlichting dient te worden vervangen met zo min mogelijk onveiligheid en overlast voor alle partijen.	1 - Tunnelbuis volledig afsluiten tot alle werkzaamheden zijn voltooid. 2 - Tunnel wordt tijdelijk (deels) afgesloten, waarbij met een parallelle ombouw in verschillende fases de nieuwe installaties parallel aan de oude worden aangebracht. Na aanbrengen van nieuwe installaties worden de oude verwijderd.	1 - Tunnelbuis volledig afsluiten tot alle werkzaamheden zijn voltooid.	Nee											
4	Contractvoorbereiding	Technisch manager	Arbeidsveiligheid, verkeersveiligheid: Verlichting dient te worden vervangen met zo min mogelijk onveiligheid en overlast voor alle partijen.	1 - Afsluitingen alleen in nachten 2 - Afsluitingen alleen in weekenden 3 - Langdurige afsluiting per verkeersbuis 4 - Langdurige afsluiting per rijrichting 5 - Vierkante afsluiting	3 - Langdurige afsluiting per verkeersbuis	Nee	In een periode van 1 week kunnen de werkzaamheden in principe worden uitgevoerd. Het kost wel wat meer beschikbaarheid overdag tov de andere opties, maar het object hoeft niet steeds opnieuw buiten dienst te worden gesteld. Het buiten dienst stellen is op zichzelf al een risicovolle activiteit, door de benodigde plaatsing van verkeersmaatregelen. Deze activiteit wordt met deze keuze beperkt. 1,2 zorgen voor langere doorlooptijd door inefficientiedoor parallel moeten ombouwen. Daarnaast zorgen de vele verkeersmaatregelen voor hogere kosten. 4,5 zorgen voor teveel overlast voor de weggebruikers.	De neiging kan bestaan om de buitenbedrijfstelling te gebruiken om vele activiteiten in die periode te plannen. Dit veroorzaakt samenlooprisico's.	34	Er kan veel tijdsdruk komen te staan op het uitvoeren van de werkzaamheden in die ene week.	35	Tijdens de week afsluiting vindt veel sluipverkeer plaats op het onderliggende wegennet.	n.v.t.		
5	Contractvoorbereiding	Technisch manager	Arbeidsveiligheid: Werkzaamheden aan de tunnel dienen plaats te vinden in de tunnelzuilen waarbij werken in het verkeer gevaarlijke situaties kan opleveren.	1 - Werkzaamheden vinden plaats in het verkeer. 2 - Werkzaamheden vinden niet plaats in het verkeer.	2 - Keuze is om werkzaamheden niet in het verkeer te laten plaatsvinden. Dit betekent dat minimaal één tunnelbuis wordt afgesloten bij werkzaamheden aan die tunnelbuis. Voorbereidende werkzaamheden waar geen buis of rijstrookafsluiting voor nodig is kunnen wel worden uitgevoerd wanneer verkeer rijdt door de tunnel.	Nee	Arbeidsrisico's ten aanzien van werken in het verkeer worden met deze keuze afgedekt gemitigeerd. Bij een mogelijke keuze om hulpdiensten via het werkvak te laten rijden dienen aanvullende maatregelen te worden getroffen om deze voertuigen en medewerkers afdoende te separeren. Bij afsluiting van tunnel(buis) worden wel extra risico's geintroduceerd ten aanzien van de verkeersveiligheid op omleidingsroutes. Dit risico wordt hieronder uitgewerkt.									
6	Contractvoorbereiding	Technisch manager	Verkeersveiligheid, omgevingsveiligheid, arbeidsveiligheid, brandveiligheid Verkeersbuis Oost 1: Algehele sluiting van de verkeersbuis levert een stremming op voor de hulpdiensten en bussen die van de tunnel gebruik maken.	1 - Bussen en hulpdiensten maken gebruik van de lokale omleidingsroute. 2 - Bussen en hulpdiensten maken gebruik van het dienstvak in de tunnel. 3 - Alleen Prio 1 hulpdiensten maken gebruik van de tunnel. 4 - Hulpdiensten en bussen kunnen geen gebruik maken van de gesloten tunnelbuis	3 - Hulpdiensten worden verzocht om door de verkeersbuizen te gaan welke gesperd zijn. In het uitzonderlijke geval dat de het niet mogelijk is om door de andere buis te gaan, zouden Prio 1 hulpdiensten door de afgesloten tunnelbuis gaan, overige gaat via omleidingsroutes.	Ja	Als prio 1 hulpdiensten gebruik maken van het werkvak in de tunnel ontstaat het risico van aanrijdgevaar van medewerkers. Tevens worden andere gevaren geintroduceerd, zoals vallende materialen op hulpvoertuigen in het werkvak. - begeleiding van hulpdiensten door het werkvak is dringend gewenst; - tijdige communicatie met werknemers in de tunnel is essentieel;	Als prio 1 hulpdiensten gebruik maken van het werkvak in de tunnel ontstaat het risico van aanrijdgevaar van medewerkers. Tevens worden andere gevaren geintroduceerd, zoals vallende materialen op hulpvoertuigen in het werkvak.	36							
7	Contractvoorbereiding		Verkeersveiligheid, omgevingsveiligheid, arbeidsveiligheid, brandveiligheid Verkeersbuis Oost 2: Algehele sluiting van de verkeersbuis levert een stremming op voor de hulpdiensten en bussen die van de tunnel gebruik maken.	1 - Bussen en hulpdiensten maken gebruik van de lokale omleidingsroute. 2 - Bussen en hulpdiensten maken gebruik van het dienstvak in de tunnel. 3 - Alleen Prio 1 hulpdiensten maken gebruik van de tunnel. 4 - Hulpdiensten en bussen kunnen geen gebruik maken van de gesloten tunnelbuis	4 - Hulpdiensten en bussen kunnen geen gebruik maken van de afgesloten tunnelbuis. Hulpdiensten en bussen kunnen via de doorsteek van Oost 2 naar de verkeerbuis Oost 1.	Ja	Vanwege de werkzaamheden in de verkeersbuis is er weinig ruimte beschikbaar. Hoogwerkers en opgestelde materialen zorgen ervoor dat de er onvoldoende ruimte is om de buis te passeren. Daarbij het risico dat door kleine materialen schade gereden kan worden.									
8	Contractvoorbereiding		Verkeersveiligheid, omgevingsveiligheid, arbeidsveiligheid, brandveiligheid Verkeersbuis West 1: Algehele sluiting van de verkeersbuis levert een stremming op voor de hulpdiensten en bussen die van de tunnel gebruik maken.	1 - Bussen en hulpdiensten maken gebruik van de lokale omleidingsroute. 2 - Bussen en hulpdiensten maken gebruik van het dienstvak in de tunnel. 3 - Alleen Prio 1 hulpdiensten maken gebruik van de tunnel. 4 - Hulpdiensten en bussen kunnen geen gebruik maken van de gesloten tunnelbuis	3 - Hulpdiensten worden verzocht om door de verkeersbuizen te gaan welke gesperd zijn. In het uitzonderlijke geval dat de het niet mogelijk is om door de andere buis te gaan, zouden Prio 1 hulpdiensten door de afgesloten tunnelbuis gaan, overige gaat via omleidingsroutes.	Ja	Als prio 1 hulpdiensten gebruik maken van het werkvak in de tunnel ontstaat het risico van aanrijdgevaar van medewerkers. Tevens worden andere gevaren geintroduceerd, zoals vallende materialen op hulpvoertuigen in het werkvak. - begeleiding van hulpdiensten door het werkvak is dringend gewenst; - tijdige communicatie met werknemers in de tunnel is essentieel;	Als prio 1 hulpdiensten gebruik maken van het werkvak in de tunnel ontstaat het risico van aanrijdgevaar van medewerkers. Tevens worden andere gevaren geintroduceerd, zoals vallende materialen op hulpvoertuigen in het werkvak.	36							
9	Contractvoorbereiding		Verkeersveiligheid, omgevingsveiligheid, arbeidsveiligheid, brandveiligheid Verkeersbuis West 2: Algehele sluiting van de verkeersbuis levert een stremming op voor de hulpdiensten en bussen die van de tunnel gebruik maken.	1 - Bussen en hulpdiensten maken gebruik van de lokale omleidingsroute . 2 - Bussen en hulpdiensten maken gebruik van het dienstvak in de tunnel. 3 - Alleen Prio 1 hulpdiensten maken gebruik van de tunnel. 4 - Hulpdiensten en bussen kunnen geen gebruik maken van de gesloten tunnelbuis	4 - Hulpdiensten en bussen kunnen geen gebruik maken van de afgesloten tunnelbuis. Hulpdiensten en bussen kunnen via de doorsteek van Oost 2 naar de verkeerbuis Oost 1.	Ja	Vanwege de werkzaamheden in de verkeersbuis is er weinig ruimte beschikbaar. Hoogwerkers en opgestelde materialen zorgen ervoor dat de er onvoldoende ruimte is om de buis te passeren. Daarbij het risico dat door kleine materialen schade gereden kan worden.									
10	Contractvoorbereiding		Verkeersveiligheid, arbeidsveiligheid: Bij afscherming van de afgesloten wegen kunnen in specifieke gevallen auto's (al dan niet met opzet) door de afzetting glippen. Hierdoor ontstaan risico's als aanrijdgevaar, maar ook vastrijden en belemmering van hulpdiensten en werkverkeer.	1 - Alle afzettingen volledig dichtzetten met een fysieke afscheiding, waarbij bereikbaarheid van het werkgebied door hulpdiensten naar het werkvak wordt belemmerd. Hulpdiensten prio 1 mag niet worden belemmerd. 2 - Afzettingen met sluiswerking waardoor hulpdiensten nog relatief makkelijk naar het afgesloten gebied kunnen. Hierbij ontstaat de mogelijkheid voor derden om deze afsluitingen (bedoeld of onbedoeld) te passeren.	1 - Onder voorwaarde dat er een veilige doorgang wordt georganiseerd. Bijvoorbeeld door Prio-1 ritten te begeleiden door de tunnel.	Ja	Uit ervaringen met andere wegafsluitingen blijkt dat derden weinig ruimte nodig hebben om toch bedoeld of onbedoeld in een afgeschermd gebied terecht te komen. Om risico's op aanrijdgevaar en belemmeringen van noodroutes te voorkomen dienen afzettingen volledig te zijn afgeschermd. Als hulpdiensten door de tunnel worden gekid kan mogelijk een vrije toegang voor hulpdiensten worden gecreëerd via de dienstweg; hulpdiensten worden dan al in een eerder stadium gesplitst van de reguliere weggebruikers.									
11	Contractvoorbereiding		Tunnelveiligheid, arbeidsveiligheid: er dient altijd een vrije vluchtweg te zijn,	1 - Vluchtweg is onderbroken en niet doorgaand van ene naar andere zijde van de tunnelingangen. 2 - Vluchtweg is doorgaand van het ene naar het andere tunneleinde.	De vluchtweg in het midden tunnel kanaal dient gegarandeerd te worden.Voorbereidende werkzaamheden kunnen uitgevoerd worden met de afspraak dat er alleen materiaal in de vluchtgang gebracht mag worden dat op dezelfde dag wordt verwerkt. Bij een calamiteit dient de vluchtweg zo snel mogelijk vrij gemaakt worden.	Ja	Aangezien tijdens de aanpassing van de verlichtring in één buis de andere buis in gebruik ik dient een vluchtweg gebongd te zijn..									
12	Contractvoorbereiding		Constructieve veiligheid: van diverse constructieve elementen is nog niet duidelijk of er gebreken zijn, en wat de sterkte van de materialen zijn. De volgende zaken zijn benoemd: - loskomende tegels in de tunnelwand; - (hangende) TTI aan het plafond/wand kunnen vallen; - gewijzigd gebruik van ruimtes; - spanngen (voor nissen en leidingen) worden aangebracht in de dragende constructie.	Genoemde risico's dienen nader te worden onderzocht.	Nader te bepalen. Met genoemde belemmeringen rekening houden in ontwerpproces.	Ja	Nader uit te werken. Enkele genoemde risico's kunnen (deels) worden beheerst door gebruik van de juiste werkmethodes en toepassing van een gedegen risicoanalyse. Verdere uitwerking van risico's en maatregelen is noodzakelijk.									
13	Contractvoorbereiding		Brandveiligheid uitvoeringsfase: elektrisch voertuig raakt in de tunnel in brand.	1 - Wel elektrisch materieel of voertuigen toestaan. 2 - Geen elektrisch materieel of voertuigen toestaan; 3 - Materieelkeuze onder voorwaarden bij de opdrachtnemer laten.	3 - Materieelkeuze is onder voorwaarden te kiezen door de opdrachtnemer. Zie contracteisen over materiaal/materieel: - mobiel materieel zoals hoogwerkers bij voorkeur elektrisch; - dieseltractie is niet verboden, maar stationair materieel dient buiten de tunnel te worden gepositioneerd; - indien materieel in de tunnel niet in elektrische vorm kan worden ingezet, dan in elk geval euro 5 motor en roetfilters voorschrijven, conform wet- en regelgeving; - laden buiten tunnel.	Ja	Overwegingen zijn: - e-voertuigen zijn brandgevaarlijker, met name bij opladen; - e-voertuigen zijn moeilijker te blussen; - e-voertuigen hebben geen schadelijke uitstoot; - e-voertuigen zijn stiller, arbeidsrisico: je hoort ze minder snel aankomen; - e-voertuigen maken minder geluid dan brandstofvoertuigen; - voertuigen op brandstof (diesel): dieseldampen zijn kankerverwekkend; - voertuigen op LPG niet toestaan: gas verzamelt zich op het laagste punt, is explosief en brandgevaarlijk.	Onvoldoende capaciteit netwerkspanning.	n.v.t.							
14	Contractvoorbereiding		Elektrische veiligheid uitvoeringsfase: Kortsluiting, diverse risico's: in dienstgang aan het werk met veel apparatuur, kabels, etc Bij vallen, uitschieten, verkeerde keuze maken is dit een risico. Kennis van het areaal is een issue: onbekende kabels, wat is in gebruik en wat niet? In het gehele werkgebied is sprake van onbekende en niet gemarkeerde K&L. Er is tevens geen schone werkomgeving. Er zijn niet altijd alle ontwerpgegevens voorhanden, zoals bij diverse e-kasten. Soms is er sprake van geknutselde connecties. Sommige leidingen buiten gebruik zijn niet spanningsloos, en aanraakveilig, staat	Bepalen hoe veilig te werken bij onbekende risico's?	n.v.t.	Ja	De meest risico's zijn naar verwachting gedekt in de bedrijfs-RI&E van de opdrachtnemer en werkwijzen zijn in principe gebongd in de betreffende normen, zoals NEN3140. Aandacht voor deze risico's in de uitvoering is echter nodig: spanningsloos werken in parallelle werkzaamheden is vrijwel onmogelijk. Deze risico's dienen te worden meegenomen in de fasering en in het ontwerp, en restrisico's dienen te worden opgenomen in de ontwerp-RI&E.CN dient de nieuwe situatie nauwkeurig vast te leggen, inclusief een goede overdracht naar de nieuwe opdrachtnemer voor beheer en onderhoud. Maar ook tijdelijke K&L en tijdelijke installaties, zoals verlichting tijdens de bouwfase dienen goed te worden geïnstalleerd en gedocumenteerd. Hiervoor eisen formuleren in het contract.									
15	Contractvoorbereiding		Voor leggen/aanpassen van K&L en plaatsing e-kasten en installatie(-delen) dient langs de weg te worden gewerkt, ook buiten de tunnel. Werk vindt grotendeels plaats achter de barrier.	1 -Rijbanen of weg tijdens werkzaamheden direct naast de weg afsluiten. 2 - Geen afsluiting.	Keuze nader te bepalen. Voorkeur heeft keuze 2, geen aparte afsluiting voor K&L, maar onder voorwaarden.	Ja	Uitgangspunt blijft dat het werk fysiek gescheiden is van het verkeer. Verleggen van Kabels en Leidingen indien mogelijk samen laten vallen met de afsluiting. Indien niet mogelijk kan het zonder wegafsluiting mits de werkzaamheden het verkeer niet storen of afleiden, of dit anderszins tot onveilige situaties leidt. Hiervoor moet wel dezelfde procedure worden doorlopen als of het een afsluiting betreft. Werkzaamheden langs de snelweg kunnen van invloed zijn op weggedrag door afleiding. Werken langs niet afgesloten snelweg levert blootstelling op aan uitlaatgassen/fijnstof/geluid. Vallende materialen kunnen een gevaar vormen voor de verkeersveiligheid. Alternatief voor afsluiting kan zijn om een snelheidsbeperking opleggen. Gedeeltelijke en gehele afsluiting met omleidingen leveren extra risico's op voor de verkeersveiligheid zie eerder genoemde risico's verkeersveiligheid.									

Rijkswaterstaat
Ministerie van Infrastructuur en Waterstaat

NAAR TOELICHTING

BTO-keuzes

Nr.	Projectfase	Bron	Stap 1: Situatie omschrijving	Stap 2: Dilemma	Stap 3: Keuze		Stap 4: Motivering	Stap 5: Gevolg									
								Omschrijf de gevolgrisico's (de gevolgen van de keuze)									
	De projectfase waarin de BTO-keuze gemaakt is.	De herkomst van de BTO-keuze.	Omschrijf de situatie waarover een keuze gemaakt moet worden.	Omschrijf de keuze mogelijkheden.	Omschrijf welke keuze is gemaakt.	in IVP	Omschrijf de afwegingen die tot de betreffende keuze hebben geleid	Gevolgrisico 1	Risico nummer Ontwerp RIE	Gevolgrisico 2	Risico nummer Ontwerp RIE	Gevolgrisico 3	Risico nummer Ontwerp RIE	Gevolgrisico 4	Risico nummer Ontwerp RIE	Gevolgrisico 5	Risico nummer Ontwerp RIE
16	Contractvoorbereiding		Bij een strakke planning en fasering is er sprake van gelijktijdigheid van veel verschillende werkzaamheden, hierdoor word elk risico (bijvoorbeeld bekneling aanrijdgevaar) versterkt. Denk bijvoorbeeld aan stofvorming, geluid en verschil in werkinstructies.	1 - Strak plannen zodat veel werk gelijktijdig plaatsvindt. 2 - Ruim plannen zodat werkzaamheden na elkaar kunnen plaatsvinden.	Keuze is nader te bepalen. Voorkeur gaat naar keuze 2 : zo min mogelijk werkzaamheden gelijktijdig laten plaatsvinden.	Ja	In basis zijn de ombouw slots bedoeld voor het vervangen van de verlichting. Indien door andere partijen werkzaamheden uitgevoerd moeten worden dan dienen deze op elkaar afgestemd te worden. De werkzaamheden van andere partijen mogen de werkzaamheden van de verlichting niet nadelig beinvloeden. Door verschillende werkzaamheden zoveel mogelijk te scheiden worden risicoversterkingen onder invloed van gelijktijdigheid voorkomen. Mensen lopen elkaar niet in de weg, werkzaamheden overlappen en beinvloeden elkaar niet en er zijn minder vervoersbewegingen in de buis. De beschikbare werkruimte neemt toe (en ruimte voor ontruiming of hulpdiensten). Bij werkzaamheden tegelijkertijd in een										
17	Contractvoorbereiding		Bestaande kabels hergebruiken in voor de nieuwe verlichtingsinstallatie	1 - Bestaande kabels mogen worden hergebruikt 2 - Bestaande kabels mogen niet worden hergebruikt	2 - Bestaande kabels mogen niet worden hergebruikt	Nee	De huidige kabels voldoen niet aan de vigerende brandklasses. De huidige kabels zijn momenteel 20-30 jaar in gebruik. Dit houdt in dat de restlevensduur van deze kabels beperkt is. Het is de bedoeling dat de verlichting na uitvoering ca. 20 jaar in gebruik is. Kabels welke vrijkomen uit de huidige installatie moeten uit het object worden gehaald. Bij het verwijderen van de kabels kunnen beschadigingen ontstaan. Gevolg voor kortsluiting en of brand.										
18	Contractvoorbereiding		Voldoen aan de tunnelstandaard	1 - Verlichting vervangen waarbij voldaan wordt aan de tijdens contractvoorbereiding vigerende tunnelstandaard 2 - Verlichting vervangen waarbij niet wordt voldaan aan de tunnelstandaard	1 - De nieuw te realiseren verlichting dient te voldoen aan de vigerende tunnelstandaard	Nee	Hoewel de Schipholtunnel nog niet voldoet aan de tunnelstandaard wordt de verlichting aangepast vooruitlopend op de V&R waarbij de tunnel naar LTS niveau gebracht gaat worden. De verlichting wordt in de V&R niet meer aangepast en moet dus op LTS niveau gebracht/voorbereid zijn.										
19	Contractvoorbereiding		Teveel mensen in de tunnels levert extra risico's op tijdens de uitvoering.	Geen dilemma.	Alle personen die niet direct betrokken zijn bij de uitvoering van de werkzaamheden weren van de werklocatie. opdrachtnemer dient toegangsregime in te stellen.	Ja	Teveel personen in de tunnel heeft direct invloed op de veiligheid. Hoe minder personen aanwezig hoe veiliger gewerkt kan worden.										
20	Contractvoorbereiding		Sociale veiligheid: verkeersregelaars bij omleidingen en afsluitingen krijgen te maken met agressie en geweld. Wat doen we hiermee (ervaring Heinenoord). Welke mogelijke maatregelen, wat geven we mee aan opdrachtnemer?	1 - inzet verkeersregelaars. 2 - inzet harde afscherming/afzetting.	Voorkeur keuze 2 vanuit veiligheid: harde maatregel zoals bijvoorbeeld vierkant omhekken. Nog nader uit te werken door ON.	Ja	Afwegingen: Keuze 1: Verkeersregelaars, geen "alleen werk": dit is geen (volledige) garantie dat er geen geweld of agressie plaatsvindt. Keuze 2: harde afscherming/ vierkant omhekken: problematisch voor hulpdiensten. Alternatief tijdelijke verkeersdrempels/busslus. Uitwerking van deze keuzen wordt door RWS nader bepaald.										
21	Contractvoorbereiding		Integrale beveiliging: Betreding van de tunnel en bijbehorende gebouwen door ontbevoegden. Zowel bij ontwerp als bij uitvoering rekening houden met: databeveiliging, pasjessysteem toepassen bij ruimtes waar tunnelsystemen staan.	Risico's/maatregelen nader te bepalen.	Door ON nader uit te werken. Hierbij moet aandacht zijn voor de toegangsregeling en aandacht voor het sluiten van deuren ter voorkoming van voor betreding door onbevoegden.	Ja	De opdrachtnemer dient aan te geven hoe hij de integrale beveiliging in de praktijk gaat regelen.										
22	Contractvoorbereiding		Bij uitvoering bij kabeldoorvoeren door tunnel kan de brandcompartimentering (deels) wegvallen. Brand kan hierdoor verder doorgaan dan nodig.	Door werkzaamheden in de tunnel wordt de brandcompartimentering onderbroken.	Dit risico dient te worden meegenomen in de fasering van de uitvoering. De opdrachtnemer dient hiervoor maatregelen te treffen.	Ja	Defecten in de compartimentering dienen zo snel mogelijk hersteld te worden volgens de daarvoor geldende werkwijze. Meestal zal dit gaan om het brandwerend afdichten van kabeldoorvoeringen.										
23	Contractvoorbereiding		Voor het aanbrengen van kabels vanuit de vluchtgang naar de verkeersbuizen zijn nieuwe sparingen benodigd	1 - Sparingen mogen, indien door de ON gegarandeerd kan worden dat dit veilig gedaan kan worden voor het wegverkeer, worden uitgevoerd worden wanneer verkeer rijd door de tunnel. 2 - Sparingen mogen niet buiten de ombouwslots worden gerealiseerd.	2 - Sparingen migen niet buiten de ombouwslots worden gerealiseerd	Ja	De ruimte vanaf de wand tot de rijstrook is beperkt. De kans dat door het boren afspattingen of onderdelen op het wegdek komen zorgt dat de veiligheid voor de weggebruiker in het geding komt.										
24	Contractvoorbereiding	BTO sessie 25-03-2025	Levensduur van de nieuw te realiseren verlichtingsinstallatie.	1 - De verlichting dient een levensduur te hebben van minimaal de levensduureisen uit de Landelijke Tunne Standaard. 2 - De verlichting wordt tijdens de V&R vervangen.	1 - De verlichting dient een levensduur te hebben van minimaal de levensduureisen uit de Landelijke Tunne Standaard.	Nee	Opdrachtenemer dient de instalatie zo te ontwerpen dat met minimaal onderhoud (excl reinigen) de verlichting een levensduur heeft van richting de 20 jaar.										
25	Contractvoorbereiding	BTO sessie 25-03-2025	Omgaan met vrijkomende materialen uit de tunnel.	1 - Direct afvoeren uit tunnel 2 - Demonteren, schoonmnaken in tunnel overeenkomstig LRT	1 - Vrijkomende materialen na demonteren direct afvoeren uit de tunnel.	Ja	Hergebruik van de verlichting wordt niet geacht. Om de werkplek zo schoon mogelijkm te houden en daarmee risico's te mitrigeren dienen de vrijkomende materialen zo snel mogelijk uit de verkeersbuis verwijderd te worden.										
26	Contractvoorbereiding	BTO sessie 25-03-2025	Werklocatie en logistiek i.r.t. terrein schiphol. Ten behoeve van de werkzaamheden zal de ON bij het project keten en opslagruimte nodig hebben.	1 - gebruik maken van dienstgebouwen en dienstterrein Dienstgebouw Noord West. Toegangsregime afstemmen met Schiphol. 2 - Alles in verkeersbuis/werkvak, zodat het aantal personen en voertuigen op het terrein van Schiphol wordt geminimaliseerd	2 - Alles in verkeersbuis/werkvak of extern, zodat het aantal personen en voertuigen op het terrein van Schiphol wordt geminimaliseerd	Ja	De dienstgebouwen staan op grondgebied van Schiphol.										
27	Contractvoorbereiding	Veiligheidscoordinator	Onderhoudbaarheid van systeemonderdelen	1 - Actieve apparatuur dient zoveel mogelijk buiten de verkeersbuis te worden ondergebracht. 2 - Geen belemmering vanuit OG meegegeven	1 - Actieve apparatuur dient zoveel mogelijk buiten de verkeersbuis te worden ondergebracht.	Nee	De actieve apparatuur (regelcomponenten en drivers) kunnen hiermee zonder afsluitingen worden vervangen. Hiermee kunnen problemen sneller worden opgelost en is het veiliger. De onderhoudbaarheid van de onderdelen in de verkeersbuis beperkt zicht dan hoofdzakelijk tot het reinigen van de armaturen.										
28																	
29																	
30																	
31																	
32																	

Rijkswaterstaat
Ministerie van Infrastructuur en Waterstaat

NAAR TOELICHTING

BTO-keuzes

Nr.	Projectfase	Bron	Stap 1: Situatie omschrijving	Stap 2: Dilemma	Stap 3: Keuze		Stap 4: Motivering	Stap 5: Gevolg									
								Omschrijf de gevolgrisico's (de gevolgen van de keuze)									
	De projectfase waarin de BTO-keuze gemaakt is.	De herkomst van de BTO-keuze.	Omschrijf de situatie waarover een keuze gemaakt moet worden.	Omschrijf de keuze mogelijkheden.	Omschrijf welke keuze is gemaakt.	in IVP	Omschrijf de afwegingen die tot de betreffende keuze hebben geleid	Gevolgrisico 1	Risico nummer Ontwerp RIE	Gevolgrisico 2	Risico nummer Ontwerp RIE	Gevolgrisico 3	Risico nummer Ontwerp RIE	Gevolgrisico 4	Risico nummer Ontwerp RIE	Gevolgrisico 5	Risico nummer Ontwerp RIE
33																	
34																	
35																	

Bijlage D Calamiteitenbestrijdingsplan RWS WNN 2024

De opdrachtnemer van deze overeenkomst is niet de calamiteitenaannemer zoals benoemd in het Calamiteitenbestrijdingsplan. De calamiteitenaannemer blijft de opdrachtnemer van het onderhoudscontract.

Rijkswaterstaat
Ministerie van Infrastructuur en Waterstaat



Rijkswaterstaat West-Nederland Noord

Calamiteitenbestrijdingsplan

Wijkertunnel
Velsertunnel
Zeeburgertunnel
Schipholtunnel
Coentunnel
Gaasperdammertunnel

Inhoudsopgave VBP DEEL CBP

Rijkswaterstaat bedrijfsinformatie

Rijkswaterstaat
Ministerie van Infrastructuur en Waterstaat

De VBP-documenten zijn om redenen van beheersbaarheid ingedeeld in tunnelspecifieke documenten en generieke documenten die voor alle tunnels gelden. De specifieke documenten zijn per tunnel verzameld achter numerieke tabs. De generieke documenten zijn verzameld achter alfabetische tabs.

Belangrijkste wijzigingen ten opzichte van vorige versie
- Wijzigingen t.o.v. vorige versie in blauw
- Nieuw CBP

	GENERIEKE DOCUMENTEN RWS WNN	
A	Calamiteitenbestrijdingsplan wegtunnels RWS WNN	
A-00-a	Voorblad CBP WNN	Nvt
A-00-b	CBP WNN Tekenlijst en verspreiding	30 september 2024
A-01	CBP WNN Deel I Inleiding en algemeen	30 september 2024
A-02	CBP WNN Deel II Calamiteiten en incidentscenario's	30 september 2024
A-03	CBP WNN Deel III Procedures Rijkswaterstaat	30 september 2024
A-04	CBP WNN Deel IV Afspraken hulpverlening	30 september 2024
A-05	CBP WNN Deel V Afkortingenlijst	30 september 2024
A-06	CBP RWS WNN Beslis- en bevoegdhedenschema	30 september 2024
A-11	Bijlage 11 RWS WNN tunnelsyst ondersteuning incidentafhandeling	30 september 2024
A-12	Bijlage 12 Formulier bommelding	5 september 2019
A-14	Bijlage 14 CBP WNN overzicht omroepberichten	30 september 2024
	Bijlagen NB Instructiekaarten worden beheerd door VWM landelijk https://corporate.intranet.rws.nl/projecten/overig/oto_wegtunnels/	
A-17	Bijlage 17 Checklist schouwen VWM versie 1 (voor WIS en OVD-RWS)	n.v.t.
A21a	Bijlage Brandmeld en inbraakproces VT, ZT, ST 1.7	16 november 2023
A21b	Bijlage Brandmeldproces WT, CT en GDT 1.0	16 november 2023
A-22	Proces bediening waterleiding WRK waternet Velsertunnel	28 november 2023
A-32	Bijlage CBP WNN Blusgasinstructie Wijkertunnel	8 maart 2013
A-62	Bijlage CBP WNN Blusgasinstructie Coentunnel	6 april 2014
	Bijlagen referentiekaarten NB Referentiekaarten worden beheerd door VWM landelijk https://corporate.intranet.rws.nl/projecten/overig/oto_wegtunnels/	

Calamiteiten-bestrijdingsplan Wegtunnels Rijkswaterstaat West-Nederland Noord

Rijkswaterstaat
Ministerie van Infrastructuur en Waterstaat

Tekenlijst ter vaststelling / accordering en verspreiding

Vaststelling

Akkoordverklaring	Afdelingshoofd district Zuid	Namens deze: R. Puggioni	Akkoord verklaard op: 29 juli 2024	Paraaf 
Vaststelling	Tunnelbeheerder	Namens deze N.S. Bagchus-Winkel	Vastgesteld op datum:	Paraaf:

Gemandateerd voor tussentijdse wijzigingen in Calamiteitenbestrijdingsplan Rijkswaterstaat West-Nederland Noord

RWS West-Nederland Noord	RWS West-Nederland Noord, district Zuid	Tunnelbeheer Organisatie (TBO): Taakverantwoordelijke CBP

Verspreiding

Ontsluiting
De documenten welke betrekking hebben op calamiteitenbestrijding in tunnels van RWS West-Nederland Noord worden digitaal ter beschikking gesteld aan alle betrokken partijen binnen RWS. Buiten RWS wordt het CBP op verzoek digitaal beschikbaar gesteld (zie verspreidingslijst).

Verspreiding nieuwe versies
Verspreiding van nieuwe versies van (delen van) het calamiteitenbestrijdingsplan is de verantwoordelijkheid van diegenen die de digitale versie ontvangen. Men is zelf verantwoordelijk voor het afwegen van nut en noodzaak.

Leidende versies
De digitale versies zoals beheerd door de Tunnelbeheer Organisatie (TBO) van RWS West-Nederland Noord.

Calamiteiten-bestrijdingsplan Wegtunnels Rijkswaterstaat West-Nederland Noord

Rijkswaterstaat
Ministerie van Infrastructuur en Waterstaat

Verspreidingslijst (digitaal)

In de lijst hieronder staan diegenen vermeld die in ieder geval een digitale versie ontvangen.

Dit CBP is toegezonden aan:	*Afdeling*	*Ter attentie van:*	*Digitaal (D)*	*Alle wijzigingen (A) of bij periodieke integrale vaststelling (P)*
RWS Verkeer- en Watermanagement	Verkeerscentrale Noordwest Nederland (VCNWN) wegverkeers-leiding)	Beheerder VCNWN Infosite R. Bruijns H. Mooij Hoofd verkeercentrale P. Post	D	A
RWS Verkeer- en Watermanagement	Directie Wegverkeer-management Afd. Operationeel Verkeer Randstad	Beheerder Intranetsite VWM-Noord R. DirksHoofd OVM randstad R. Stegman	D	A
Veiligheidsbeambte Rijkstunnels	Bureau Veiligheidsbeambte	Veiligheidsbeambte B. Janssen	D	P
RWS Verkeer- en Watermanagement	Directie Bedrijfsvoering, Communicatie en Crisiscoördinatie, Afdeling Crisismanagement	Accountmanager Crisisbeheersing L. Bradley	D	A
Omgevingsdienst Noordzeekanaalgebied	Toezicht en handhaving	Afdelingshoofd A. Noort	D	P
Brandweer Kennemerland		R. Joustra	D	
GGD/GHOR Kennemerland		M. Eggink	D	
Meldkamer Noord-Holland		M. Zwart	D	
Politie eenheid Noord-Holland		B. Wiegers	D	
Brandweer Amsterdam-Amstelland		R. Galesloot	D	
Meldkamer/DROC Amsterdam-Amstelland		P. Brasik	D	
Ambulance Amsterdam		P. Heymeijer	D	
Politie eenheid Amsterdam		P. Stoffels	D	

Calamiteitenbestrijdingsplan

(CBP) Wegtunnels

Rijkswaterstaat

West-Nederland Noord

Rijkswaterstaat
Ministerie van Infrastructuur en Waterstaat

Deel I Inleiding en algemene informatie

Dit CBP bevat operationele afspraken tussen RWS West-Nederland Noord, de Veiligheidsregio's Amsterdam-Amstelland en Kennemerland en de regionale politie-eenheden Amsterdam en Noord-Holland van de Nationale Politie over de (gezamenlijke) inzet bij incidenten in tunnels.
Deel I bevat het doel van het CBP, de wettelijke grondslag, de samenhang met andere plannen en de kwaliteitsborging.

Beheersgebied

Per tunnel is het beheersgebied grofweg ingedeeld volgens onderstaande tabel:

		Beheersgebied	
Tunnel:	Wegnummer:	Van km:	Tot km:
Velsertunnel	A22	11,1	13,0
Wijkertunnel	A9	50,9	52,5
Schipholtunnel	A4	6,6	7,7
Coentunnel Westbuizen	A10	29,2	31,1
Coentunnel Oostbuizen	A10	29,3	31,6
Zeeburgertunnel	A10	7,8	9,4
Gaasperdammertunnel	A9	10,2	7,2

Doelgroep

De operationele medewerkers van:
1. RWS Verkeer- en Watermanagement (VWM), te weten:
   a. de (coördinerend) wegverkeersleiders bij de Verkeerscentrale Noordwest Nederland (VCNWN);
   b. de weginspecteurs en Officieren van Dienst-Rijkswaterstaat bij Operationeel Verkeer Randstad;
2. de hulpverleningsdiensten.

Werkinstructies

De procedures van RWS zijn opgenomen in de vorm van instructiekaarten. De procedures in de instructiekaarten zijn afgestemd op de bedrijfsprocessen van RWS en met de inzetprocedures van de hulpverleningsdiensten.

1. Wettelijke grondslag

Warvw

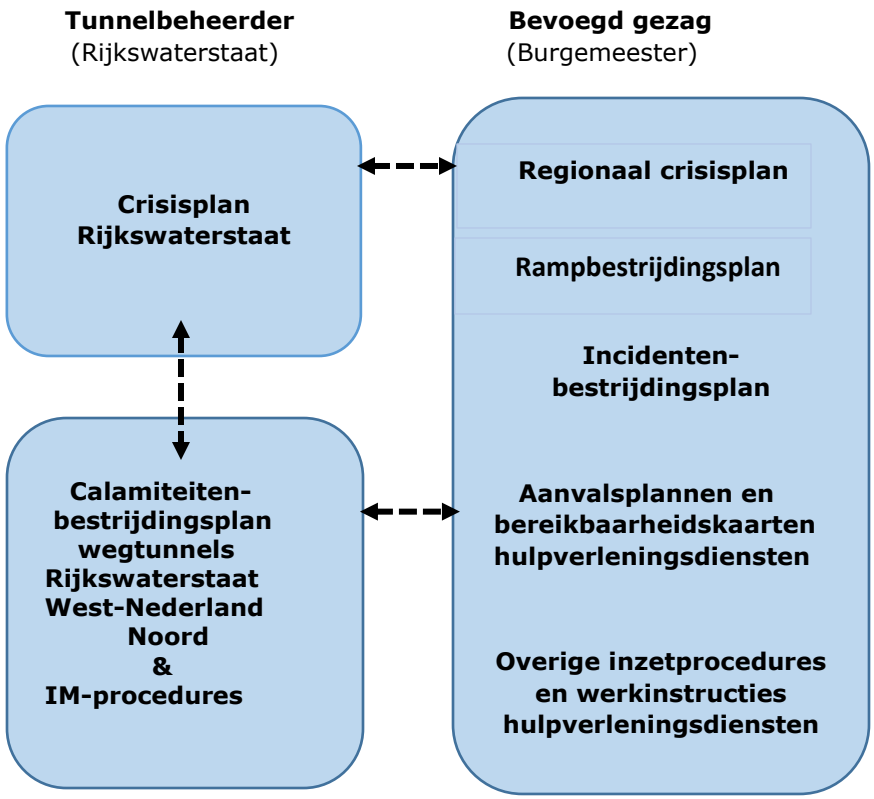
Het CBP is een wettelijk voorgeschreven plan. Het CBP bevat afspraken tussen de tunnelbeheerder van RWS, de Veiligheidsregio's en de politie-eenheden. Het plan is afgestemd op de planvorming (procedures en bereikbaarheidskaarten) van de hulpverleningsdiensten.

Rarvw

De Regeling aanvullende regels veiligheid wegtunnels (Rarvw) bevat regels met betrekking tot de inhoud van het Veiligheidsbeheerplan (VBP). Het CBP is een zelfstandig onderdeel van het VBP. Dit houdt in dat het CBP in principe los van het VBP kan worden geëvalueerd en geactualiseerd.

3. Samenhang met andere plannen

De samenhang tussen het CBP en andere plannen bij RWS en de binnen de Veiligheidsregio's Amsterdam-Amstelland en Kennemerland samenwerkende hulpverleningsdiensten is hieronder weergegeven.



Samenhang plannen. Het Crisisplan Rijkswaterstaat is een generiek plan. Dit plan beschrijft de structuur van de crisisorganisatie van RWS en geeft weer hoe de crisisorganisatie werkt tijdens opschaling. De crisisorganisatie van Rijkswaterstaat kent in het crisisplan drie opschalingsniveaus: fase 1, fase 2 en fase 3.
Het CBP is een onderliggend plan van het Crisisplan Rijkswaterstaat waarop dus ook de in het crisisplan benoemde coördinatieniveaus van toepassing zijn.

Als basis voor het CBP zijn de Bedrijfsprocessen (UPP) RWS Tunnelsysteem (onderdeel van de landelijke Tunnelstandaard van RWS) van toepassing.

In het Regionaal Crisisplan is de multidisciplinaire calamiteitenorganisatie van de veiligheidsregio beschreven.
De brandweer heeft voor de tunnels aanvalsplannen waarin de bereikbaarheid en de inzetprocedures zijn vastgelegd.
De Veiligheidsregio Amsterdam-Amstelland (VRAA) beschikt daarnaast over het Calamiteitenplan wegtunnelincidenten. Dit is een generiek plan voor alle wegtunnels in Amsterdam-Amstelland. In dit plan is de
verdeling van verantwoordelijkheden van de hulpverleningsdiensten en zijn de calamiteitenorganisaties van de beheerders beschreven. Bij het plan ligt de nadruk op grote(re) incidenten (calamiteiten) waarbij een of meer hulpverleningsdiensten operationeel zijn gealarmeerd.

4. Kwaliteitsborging

Beheer

Dit plan wordt namens de Tunnelbeheerder van RWS West-Nederland Noord beheerd door de Tunnelbeheer Organisatie (TBO) van RWS West-Nederland Noord.

Namens afdelingshoofd district Zuid
West-Nederland Noord is TBO verantwoordelijk voor:

- Het afstemmen en (laten) verwerken van wijzigingen.
- Het laten toetsen van wijzigingen van het CBP door de afdeling Transitiemanagement van de VCNWN (toets op uitvoerbaarheid van wijzigingen door OVM/VCNWN).
- Het laten bekrachtigen van wijzigingen.
- Het doorgeven van relevante wijzigingen aan de hulpverleningsdiensten en aan de interne organisatie van de Tunnelbeheerder.
- Het op geordende wijze archiveren van actuele en vervallen documenten. De wijze waarop dit gebeurt, staat op de volgende pagina beschreven onder "Actualisatie".



Actualisatie Dit CBP wordt één keer per 4 jaar of zoveel vaker als nodig is geëvalueerd en zo nodig geactualiseerd. De evaluatie omvat zowel het CBP van RWS West-Nederland Noord als de aanvals- en inzetplannen van de hulpverleningsdiensten in de Veiligheidsregio's Amsterdam-Amstelland en Kennemerland.

Verantwoordelijk voor de uitvoering van de evaluatie zijn:

RWS West-Nederland Noord	Tunnelbeheer Organisatie (TBO)
Politie-eenheid Noord-Holland	Contactpersoon politie-eenheid Noord-Holland
Hulpverleningsdiensten Veiligheidsregio Kennemerland	Contactpersoon Brandweer/Veiligheidsregio Kennemerland Meldkamer Noord-Holland
Hulpverleningsdiensten Veiligheidsregio Amsterdam-Amstelland	Contactpersonen Brandweer/ Veiligheidsregio Amsterdam-Amstelland Meldkamer (Dienst Regionaal Operationeel Centrum) Amsterdam-Amstelland
Politie-eenheid Amsterdam	Contactpersonen politie-eenheid Amsterdam
Veiligheidsbeambte Rijkswaterstaat	De veiligheidsbeambte of een door haar aangewezen adviseur

Van de evaluatie wordt een verslag gemaakt met een overzicht van wijzigingsvoorstellen.
Wijzigingen worden afgestemd met betrokkenen en doorgevoerd. Het verslag wordt gezonden naar de hulpverleningsdiensten en de veiligheidsbeambte, en ter informatie ook naar het bevoegd gezag van de tunnel. Het verslag wordt gearchiveerd in het tunnelveiligheidsdossier (TVD).

Tussentijdse aanpassingen kunnen nodig zijn wanneer uitkomsten van incidenten en oefeningen, wetswijzigingen, areaalwijzigingen (nieuwe tunnels) en wijzigingen in operationele procedures daar aanleiding toe geven. Als een dringende aanpassing in de werkwijze mogelijk mocht zijn, wordt een afweging van de urgentie en de wijze van implementatie van de vereiste beheersmaatregel(en) uitgevoerd. Indien nodig wordt in aanvulling op het vastgestelde plan een tijdelijke beheersmaatregel geïmplementeerd, dit vooruitlopend op een nieuw plan welke de bewuste maatregel omvat.

Als het initiatief voor (een) wijziging(en) vanuit een of meer hulpverleningsdiensten komt, wordt dit besproken met de beheerder van dit CBP.

Alle aanpassingen gebeuren waar nodig in afstemming met de documenten van de veiligheidsregio's en regionale politie-eenheden en worden inhoudelijk zoveel mogelijk afgestemd op het in de landelijke Tunnelstandaard (LTS) van RWS opgenomen format CBP, de in de LTS opgenomen Uniforme Primaire Processen/Procedures (UPP) en de NIPV-Handreiking voor multidisciplinaire afstemming bij incidentbestrijding in wegtunnels.

De contactpersonen voor het CBP bij RWS West-Nederland Noord en de hulpverleningsdiensten stemmen wijzigingen van de eigen documenten af met de andere partijen. Een wijzigingsvoorstel (inclusief prioritering) wordt ter vaststelling voorgelegd aan de beheerder van het CBP. Deze neemt een besluit en stelt (het onderdeel van) het CBP opnieuw vast.

Ingebruikname

De contactpersoon van RWS West-Nederland Noord en de contactpersonen van de hulpverleningsdiensten zorgen voor verspreiding en implementatie van nieuwe of gewijzigde documenten binnen de eigen organisaties.

Elke versie van het CBP wordt pas in gebruik genomen als de doelgroep(en) op de hoogte is (zijn) gesteld van de wijzigingen en/of hierover is geïnstrueerd.

De ingebruikname van elk nieuw of gewijzigd document wordt zo nodig ondersteund met een geschikte uitleg en/of instructie aan de betrokken operationele medewerkers. De omvang van de uitleg en/of instructie hangt af van de aard van de wijziging. Wanneer deze niet ingrijpend is, kan meestal worden volstaan met een korte uitleg van de wijziging(en).

Archivering

De volgende documenten worden gearchiveerd:

- Alle goedgekeurde versies van CBP-documenten.
- Alle vervallen versies van CBP-documenten.
- Wijzigingsvoorstellen, inclusief afstemmingsinformatie.
- Verslagen van evaluaties van het CBP.

De beheerder van het CBP archiveert deze documenten in het tunnelveiligheidsdossier.

Calamiteitenbestrijdingsplan

(CBP) Wegtunnels

Rijkswaterstaat

West-Nederland Noord

Rijkswaterstaat
Ministerie van Infrastructuur en Waterstaat

Deel II Calamiteiten-/incidentscenario's

1. Inleiding

In het CBP zijn de procedures beschreven voor de onverwachte voorvallen die zich kunnen voordoen in een wegtunnel. In de Uniforme Primaire Processen (onderdeel van de landelijke RWS Tunnelstandaard) zijn de onverwachte voorvallen uitgesplitst in de volgende drie categorieën:

Calamiteiten:

- Brand of het vermoeden daarvan.
- Vrijkomen van gevaarlijke stoffen of het vermoeden daarvan.
- Ernstige aanrijding.
- Brand in de verkeerscentrale (VC).
- Bommelding.
- Tunnel ter beschikking van het bevoegd gezag.

Incidenten:

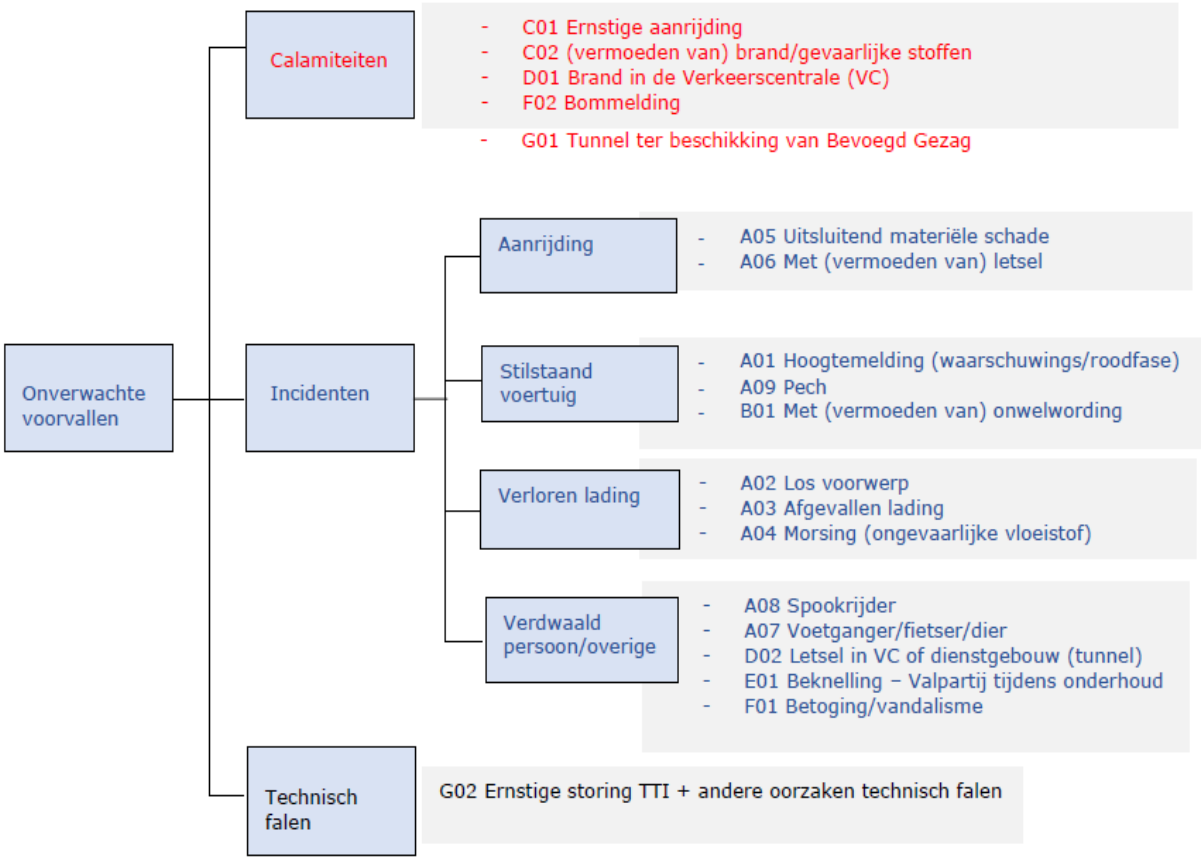
- Aanrijdingen.
- Stilstaande voertuigen.
- Verloren lading.
- Voorvallen met verdwaalde personen.

Technisch falen:

Ernstige storing van de Tunnel Technische Installatie (TTI) en andere oorzaken van technisch falen.

2. Clustering onverwachte voorvallen (incidentscenario's)

Vanuit de indeling in calamiteiten, incidenten en technisch falen volgen de verschillende procedures A01 t/m G02 om de voorvallen af te handelen. In het op de volgende pagina opgenomen overzicht uit de "Bedrijfsprocessen (UPP) RWS Tunnelsysteem", zijn de procedures weergegeven per categorie (calamiteiten, incidenten en technisch falen).



Het CBP betreft dus niet alleen de afhandeling van calamiteiten, maar ook de afhandeling van incidenten in de tunnels in beheer bij RWS West-Nederland Noord en (zeer summier beschreven) de afhandeling van technische storingen. Bijlage 5 bevat een beslis- en bevoegdhedenschema dat van toepassing is voor de te nemen maatregelen bij storingen (Prio 1, 2, 3 en 4 storingen conform de Faaldefinities[1]).

[1] Regionale Faaldefinities wegtunnels RWS WNN en VCNWN, versie 20 februari 2020

Deel III Procedures RWS

Deel III bevat de procedures en instructies voor de doelgroep: Wegverkeersleider (WVL), de Coördinerend Wegverkeersleider (cWVL), de Weginspecteur (WIS) en de Officier van Dienst-Rijkswaterstaat (OVD-RWS).

1. Functie- en rolbeschrijvingen WVL, (c)WVL, WIS en OVD-RWS
In onderstaande tabel wordt per functie/rol een korte beschrijving gegeven.

WVL	De WVL stuurt en geleidt het verkeer in een bepaalde regio (operationeel verkeermanagement én incident management) op het Hoofd Wegennet (HWN) vanuit een regionale verkeerscentrale. Een onderdeel van dit werk is het bedienen van de standaard (veiligheids)systemen en verkeersgeleidingssytemen die de veiligheid en de doorstroming in tunnels beïnvloeden.
cWVL	De cWVL coördineert de uitvoering van het werk in de regionale Verkeerscentrale. Hij zorgt voor interne kwaliteitsbewaking tijdens de diensten door procesondersteuning (coaching) en prioritering van werkzaamheden. Bovenregionale verkeersmaatregelen worden afgestemd met een landelijke wegverkeersleider bij het Verkeerscentrum Nederland (VCNL).
WIS	De WIS is "oren en ogen" op de weg. De WVL stuurt de WIS naar alle voorvallen die de doorstroming en de veiligheid op het HWN beïnvloeden. De WIS handelt ter plaatse incidenten en calamiteiten af op het HWN (en in tunnels) als vertegenwoordiger van Rijkswaterstaat.
OVD-RWS	Bij complexe incidenten, calamiteiten en ernstige storingen schaalt de WVL op naar de OVD-RWS (fase 1) die ter plaatse namens RWS optreedt als liaison naar de hulpverleningsdiensten (HD) en de aanwezige weginspecteur(s) aanstuurt. De OVD-RWS bepaalt of opschaling bij RWS naar coördinatieniveau fase 1 voldoende is. Tevens is de OVD-RWS degene die, via de voorzitter van het landelijk Crisisteam Rijkswaterstaat (CT-RWS), de beslisser van het CT-RWS adviseert om verder op te schalen naar fase 2.

2. Procedures Rijkswaterstaat
Rijkswaterstaat heeft alle af te handelen voorvallen in tunnels beschreven in Bedrijfsprocessen (UPP) RWS Tunnelsysteem (UPP-Tunnels), dat onderdeel is van de landelijke RWS Tunnelstandaard (LTS).
UPP-Tunnels is voor nieuwe tunnels tevens de basis voor de standaardtechniek in tunnels.

Instructiekaarten

a. Generieke instructiekaarten
RWS heeft landelijk generieke instructiekaarten vastgesteld voor de WVL, cWVL, WIS en OVD-RWS. Deze generieke instructiekaarten zijn één op één afgeleid van UPP-tunnels. Deze instructiekaarten zijn opgenomen op de Intranet site: OTO Wegtunnels (rws.nl)

De instructiekaarten voor de (c)WVL zijn in drie fases opgedeeld (conform UPP-Tunnels):

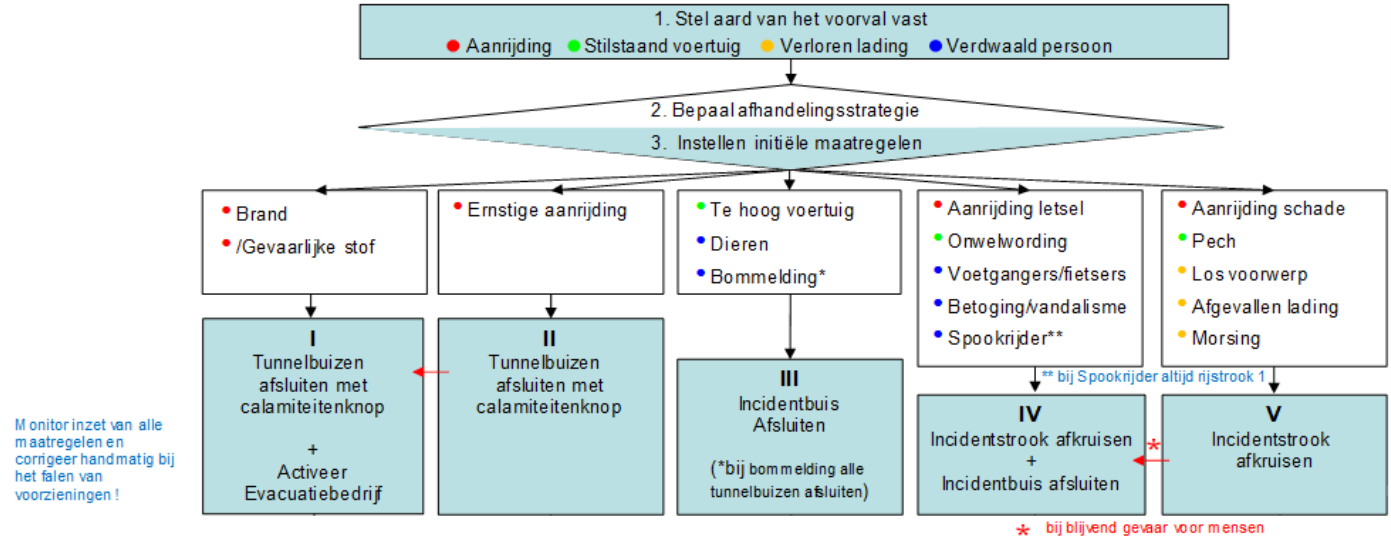
Fase 1: 1. Vaststellen aard van het voorval
2. Bepalen afhandelingsstrategie
3. Instellen initiële maatregelen
4. Informeren en Oproepen
Fase 2: 5. Instellen additionele maatregelen
Fase 3: 6. Herstellen en Normaliseren
7. Loggen en Registreren

Per scenario zijn initiële en additionele maatregelen van toepassing. Initiële maatregelen zijn de maatregelen die in de eerste minuten na het voorval plaatsvinden. De additionele maatregelen volgen wanneer de hulpverleningsdiensten en/of de OVD-RWS/WIS ter plaatse zijn.

Er zijn vijf initiële maatregelen:

Maatregel I: Tunnelbuizen afsluiten met calamiteitenknop + activeer evacuatiebedrijf.
Maatregel II: Tunnelbuizen afsluiten met calamiteitenknop.
Maatregel III: Incidentbuis afsluiten.
Maatregel IV: Incidentstrook afkruisen + incidentbuis afsluiten.
Maatregel V: Incidentstrook afkruisen.

Onderstaande figuur bevat een schematisch overzicht van fase 1, stappen 1 t/m 3 (zie hiervoor de vorige pagina). Hierin zijn de beslissing tot het nemen van initiële maatregelen en de initiële maatregelen blauw gekleurd om het verband tussen de stappen aan te geven.



Figuur: schematische weergave fase 1 (stappen 1 t/m 3).

In de instructiekaarten zijn maatregelen aangegeven voor het handelen bij calamiteiten en incidenten met een directe handeling in de tunnel (maatregelen I t/m V).

In de hiernavolgende tekst (vanaf pagina 4) zijn de instructiekaarten toegelicht, met per activiteit aanvullende informatie. Deze tekst dient als naslagwerk voor de betreffende medewerkers.

Naast de bovengenoemde situaties zijn ook kort de procedures beschreven bij "overige voorvallen". De procedures voor deze situatie zijn opgenomen in de toelichting. Dit zijn:
- Brand in de Verkeerscentrale (VC).
- Beknelling/valpartij tijdens onderhoud.
- Brand met ongeval in dienstgang
- Tunnel ter beschikking van bevoegd gezag, en
- Ernstige storing tunnel technische installaties (TTI) en andere oorzaken technisch falen tunnelveiligheid.

b. Referentiekaarten

Tevens zijn per functiegroep referentiekaarten opgesteld waarin per tunnel de specifieke afwijkingen zijn opgenomen ten opzichte van UPP-tunnels (procedures en (technische) voorzieningen)) en object specifieke zaken (aanrijdroutes, vluchtconcept e.d.).
De Referentiekaarten zijn opgenomen op de Intranet site: OTO Wegtunnels (rws.nl)

Toelichting instructiekaart (c)WVL

FASE 1: VASTSTELLEN AARD VAN HET VOORVAL (stap 1), BEPAAL DE AFHANDELINGSSTRATEGIE (stap 2), INSTELLEN INITIËLE MAATREGELEN (stap 3) en INFORMEREN EN OPROEPEN (stap 4)

1. Stel aard van het voorval vast

Alarmen/meldingen van het tunnelsysteem, MTM, telefoontjes van de gemeenschappelijke meldkamer (Meldkamer (OC)), maar vooral ook eigen waarneming via CCTV geven de eerste indicaties dat er een voorval heeft plaatsgevonden in de tunnel.

Door de camera bij het gepresenteerde alarm te selecteren kan een nader alarm(video)beeld van het voorval verkregen worden.

In deze stap is het van belang een eerste beeld te vormen van het voorval. Is het een:

- Aanrijding.
- stilstaand voertuig (of een naderend te hoog voertuig).
- verloren lading.
- of een verdwaald persoon.

Er is uiteraard een aantal voorvallen waarbij het direct duidelijk is waar het om gaat, zoals een te hoog voertuig, een spookrijder en een bommelding. Mocht de bommelding telefonisch rechtstreeks bij de WVL gemeld worden, dan moet de WVL de inhoudelijk verkregen informatie noteren (zie bijlage "Formulier bommelding"). Het verloop van alle voorvallen in de tunnels wordt gelogd door de WVL. Significante voorvallen worden aangemeld door de (c)WVL voor evaluatie. De (c)WVL zorgt ook dat de logging van deze voorvallen wordt gecompleteerd in het tabblad Tunnels en wordt toegevoegd aan het shiftjournaal. De evaluatie van significante voorvallen gebeurt door de tunnelbeheerder.
NB: Het loggen is een primair (schaduw)proces dat gelijk oploopt met de VWM operationele (tunnel) processen. Beschrijving van het logproces is te vinden op de VKA-site[1]: P01 Proces Loggen.

2. Bepaal de afhandelingsstrategie

In tweede instantie is het zaak om na de eerste beeldvorming een nadere typering te maken van het voorval. Bij elk type voorval hoort een bepaalde afhandelingsstrategie met specifieke initiële maatregelen (zie hiervoor de figuur op pagina 2 en de generieke instructiekaart voor de WVL en cWVL).
Het is zaak "het ergste" het eerst te herkennen/uit te sluiten (is het een calamiteit of een incident):

Bij maatregel I

- (Vermoeden van) Brand en/of gevaarlijke stoffen: er kan sprake zijn van een alarm van de zicht-/rookmeting of een alarm van het uitnemen van slanghaspels en draagbare brandblussers. Het tunnelsysteem zal dan een stand-by bedrijf aanbieden. Als binnen een kort tijdsbestek een SOS-detectie plaatsvindt in de verkeersbuis én een alarm van de zicht-rookmeting (rookdetectie) in de verkeersbuis én een detectie van het openen van een hulppostkast of (wat dit laatste betreft) een

[1] https://corporate.intranet.rws.nl/Kennis_en_Expertise/Kennisvelden/Wegverkeer/Verkeerskundige_Afspraken_VKA/Verkeersmanagement/Operationeel_verkeersmanagement/

detectie van een uitgenomen brandblusser of detectie van het gebruik van een slanghaspel, zal het tunnelsysteem automatisch calamiteitenbedrijf aanbieden, behalve bij de Wijkertunnel waar geen automatisch calamiteitenbedrijf aanwezig is. Dit is een calamiteit.

Bij maatregel II

- Ernstige aanrijding: Dit is een hoog energetisch ongeval. De rijbaan is gestremd (vermoedelijk is geen slagvaardige hulpverlening mogelijk via de incidentbuis). Er is geen (vermoeden) van brand en/of gevaarlijke stoffen. Ook dit is een calamiteit.
  Bij inzet van maatregel II wel altijd alert blijven of toch moet worden opgeschaald naar I.

  Een hoog energetisch ongeval is voor de WVL identificeerbaar aan de hand van de schouwkaart IM[2] in combinatie met camerawaarneming.

Bij maatregel III

Deze voorvallen zijn meestal duidelijk te herkennen en aldus te typeren.
- Een te hoog voertuig wordt gemeld door het systeem. Dit is een incident.
- Een dier in de tunnel is te herkennen met camerawaarneming. Dit is een incident.
- Een bommelding wordt gecategoriseerd als een calamiteit en zal meestal telefonisch worden gemeld.

Bij maatregel IV:

- Aanrijding met (vermoeden van) letsel: hier zijn minder voertuigen betrokken dan bij een ernstige aanrijding en mogelijk is de rijbaan nog gedeeltelijk vrij. Maar er is wel een vermoeden van letsel (hierbij vormt de schouwkaart IM in combinatie met camerawaarneming een hulpmiddel). Dit is een incident.
- (Vermoeden van) onwelwording: dit is misschien nog lastig te onderscheiden van pech. Maar als het voertuig vreemd tot stilstand is gekomen en de inzittenden niet reageren op het omroepbericht is het vermoedelijk een onwelwording. Dit is een incident.
- Voetgangers/fietsers: dit is te herkennen met camerawaarneming. Bij voetgangers is het wel zaak om uit te sluiten dat er ergens nog een auto staat. Dit is een incident.
- Betoging/vandalisme: te herkennen met camerawaarneming. Dit is een incident.
- Spookrijder: wordt meestal gemeld door de Meldkamer (OC), Verkeerscentrum Nederland (VCNL) of is te ontdekken door eigen camerawaarneming op het netwerk. Voorbij de tunnel (tot circa 600 meter) en in de tunnel geeft het tunnelsysteem een melding. Een spookrijder is een incident.

Bij maatregel V:

- Aanrijding uitsluitend materiële schade (UMS): dit kan een "kop-staart botsing" zijn (met een beperkt aantal auto's) waarbij er geen vermoeden is van letsel. Via camerawaarneming is duidelijk dat er geringe schade is (mensen zijn uit de auto gekomen). Dit is een incident.
- Pech: dit is een stilstaand voertuig, meestal met alarmlichten aan. Dit is een incident.
- Los voorwerp: te herkennen via camerawaarneming. Dit is een incident.
- Afgevallen Lading: te herkennen via camerawaarneming. Dit is een incident.

[2] Zie voor Schouwkaart IM: https://www.incidentmanagement.nl/downloadspublicaties/2283182.aspx
NB: Een kettingbotsing die voldoet aan de hierin genoemde kenmerken wordt ook behandeld als een ernstige aanrijding. Andere kettingbotsingen worden behandeld als een incident. Bij het opstellen van de Rarvw werd er vanuit gegaan dat de gevolgen van een kettingbotsing altijd vergelijkbaar zijn met die van een ernstige aanrijding. In de praktijk is gebleken dat er regelmatig kettingbotsingen voorkomen die niet meer zijn dan een aanrijding met meerdere voertuigen. De hulpdiensten behandelen deze kettingbotsingen niet als een calamiteit. Het is dan niet nodig en zelfs ongewenst dat de calamiteitenknop wordt ingedrukt. Een afhandeling als incident volstaat in dat geval.

- Morsing: mogelijk te herkennen via camerawaarneming of melding via de Meldkamer (OC). Dit is een incident.

Blijvend gevaar voor mensen:
Het verschil tussen maatregel V en maatregel IV is dat bij V alleen de incidentstrook afgekruist wordt en een snelheidsmaatregel geplaatst wordt op de ernaast gelegen vrije rijstrook en dat bij IV nog aanvullend op de afkruising van de incidentstrook ook de incidentbuis gesloten.
Bij inzet van maatregel V wel altijd alert blijven of niet moet worden opgeschaald naar IV.

Het aanvullend sluiten van de incidentbuis (maatregel IV) is nodig als de WVL voorziet dat ondanks de afkruising van de incidentstrook er toch een blijvend gevaar voor mensen blijft bestaan. Mogelijke criteria hiervoor zijn:

- Het voertuig, de inzittenden of de lading op zichzelf brengt een veiligheidsrisico met zich mee. Bijvoorbeeld: er staat een tankwagen met pech, er is een touringcar gestrand, een auto met een baby/kleine kinderen aan boord, een vrachtwagen met een gevaarlijke lading.
- Er zijn te weinig vrije rijstroken.
- De afstand van het voorval op de rijstrook waar het zich voordoet tot de aslijn van de ernaast gelegen vrije rijstrook is te klein.
- De snelheid van de voertuigen op de (ernaast gelegen) vrije rijstrook is te hoog en het gedrag van de voertuigen op de vrije rijstrook is onveilig (de bestuurders maken bijvoorbeeld onverwachte manoeuvres).

Het alerteringsniveau van dat moment kan ook een rol spelen. De Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) kan een verhoogde terreurdreiging voor één of meerdere tunnels afkondigen. Op dat moment is de procedure 'verdachte voertuigen in tunnels' van kracht. Deze informatie komt via de NCTV binnen bij de beslisser fase 2 van het CT-RWS. Via het CT-RWS wordt het OVM-Piket van de betrokken regionale verkeerscentrale (RVC) gealarmeerd. Dit betekent dat de WVL bij verdachte situaties direct overgaat tot het afsluiten van de tunnel. Alles wat niet normaal door de tunnel rijdt is dan verdacht[3].

3. Instellen initiële maatregelen

Zoals aangegeven in de figuur op pagina 2 en de generieke instructiekaart van de WVL en cWVL, hoort bij elk type voorval een specifieke set initiële maatregelen.

Bij I: Tunnelbuizen afsluiten met calamiteitenknop + activeer evacuatiebedrijf

- Druk op de calamiteitenknop of bevestig het calamiteitenbedrijf als de tunnel dit automatisch genereert[4].
- Monitor de inzet van alle maatregelen en neem corrigerende maatregelen bij falen van voorzieningen. Als een bepaalde voorziening niet het gewenste gedrag vertoont dan moet de WVL dit corrigeren, bijvoorbeeld door de betreffende voorziening handmatig te bedienen.
- Het tunnelsysteem zal alle maatregelen van het calamiteitenbedrijf instellen (en heeft mogelijk reeds de voorzieningen voor een (veilige) vluchtroute geactiveerd door in stand-by bedrijf te gaan)).
- Activeer het evacuatiebedrijf.

- Doordat het evacuatiebedrijf is geactiveerd, wordt automatisch in de incidentbuis en het middentunnelkanaal (MTK) / veilige ruimte van de Wijkertunnel, Velsertunnel, Coentunnel en Gaasperdammertunnel de standaard evacuatie-instructie voor de weggebruikers omgeroepen in twee talen (Nederlands en Engels). In de Zeeburgertunnel en Schipholtunnel moet deze in 2 talen uit te

[3] Zie VKA: C03 Alertinstructie verdacht voertuig in tunnels en T01 Dreiging in tunnels (zie VKA site)
[4]. Standaard tunnels hebben niet meer een fysieke calamiteitenknop op de desk.
Er zijn twee manieren om calamiteitenbedrijf te activeren: via de "calamiteitenknop" op het MAP Touch Panel of via de "calamiteitenknop" op de grafische userinterface (GUI).

zenden standaard evacuatie-instructie (”Dit is een noodsituatie. Verlaat uw voertuig, verlaat de tunnel via de vluchtdeur”) handmatig worden geactiveerd (zie bijlage 11 bij geactiveerde systemen onder Evacuatiebedrijf). Daarnaast wordt op de informatie-display van de autoradio het volgende tekstbericht getoond: "Tunnelincident, volg instructies, follow instructions".
- Spreek (aanvullend) achterblijvers aan via de luidsprekerinstallatie (in het Engels en Nederlands).

NB: Bij een calamiteit in de Gaasperdammertunnel activeert het tunnelsysteem een beveiligde, geautoriseerde beeldverbinding met de Meldkamer (OC)[5]. Het meldkamerpersoneel kan dan meekijken met het beeld dat de WVL heeft geactiveerd. Dit beeld wordt ook getoond op het hulpdienstpaneel (HDP) bij de tunnelingang. Op verzoek van de Meldkamer (OC) kan de WVL bij de Gaasperdammertunnel ook bij bommelding of bij betoging/vandalisme handmatig een beeldverbinding tot stand te brengen met de Meldkamer (OC).

Bij II: Tunnelbuizen afsluiten met calamiteitenknop
- Druk op de calamiteitenknop.
- Ook hier monitoren van de inzet van maatregelen en correctie bij falen voorzieningen[6].
- Indien er nog rijstroken vrij zijn, dan is het wenselijk dat de WVL het verkeer dat bovenstrooms van het voorval tot stilstand is gekomen, gecontroleerd (met afkruising van de incidentstrook en een snelheidsmaatregel op de vrije rijstrook[7]) de tunnelbuis uit laat rijden.

NB: De WVL moet in korte tijd beslissen of hij op de calamiteitenknop drukt of niet. Qua besluitvorming zal zijn focus primair gericht zijn op de ernst van de calamiteit en secundair op de stremming van de rijbaan. Dus bij een ernstige aanrijding (waarneembare hoogenergetische impact) dient hij op de calamiteitenknop te drukken. In de eerste momenten na een ernstige aanrijding zal de rijbaan vermoedelijk in ieder geval korte tijd gestremd zijn, omdat weggebruikers stroomopwaarts in de remmen gaan. Indien blijkt dat het verkeer (toch) oplost en er een vrije rijstrook verschijnt waardoor de hulpverlening het incident effectief kan bereiken via de incidentbuis, dan mag de WVL *in overleg met* de Meldkamer (OC) afschalen van Maatregel II (procedure C01 ”Ernstige aanrijding”) naar Maatregel IV (procedure A06 ”aanrijding met (vermoeden van) letsel”).

Bij III: Incidentbuis afsluiten
- Bij een te hoog voertuig zullen de verkeerslichten van de tunnelbuis automatisch op (onvoorwaardelijk) rood gaan.
- Bij dieren: omdat een dier zich onvoorspelbaar gedraagt, heeft het geen zin om eerst een rijstrook af te kruisen en wordt dus de gehele tunnelbuis gesloten. Hiermee worden gevaarlijke uitwijkmanoeuvres voorkomen. Het sluiten van de tunnelbuis vindt plaats met de verkeerslichten en afsluitbomen.
- Bommelding die bij VCNWN binnenkomt:
  a. Bommelding die specifiek gericht is op de tunnel:
     - melding via de Meldkamer (OC) doorgeven aan politie en nadere instructies van de politie opvolgen.
     - sluit alle tunnelbuizen met verkeerslichten en afsluitbomen na opdracht van de politie.[8]
  b. Bommelding die niet specifiek gericht is op de tunnel, maar in de nabijheid van de tunnel:
     - melding via de Meldkamer (OC) doorgeven aan politie en vraag advies aan Meldkamer (OC).

[5] De beeldvoorziening naar de Meldkamer (OC) zorgt ervoor dat in de Meldkamer (OC) het detailbeeld dat door het camerasysteem wordt getoond aan de wegverkeersleider, kan worden weergegeven.
[6] Deze actie geldt uiteraard ook III, IV en V maar wordt in de toelichting verder niet meer vermeld.
[7] Dit is geautomatiseerde actie, die niet door de WVL wordt uitgevoerd.
[8] Is conform instructie van de Bureaus Conflict en Crisisbeheersing (CCB) van de politie-eenheden Amsterdam en Noord-Holland. Deze instructie is vermeld op de Referentiekaarten van de (c)WVL, zie: OTO Wegtunnels (rws.nl)

Bij IV: Incidentstrook afkruisen + incidentbuis afsluiten

- Geef opdracht tot het geheel afkruisen van de incidentstrook waarop het voorval heeft plaatsgevonden en zet gelijktijdig een snelheidsmaatregel van 70 op de ernaast gelegen vrije strook (bij een voorbereide maatregel in MTM kruist MTM de strook over de gehele lengte van de tunnel af en zet gelijktijdig een snelheidsmaatregel van 70 op de ernaast gelegen vrije strook. Zo worden gestrande weggebruikers op de incidentstrook en de overige weggebruikers die nog in de tunnel rijden beschermd tegen een mogelijke aanrijding;
- Sluit onmiddellijk na het afkruisen ook de tunnelbuis aangezien er een (vermoeden) van een blijvend gevaar voor mensen is. Verifieer met de camera dat de afsluitbomen veilig naar beneden kunnen.

- **Spookrijder**:
  - Indien er in de nabijheid op het traject van de tunnel een spookrijder wordt gesignaleerd moet opdracht worden gegeven om rijstrook 1 (= de eerste rijstrook, met de rijrichting van het verkeer mee, gerekend vanaf de middenberm) voor de afsluitbomen van de tunnel af te kruisen van het signaleringsportaal dat vooraf gaat aan het portaal met de verkeerslichten tot de plaats waar de spookrijder is gesignaleerd.
  - Indien het mogelijk is de tunnel tijdig te sluiten, dan wordt in aanvulling op het afkruisen van rijstrook 1 ook de tunnelbuis gesloten met verkeerslichten en afsluitbomen. Het risico dat een spookrijder de afsluitbomen raakt is te prefereren boven het risico dat de spookrijder een medeweggebruiker raakt. NB: de WVL dient de werkinstructie VKA:I07 Spookrijder te volgen.
  - Bij een spookrijder in een van de parallelbuizen van de GDT wordt de buis, als het mogelijk is de tunnel tijdig te sluiten, met de (primaire) afsluitbomen afgesloten op de A9 en op de invoeger van de S112 (verkeerslichten op rood + fysiek afsluiten met de afsluitbomen).
    NB: De WVL dient hier bovendien de werkinstructie VKA:I07 Spookrijder te volgen.

Bij V: Incidentstrook afkruisen
- Geef opdracht tot het geheel afkruisen van de incidentstrook waarop het voorval heeft plaatsgevonden en zet gelijktijdig een snelheidsmaatregel van 70 op de ernaast gelegen vrije strook.

NB: In een verkeersbuis met meer dan 2 rijstroken is het sluiten van de verkeersbuis niet nodig indien met het afkruisen van een tweede rijstrook blijvend gevaar voor mensen wordt vermeden.

4. Informeren en oproepen

Monitor evacuatie
- In afwachting van de hulpverleningsdiensten (HD) monitort de WVL de situatie in de tunnel en de evacuatie. Enerzijds om de HD goed te kunnen informeren, anderzijds om te zien of iedereen de tunnel daadwerkelijk verlaat. Eventueel worden nog aanvullende evacuatie-instructies gegeven, zoals beschreven bij stap 3. Deze activiteit gebeurt alleen ingeval geëvacueerd moet worden i.v.m. brand en/of gevaarlijke stoffen.

Instrueer weggebruiker
- Bij voorvallen waarbij de tunnelbuis niet gesloten wordt (en dus één of meer rijstroken beschikbaar blijven voor de doorstroming van het verkeer) moet indien mogelijk een algemene waarschuwingsboodschap worden geactiveerd (tekstbericht) die op het informatie-display van de autoradio zichtbaar is.
  Tevens wordt op de HF-installatie "ingebroken" op het radiosignaal, zodat de boodschap te horen is via de autoradio (zie bijlage 14 overzicht Omroepberichten).
- De bij het voorval betrokken weggebruikers worden - via de luidsprekerinstallatie (tweetalig uit te spreken boodschap) – verzocht naar de hulppost te gaan en met de noodtelefoon contact op te nemen met de WVL (in de boodschap operator genoemd (zie bijlage 14 overzicht Omroepberichten).

- In de hulppost krijgt de weggebruiker via de noodtelefoon een nadere veiligheidsinstructie inhoudende wat te doen of te laten tot de komst van de WIS en de HD.
  - Geen barrier beschikbaar[9]: snelheid op de vrije strook terugbrengen van 70 naar 50 en de weggebruiker vragen te wachten 50 meter voorbij het voertuig. De weggebruiker blijft zodoende tot de komst van de WIS in de "schaduw" van zijn auto, om te voorkomen dat hij (direct) aangereden wordt[10]. De WIS of de eerst aanwezige vertegenwoordiger van de hulpverleningsdiensten (HD) zal zijn voertuig zodanig voor het gestrande voertuig plaatsen dat er voldoende veiligheidsruimte is waardoor dit voertuig als buffer optreedt voor het gestrande voertuig. Indien de WIS en/of HD niet op tijd kunnen arriveren of blijvend gevaar voor mensen ontstaat, dient de WVL te besluiten om de tunnelbuis te sluiten.
- Ingeval van een calamiteit met brand en/of gevaarlijke stoffen heeft de instructie van de weggebruikers al automatisch plaatsgehad in stap 3 (zie hiervoor). In stap 4 is het zaak alert te blijven en handmatig eventueel de mondelinge evacuatieboodschap voor achterblijvers te herhalen.
- Bij een ernstige aanrijding wordt handmatig omgeroepen dat het verkeer voor langere tijd vaststaat, dat men de voertuigen uit moet zetten en moet wachten op de hulpverleningsdiensten (ook in dit geval een tekstbericht op de autoradio met "volg instructies").
- Ook voor voetgangers/fietsers in de tunnel en voor de spookrijder zijn er aparte boodschappen die afgespeeld kunnen worden (zie bijlage 14 overzicht Omroepberichten).

Informeer Meldkamer (OC)
- De Meldkamer (OC) wordt door de WVL altijd geïnformeerd over calamiteiten en ernstige storingen waarbij een tunnelbuis of de tunnel wordt gesloten.
- De Meldkamer (OC) wordt ook geïnformeerd over de volgende incidenten:
  - aanrijding met letsel of een vermoeden van letsel.
  - stilstaand voertuig met onwel wording of een vermoeden van onwel wording.
  - een betoging.
  - vandalisme.
  - aanwezigheid van voetgangers, fietsers of dieren, en
  - spookrijder.
- De (c)WVL maakt voor melding van het voorval aan de Meldkamer (OC), WIS en OVD-RWS gebruik van een uitvraagprotocol (zie voor de onderdelen van dit protocol: Deel IV "Afspraken met hulpverleningsdiensten" van dit CBP).

NB: de WVL kan bij de Gaasperdammertunnel de beeldverbinding met de Meldkamer (OC) handmatig tot stand te brengen bij een bommelding of bij betoging/vandalisme.

Zet WIS in/zet OVD-RWS in
- De WIS wordt door de WVL ingezet voor elk voorval waarbij zijn hulp en ondersteuning gewenst is.
- Bij calamiteiten ernstige incidenten, ernstige storingen en ernstig falen van de civiele constructie/infra, welke effect hebben op de omgeving en/of waarbij coördinatie nodig is op de incidentlocatie, alarmeert de WVL (conform opschalingscriteria) de OVD-RWS die ter plaatse gaat en de WIS aanstuurt. In voorkomende gevallen kan de OVD-RWS, mede aan de hand van de opschalingscriteria, kiezen voor coördinatie op afstand. Wanneer de WIS of de WVL expliciet aan de OVD-RWS verzoekt om ter plaatse te komen, moet de OVD-RWS hier gehoor aan geven. De opschaling verloopt altijd via de Verkeerscentrale.
- In deze situaties is sprake van opschaling naar coördinatieniveau fase 1 (Crisisplan Rijkswaterstaat).

[9] In de tunnels waarop dit CBP betrekking heeft is geen barrier aanwezig.
[10] NB: De afstand van 50 meter is mogelijk – vanwege de hardheid van de barrier – niet groot genoeg om het gestrande voertuig separaat als buffer te laten fungeren tot de komst van de WIS. Er is echter niet voor gekozen om de gestrande weggebruiker nóg verder van het gestrande voertuig weg te zetten, omdat de kans dat de weggebruiker direct worden aangereden en daar blijvend letsel aan overhoudt hoger wordt ingeschat dan de kans dat dit bij een indirecte aanrijding (gestrande voertuig wordt geraakt en glijdt via de harde barrier door naar de wachtende weggebruiker) gebeurt.

De OVD-RWS is in dat geval bij/vanuit RWS verantwoordelijk voor de operationele leiding en coördinatie van het voorval (zowel in het brongebied als in het direct aangesloten effectgebied)[11].
- Er zijn verschillende voorvallen waarbij het mogelijk is dat de OVD-RWS zelf verder opschaalt naar het (landelijk) Crisisteam RWS (CT-RWS).[12]
- Bij een eenvoudig incident (bij het sluiten van een incidentstrook of het kort sluiten van een tunnelbuis) wordt de OVD-RWS niet geïnformeerd.

Herverdeel taaklast (bij overbelasting)
In de generieke instructiekaart van de (c)WVL is met de kleur grijs aangegeven welke taken in aanmerking komen om door de cWVL te worden overgenomen of te worden herverdeeld over andere WVL's, dit om ervoor te zorgen dat de WVL zich primair op het voorval in de tunnel kan concentreren als dit gezien diens werkdruk wenselijk/nodig is. Dit zal voornamelijk het geval zijn bij de afhandeling van calamiteiten en minder bij de afhandeling van incidenten (vandaar dat de "X" hier tussen haakjes is geplaatst).

Informeer VCNL > 15 minuten
- Alle voorvallen die - naar inschatting van de WVL of de CWVL - langer dan 15 minuten duren, moeten worden gemeld aan VCNL (met een restduurschatting). Dit vanwege het belang voor de verkeersinformatie en de mogelijkheid om tijdig een afweging voor een bovenregionale omleiding te kunnen maken.

Informeer via DRIP
- Indien de route naar de tunnel beschikt over een DRIP dienen weggebruikers die de tunnel naderen attent gemaakt te worden op het voorval en de mogelijke vertraging die dit met zich meebrengt.

Roep Berger op
- In de meeste gevallen zal het Landelijk Centraal Meldpunt (LCM) – ingeval van personenauto(`s) – of het Centraal Meldpunt Vrachtautoberging (CMV) – ingeval van vrachtauto(`s) - via de IM-regeling al een berger op pad gestuurd hebben indien weggebruikers het voorval via 112 gemeld hebben. Als dit niet het geval is belt de WVL met het LCM/CMV en verzoekt om een berger.

Informeer Pikethouder OVM
- Indien de tunnel vanwege een calamiteit of een ernstige storing wordt gesloten informeert de cWVL de pikethouder Operationeel Verkeersmanagement (OVM).

[11] De WVL kan de OVD-RWS faciliteren met het bereiken van het regio-piket. Tevens kan de OVD-RWS op basis van het beeld van de calamiteit, de storing of van het falen van de civiele constructie/infra bepalen of opschaling naar coördinatieniveau fase 1 voldoende is of om, via de technisch voorzitter van het landelijk Crisisteam RWS (CT-RWS), de beslisser van het CT-RWS te adviseren verder op te schalen naar coördinatie-niveau fase 2. Wanneer is opgeschaald naar coördinatieniveau fase 2 blijft de OVD-RWS verantwoordelijk voor de operationele leiding ter plaatse. De OVD-RWS zal in dat geval toestemming aan de beslisser CT-RWS moeten vragen voor het weer vrijgeven van de tunnel. Zie voor nadere informatie de toelichting op de "Instructiekaart WIS/OVD-RWS" bij "Korte informatie ten aanzien van voorvallen op coördinatieniveau fase 1 van het Crisisplan Rijkswaterstaat" en "Geef tunnel vrij".

[12] Voorvallen waarbij opschaling naar fase 2 een serieuze optie is/mogelijk vaker wordt voorkomt, betreffen:
- Afgesloten tunnel vanwege slecht weer (wateroverlast, sneeuw, ijzel) (zie procedure N02), Ernstige Aanrijding (zie procedure C01), Calamiteit met Brand en/of gevaarlijke stoffen (zie procedure C02), Brand in de Verkeerscentrale (zie procedure D01), Bommelding (zie procedure F02), Tunnel die ter beschikking is gesteld van het Bevoegd Gezag (zie procedure G01) ,Ernstig ongeval tijdens onderhoud in een tunnel (zie procedure E01), Betoging/vandalisme in een tunnel (zie procedure F01), Prio 1 storingen waarbij de tunnel gesloten wordt dan wel storingen waarbij de hersteltermijn dreigt te overschrijden en de tunnel gesloten zou moeten worden (zie procedure G02).

FASE 2: INSTELLEN ADDITIONELE MAATREGELEN (STAP 5)

Stel eventueel een alternatieve route in

- Indien er een kritische vertraging optreedt vanwege een voorval in een tunnel, dan dient een alternatieve route te worden ingesteld. Voor het activeren van Groot- en Kleinschalige Alternatieve Routes (GAR en KAR) of CBM (Cross Border Management) moet aan minstens één van de onderstaande criteria worden voldaan:
  - de (verwachte) restduur van het voorval is groter of gelijk aan 30 minuten;
  - de (verwachte) vertraging is groter of gelijk aan 15 minuten;
  - de (verwachte) reistijd op de primaire route is groter of gelijk aan de reistijd op de alternatieve route.[13]

Voor specifieke regelscenario's: hierop zijn de regelscenario's van de verkeerscentrale van toepassing.

Faciliteren aanrijden HD (hulpverleningsdiensten)

- De WIS, de OVD-RWS en de HD benaderen incidenten in principe[14] altijd via de incidentbuis met de rijrichting mee. Bij gevaar voor mensen is de incidentbuis gesloten.
- De HD benaderen calamiteiten (brand/gevaarlijke stoffen, ernstig aanrijding) in principe via de gesloten ondersteunende buis met de rijrichting mee.
- De WVL geeft de bevelvoerder van de HD bij calamiteiten toegang tot de ondersteunende tunnelbuis.
- De bevelvoerder van de verkennende eenheid van de HD beslist ter plaatse of verkenning via de ondersteunende buis of direct in de incidentbuis nodig of gewenst is.[15] De (c)WVL kan hierbij adviseren via de Meldkamer (OC).
- De hoogst leidinggevende van de HD kan na inspectie van de tunnelbuis (door de verkennende eenheid van de HD onder leiding van de bevelvoerder van deze eenheid), toestemming geven aan de overige HD, de OVD-RWS en de WIS om de incidentbuis in de rijrichting te benaderen.
- WVL geeft de HD, de OVD-RWS en de WIS bij incidenten waarbij één tunnelbuis is afgesloten, toegang tot de incidentbuis.

Briefing HD

Met de briefing wordt bedoeld dat men op de hoogte wordt gebracht van de laatste specifieke informatie.

- Bij een vermoeden van brand of gevaarlijke stoffen (calamiteit) brieft de WVL de eerst aankomende tankautospuit (TS) van de brandweer. Bij calamiteiten waar de brandweer niet wordt ingezet (wat kan voorkomen bij een ernstige aanrijding) is dit de bevelvoerder/hoogst leidinggevende van de eerst aangekomen surveillance eenheid van de politie of de WIS/OVD-RWS. Bij de Gaasperdammertunnel is voor de briefing van de brandweer het hulpdienstpaneel (HDP) beschikbaar waarmee (ook) de situatie in de tunnel kan worden bekeken. De OVD-RWS en de WIS worden later door de hoogst-leidinggevende van de HD gebriefd (in het motorkapoverleg (MKO) dan wel het CoPI)).
- Onderdeel van de briefing is het bevestigen van het nummer van de vluchtdeur die voor verkenning gebruikt kan worden. Om snel te kunnen verkennen en hulp te bieden, hebben de HD een veilige vluchtdeur nodig om vanuit de ondersteunende buis door te kunnen steken naar de plaats in de incidentbuis waar het voorval heeft plaatsgevonden. Bij (vermoeden) van brand en/of gevaarlijke stoffen dient dit een vluchtdeur te zijn bovenstrooms van het voorval.

[13] Er is een redelijke alternatieve route voorhanden, d.w.z. de route leidt over het Rijkswegennet of ter plaatse geschikte N-wegen en is (grotendeels) vrij van verkeershinder. Zie voor verdere toelichting en werkinstructie het protocol VKA: D01 (De)activeren Alternatieve Routes.

[14] Ambulances aan de verkeerde kant van de tunnel die een noodoproep krijgen kunnen eventueel doorsteken via de CADO (uiteraard nadat de ondersteunende buis eerst gesloten is).

[15] Bij (vermoeden van) brand en/of uitstroom van gevaarlijke stoffen zal de verkenning van de incidentbuis in principe altijd via de ondersteunende buis (moeten) plaatsvinden. Bij gevaarlijke stoffen in de tunnel kan de bevelvoerder van de verkennende eenheid er, mede afhankelijk van de weersomstandigheden, voor kiezen om van dit principe af te wijken. Bij ernstige aanrijding (hoog energetisch ongeval en de rijbaan is gestremd) kan na het indrukken van de calamiteitenknop het verkeer oplossen en een vrije rijstrook in de incidentbuis verschijnen, waardoor de hulpverlening het incident effectief kan bereiken via de incidentbuis.

Briefing OVD-RWS/WIS

- Bij incidenten brieft de WVL de OVD-RWS en de WIS (telefonisch). Zij briefen de HD die ter plaatse komt.

Geef toegang

- Bij ernstige aanrijding mag de WVL aan alle hulpverleningsdiensten toegang verlenen tot de *ondersteunende* buis. De eerst aangekomene van de hulpverleningsdiensten (ook de WIS/OVD-RWS) mag de verkenning uitvoeren. Ambulance medewerkers mogen geen verkenning uitvoeren, alleen onder begeleiding van Brandweer, Politie of WIS/OVD-RWS.

- Bij vermoeden van Brand en/óf gevaarlijke stoffen krijgt alleen de bevelvoerder van de tankautospuit van de Brandweer toegang tot de ondersteunende buis. Alleen hij kan de verkenning uitvoeren. Overige hulpverleningsdiensten en de WIS krijgen pas toegang tot de ondersteunende buis als de bevelvoerder van de tankautospuit van de Brandweer (of de hoogst-leidinggevende van de Brandweer indien die inmiddels aanwezig is) hiervoor het "sein veilig" heeft gegeven.

- Voor directe benadering van de *incidentbuis* door overige hulpverleningsdiensten is bij een Ernstige aanrijding toestemming nodig van de hoogst-leidinggevende van de eerst aanrijdende eenheid (of de bevelvoerder van de betreffende hulpverleningsdienst als de hoogst-leidinggevende nog niet aanwezig is). Dit kan brandweer, politie of WIS/OVD-RWS zijn. Bij vermoeden van Brand en/of gevaarlijke stoffen dient ook eerst een "sein veilig" te zijn afgegeven door de hoogst-leidinggevende van de Brandweer (of de bevelvoerder van de brandweer als zijn hoogst-leidinggevende nog niet aanwezig is) alvorens de overige hulpverleningsdiensten en WIS/OVD-RWS de incidentbuis kunnen benaderen.

Voer opdrachten HD/OVD-RWS/WIS uit

- Indien de HD aanwezig zijn op de plaats van het voorval, dan voeren zij het bevel over de te treffen additionele maatregelen in de tunnel. Indien de HD er niet zijn, voert de OVD-RWS ter plaatse het bevel en anders (indien of zolang de OVD-RWS niet ter plaatse is) de WIS ter plaatse. De cWVL en de WVL in de VC ondersteunen de maatregelen die de HD, OVD-RWS en WIS aangeven.
- Communicatie van hulpdiensten met de VC verloopt via de OVD-RWS/WIS ter plaatse. Zijn zij niet aanwezig dan verloopt communicatie bij voorkeur via de Meldkamer (OC).
- Bij problemen met verbindingen kan de communicatie lopen via de noodtelefoon. De WVL dient zich er bij calamiteiten van te vergewissen dat hij spreekt met de bevelvoerder van de verkennende eenheid van de HD of de hoogst-leidinggevende[16].
- Het is mogelijk om ventilatie terug te schakelen en/of geluidbakens en geautomatiseerde omroepberichten uit te zetten zodra deze systemen geen meerwaarde meer hebben (brand is geblust of zelfredzaamheidsfase is voorbij). Ventilatie, geluidbakens en geautomatiseerde omroepberichten kunnen zorgen voor geluidshinder, zodat het terugschakelen of uitzetten van deze systemen de communicatie ten goede komt. Ventilatie kan ook zorgen voor een lage gevoelstemperatuur of afkoeling. De brandweer ter plaatse geeft opdracht tot het terugschakelen of uitzetten van genoemde systemen, maar de WVL of de ter plaatse aanwezige OVD-RWS of (bij diens afwezigheid) WIS kan dit ook voorstellen bij de brandweer.

Monitor veilig werken

- De WVL ziet erop toe dat de Richtlijn eerste veiligheidsmaatregelen bij verkeersincidenten (REVI) in acht wordt genomen. Bij afwijking van de richtlijn maakt de WVL de HD, OVD-RWS en WIS hier nadrukkelijk op attent.

Bewaak afhandeltijd

- Het is de taak van de WVL om te monitoren dat de afhandeling van het voorval zodanig geschiedt dat de doorstroming zo snel mogelijk weer kan worden hersteld. De WVL kan hiervoor adviezen geven aan de OVD-RWS en WIS ter plaatse.

[16] Bij twijfel expliciet uitvragen dat betrokkene spreekt in opdracht van de hoogst-leidinggevende van de HD.

Informeer VCNL
- De (c)WVL houdt ook VCNL op de hoogte van de vorderingen zodat weggebruikers geïnformeerd blijven.

FASE 3: HERSTELLEN EN NORMALISEREN (STAP 6), LOGGEN EN REGISTREREN (STAP 7)

Stel Onderhoud-Herstelbedrijf in
- Een tunnel die afgesloten is via de calamiteitenknop kan alleen via "Onderhoud-Herstel na Calamiteitenbedrijf" weer in "Normaal Bedrijf" gekregen worden. Ingeval het evacuatiebedrijf is geactiveerd moet de betreffende tunnelbuis eerst weer teruggeschakeld worden naar calamiteitenbedrijf. Zie hiervoor bedieningsinstructies.

Herstel doorstroming in opdracht van OVD-RWS/WIS
- De OVD-RWS/WIS moeten o.a. zorgen dat de doorstroming zo snel mogelijk weer op gang komt. Dat kan door in ieder geval 1 rijstrook vrij te maken en het verkeer doorgang te verlenen. Voorwaarde is dat dit veilig kan (met afkruising van de incidentstrook en beveiligd door de WIS, een snelheidsmaatregel van 50 km op de ernaast gelegen vrije rijstrook; verder afhandeling incident op voldoende afstand van de aslijn met de vrije rijstrook en conform gestelde voorwaarden door de hoogst-leidinggevende van de HD).
- Het kan zijn dat dit niet (tijdig) mogelijk is. Dan moet georganiseerd worden dat het gestrande verkeer vóór de calamiteit of incident weggeleid wordt conform het protocol VKA: D04 wegleiden opgesloten verkeer. De WVL dient deze maatregelen vanuit de VC te ondersteunen. Bijvoorbeeld door het verkeer gecontroleerd de tunnelbuis uit te laten rijden:
  - A. Het verkeer laten keren en via de stroomopwaarts gelegen toerit omleiden over het onderliggend Wegennet.
  - B. (Toepassen als optie A niet mogelijk is:) Het verkeer door de CaDo in de middenberm laten keren en via de andere weghelft terug laten keren naar het stroomopwaarts gelegen knooppunt en vanaf daar omleiden over het hoofdwegennet.

Schouw tunnelbuis
- De WVL schouwt de tunnelbuis met de camera's nadat hij van de OVD-RWS of WIS telefonisch toestemming heeft gekregen om de tunnelbuis weer te openen.
  Voorafgaand aan deze toestemming heeft de WIS of OVD-RWS eerst een eigen schouw ter plaatse uitgevoerd[17].
- Indien is opgeschaald naar coördinatieniveau fase 2 bepaalt de beslisser van het landelijk Crisisteam RWS (CT-RWS) of de tunnel(buis) weer open mag. Hij communiceert dit met de OVD-RWS en deze informeert de (c)WVL.
- Een mogelijk herstel en test van de uitrusting van de tunnel kan aan het openstellen van de tunnel(buis) voorafgaan.

Stel Normaal Bedrijf in
- Zoals hiervoor al aangegeven, wordt een tunnel die afgesloten is via de calamiteitenknop éérst in "Onderhoud-Herstel na Calamiteitenbedrijf" gebracht. Hierna dient de tunnel eerst in "Normaal Bedrijf" te worden geschakeld om te kunnen openen. Zie hiervoor bedieningsinstructies.

[17] Voordat de WIS/OVD-RWS de tunnel kan vrijgeven dient hij de checklist af te werken.

Verwijder afkruising, etc.
- Alvorens een tunnelbuis geopend wordt, dienen eerst de getroffen verkeersmaatregelen, zoals afkruisingen, te worden verwijderd.

Open tunnelbuis voor verkeer
- Ingeval sprake is van coördinatieniveau fase 1 beslist de OVD-RWS bij/vanuit RWS over het weer vrijgeven van de tunnel voor het verkeer. Indien is opgeschaald naar coördinatieniveau fase 2 beslist de beslisser van het landelijk Crisisteam RWS (CT-RWS) hierover[18].
- Het vrijgeven van een tunnelbuis voor verkeer door de WVL kan slechts na uitdrukkelijke schouw. Zie hiervoor ook de toelichting op de instructiekaart van de WIS/OVD-RWS bij Fase 3.

Informeer Meldkamer (OC)
- In die gevallen waarbij de HD betrokken zijn geweest bij de afhandeling van het voorval, meldt de WVL aan de Meldkamer (OC) dat de tunnel(buis) weer open is. Dit gebeurt ook bij ernstige storingen met een (gedeeltelijke) sluiting als gevolg.

Informeer VCNL
- Alle voorvallen die gemeld zijn bij VCNL worden daar ook weer afgemeld. Dit vanwege het belang voor de verkeersinformatie en de mogelijkheid om tijdig de opheffing van een bovenregionale omleiding te kunnen voorbereiden.

Hef alternatieve route op
- Indien er een alternatieve route is ingezet moet deze weer worden opgeheven.

Informeer Pikethouder OVM
- Indien Pikethouder(s) (is) (zijn) geïnformeerd dan ook weer bij deze afmelden dat de situatie is hersteld.

Herstel taakverdeling
- De c-WVL kan de oude taakverdeling herstellen.

Completeer log
- Tijdens de afhandeling van het voorval is het loggingssysteem steeds bijgewerkt (in het tabblad Tunnels). Ook het tunnelsysteem houdt bij welke toestanden, meldingen, alarmen, etc. wanneer hebben plaatsgevonden. Bij het completeren van de logging kunnen deze gegevens aan de logging worden toegevoegd, bijvoorbeeld als het een significant voorval betreft. Ook informatie van de WIS en de OVD-RWS kan worden toegevoegd.

Registreer significantie
- Significante voorvallen worden aangemeld door de (c)WVL voor evaluatie na overleg met de OVD-RWS/WIS. De (c)WVL zorgt tevens dat de logging van deze voorvallen wordt gecomplementeerd in het tabblad Tunnels en toegevoegd aan het shiftjournaal. De wijze van registreren is beschreven in UPP. De tunnelbeheerder evalueert significante voorvallen in de tunnels.

[18] Zie voor nadere informatie de toelichting op de "Instructiekaart WIS/OVD-RWS" bij "Korte informatie ten aanzien van voorvallen op coördinatieniveau fase 1 van het Crisisplan Rijkswaterstaat" en "Geef tunnel vrij".

Toelichting instructiekaart WIS en OVD-RWS

Onderstaande tekst dient als naslagwerk voor de betreffende medewerkers.

In de toelichting op het werk van de c-WVL zijn belangrijke zaken vermeld die ook van belang zijn om te weten voor WIS/OvD-RWS. Dit moet door de WIS/OVD-RWS gekend worden om goed te kunnen samenwerken met de (c)WVL en de hulpverleningsdiensten (HD). Het is nodig hier eerst kennis van te nemen alvorens de eigen toelichting te lezen. Omgekeerd dienen de WVL en c-WVL kennis genomen te hebben van de onderhavige toelichting voor de WIS en OVD-RWS.

Korte informatie ten aanzien van voorvallen op coördinatieniveau fase 1 van het Crisisplan Rijkswaterstaat.
Alvorens (de) stappen van de instructiekaart zelf nader toe te lichten, wordt hieronder eerst in een notendop informatie gegeven over dit thema. De meeste informatie is hierna ook verwerkt in de toelichting op enkele stappen van de instructiekaart zelf.

Bij calamiteiten/ernstige incidenten, ernstige storingen en ernstig falen van de constructie/infra, die effect hebben op de omgeving en/of waarbij coördinatie nodig is op de incidentlocatie, wordt de OVD-RWS (conform opschalingscriteria) door de WVL gealarmeerd en gaat de OVD-RWS ter plaatse. In dat geval is de OVD-RWS *bij/vanuit* RWS verantwoordelijk voor de operationele leiding en coördinatie van het voorval (zowel in het brongebied als in het direct aangesloten effectgebied). De OVD-RWS draagt hiermee bij/ vanuit RWS de verantwoordelijkheid over het incident[19]. In voorkomende gevallen kan de OVD-RWS, mede aan de hand van de opschalingscriteria, kiezen voor coördinatie op afstand.
De OVD-RWS kan voor gewenste bijstand en advies de regiopikethouder van RWS WNN benaderen, die hiertoe via een bellijst (regionale) deskundigheid kan mobiliseren. De WVL kan de OVD-RWS faciliteren met het bereiken van het regiopiket.
De OVD-RWS kan op basis van het beeld van het voorval bepalen of opschaling naar fase 1 voldoende is of om, via de technisch voorzitter van het landelijk Crisisteam Rijkswaterstaat (CT-RWS), de beslisser van het CT-RWS te adviseren verder op te schalen naar coördinatieniveau fase 2.
De OVD-RWS is bevoegd de tunnel vrij te geven als is opgeschaald naar coördinatieniveau fase 1. Als opgeschaald is naar coördinatieniveau fase 2 bepaalt de beslisser van het CT-RWS of de tunnel weer open mag. Deze communiceert dit met de OVD-RWS en deze informeert de c-WVL. Wanneer is opgeschaald naar coördinatieniveau fase 2 blijft de OVD-RWS bij/vanuit RWS verantwoordelijk voor de operationele leiding ter plaatse.
Bovenstaand proces is weergegeven in het schema in bijlage 5 "Beslis- en bevoegdhedenschema: Sluiten, openen en open houden tunnels bij falen en calamiteiten".

Toelichting instructiekaart

Ga naar locatie

- Bij (vermoeden van) Brand en/of gevaarlijke stoffen betreft dit de opstelplaats bij de ondersteunende buis die in dit plan daarvoor is aangewezen. Je gaat de tunnel (noch de ondersteunende buis noch de incidentbuis) niet in. Je mag pas de ondersteunende buis in als de hoogst-leidinggevende van de brandweer hier het "sein veilig" voor gegeven heeft. Ook voor het benaderen van de incidentbuis dient eerst een "sein veilig" te zijn afgegeven door de hoogst-leidinggevende van de Brandweer.
- Bij een ernstige aanrijding mag je direct de ondersteunende buis in en als je het eerst ter plaatse bent mag je via de ondersteunende buis ook de verkenning uitvoeren in de incidentbuis, eventueel ondersteund door ambulancemedewerkers als die eveneens gelijktijdig ter plaatse zijn. Indien Brandweer of Politie ter plaatse zijn, dan voeren zij de verkenning uit (Brandweer > Politie). Als je zelf de verkenning hebt uitgevoerd en Brandweer en/of Politie komen daarna ter plaatse dan draag je de bevelvoering aan hen over. Directe benadering van de incidentbuis door overige hulpverleningsdiensten mag na toestemming van de hoogst-leidinggevende ter plaatse (Brandweer>Politie > OVD-RWS/Wis) of indien de betreffende hoogst-leidinggevende nog niet ter plaatse is – na toestemming van de wel aanwezige bevelvoerder van de betreffende hulpverleningsdienst.

[19] De eindverantwoordelijkheid ligt bij de tunnelbeheerder (HID) van de RWS-regio waar het incident zich afspeelt.

- Bij een te hoog voertuig kan de WIS opgeroepen worden om het te hoge voertuig op te meten op de hiervoor beschikbare opstelplaats.
- Bij betoging/vandalisme kan de WIS pas de tunnel in na toestemming van de hoogst-leidinggevende van de HD (de OVD-Politie). De WIS kan hierop wachten bij de opstelplaats van de incidentbuis.
- Voetgangers en fietsers worden aangehouden en opgevangen door de politie. De WIS kan wel de tunnel in om de voetganger/fietser te observeren, maar blijft in de auto. De voetganger/fietser krijgt zijn veiligheidsinstructies van de WVL (via de omroepinstallatie).
- Bij een dier in de tunnel kan de WIS wel de gesloten tunnelbuis inrijden om het dier te lokaliseren voor de dierenambulance. Niet zelf het dier afvoeren. Blijf in de auto.
- Bij een bommelding gaan de WIS en de OVD-RWS naar de opstelplaats bij de ondersteunende buis.
- Ingeval van een spookrijder zal de WVL deze indien mogelijk tot stoppen dwingen door de afsluitboom neer te laten. In overleg met de WVL dient bepaald te worden naar welke locatie de WIS zich moet begeven en wat de meest veilige route is (mogelijk via het onderliggend wegennet) om deze te bereiken. Dit zal per tunnel verschillen. De spookrijder kan hier mogelijk worden opgevangen en aan de politie worden overgedragen (mocht deze nog niet aanwezig zijn). De kans bestaat dat een spookrijder onder invloed van alcohol en/of drugs handelt. Houd dus altijd rekening met de eigen veiligheid en benader de spookrijder voorzichtig. Wacht bij twijfel op de politie.
- Bij de meeste andere voorvallen rijdt de WIS de tunnel in naar de plaats waar het voorval heeft plaatsgevonden.

Ontvang briefing WVL

- Bij een (Vermoeden) van Brand en/of Gevaarlijke stoffen zal de aandacht van de WVL in eerste instantie uitgaan naar het briefen van de bevelvoerder van de verkennende eenheid van de Brandweer (hierbij wordt bij de Gaasperdammertunnel gebruik gemaakt van het hulpdienstpaneel aan het begin van de tunnelbuis). De WIS/OVD-RWS wacht bij de opstelplaats tot de brandweer de hulpverleners brieft over het plan van aanpak.
- Bij een Ernstige aanrijding wordt de eerst aangekomene van de hulpverleningsdiensten gebriefd door de WVL. Dit kan ook de WIS/OVD-RWS zijn. Alle hulpverleningsdiensten en de WIS/OVD-RWS hebben toegang tot de ondersteunende buis. De eerst aangekomene voert ook de verkenning uit (dat kan ook de WIS/OVD-RWS zijn) en zorgt ervoor dat de overige hulpverleningsdiensten geïnformeerd worden over de toestand in de incidentbuis.
- In de meeste overige gevallen zal de WVL de WIS/OVD-RWS voorzien van de laatste informatie tijdens het aanrijden of bij aankomst bij de tunnel.

Stel voorval veilig

- De WVL zal al naar gelang de veiligheidssituatie een keus gemaakt hebben om:
  - op de calamiteitenknop te drukken (Maatregel I en II).
  - de incidentbuis af te sluiten (Maatregel III).

o de incidentrook waar het voorval staat af te kruisen en een snelheidsmaatregel te zetten op de ernaast gelegen vrije strook én aanvullend de incidentbuis af te sluiten (IV), of
o de incidentrook waar het voorval staat af te kruisen en een snelheidsmaatregel te zetten op de ernaast gelegen vrije strook (V) .[20]

- Bij de voorvallen onder I en II zal beveiliging afhangen van het aanvalsplan dat de HD inzetten.
- Bij voorvallen onder III is de Richtlijn eerste veiligheidsmaatregelen bij verkeersincidenten (REVI) alleen van toepassing als bijvoorbeeld een te hoge vrachtwagen op de vluchtstrook moet gaan staan.
  - In de regel zal een te hoog voertuig door de WVL naar de opstelplaats voor te hoge voertuigen zijn gepraat.
  - Check als het voertuig te hoog is of het eventueel kan zakken tot onder de 4.00 meter. In dat geval mag het voertuig zijn weg vervolgen via de tunnelbuis.
  - Stem bij een te hoog voertuig altijd af met de WVL wat er moet gebeuren. Het kan zijn dat de politie de chauffeur komt bekeuren. Geef in alle gevallen het kenteken van het te hoge voertuig door aan de WVL.

[20] In tunnels met meer dan twee rijstroken kan de WVL ervoor gekozen hebben om twee rijstroken af te sluiten als dit het gevaar voor mensen neutraliseert.

  - Zodra alles is afgehandeld vraagt de WIS aan de WVL om de opstelplaats te openen zodat het te hoge voertuig zijn weg via een alternatieve route kan vervolgen.
- De voorvallen onder IV en V worden beveiligd volgens de REVI.

Stem Plan van Aanpak (PvA) af met HD
- De hoogst leidinggevende van de HD (Brandweer > Politie > Wis/OVD-RWS) bepaalt bij incidenten en calamiteiten het aanvalsplan:
  a. Niveau van Gecoördineerde Regionale Incidentbestrijdings Procedure (GRIP).
  b. Inrichting Commando Plaats Incident (CoPI) [21].
  c. Taakverdeling en wijze van communicatie.
- De OVD-RWS of de WIS (indien of zolang geen OVD-RWS aanwezig is) leveren hun inbreng in het PvA, met name expertise op het gebied van tunnelveiligheid, incident management en operationeel verkeersmanagement.
- De OVD-RWS en WIS stemmen hun onderlinge taakverdeling af. Op de instructiekaart zijn de activiteiten gemarkeerd die de OVD-RWS bij voorkeur aan zichzelf voorbehoudt.
  Als er is opgeschaald tijdens de afhandeling van het voorval geeft de OVD-RWS leiding aan de WIS.

Stem Plan van Aanpak (PvA) af met WVL
- De OVD-RWS of de WIS (indien of zolang geen OVD-RWS aanwezig is) communiceert het PvA met de WVL.
- Opdrachten van de hoogst-leidinggevende van de HD aan de WVL lopen via de OVD-RWS of de WIS als de OVD-RWS (nog) niet aanwezig is[22].
- De OVD-RWS/WIS geeft een eerste inschatting van de afhandelingsduur van het voorval af.

Sluit eventueel buis in verband met veilig werken
- Als het mogelijk is het voorval af te handelen zonder de tunnelbuis te sluiten, heeft dat de voorkeur. Echter, het moet wel veilig zijn voor de WIS en de bergers.
- De WIS kan daarom te allen tijde aan de WVL verzoeken de tunnelbuis waarin het voorval heeft plaatsgevonden te sluiten als de afhandeling van het voorval (het verwijderen van verloren lading, afslepen van voertuigen, etc.) gevaar voor mensen oplevert (bergers, calamiteitenaannemers, weggebruikers, etc.).
- Bij een los voorwerp dat verwijderd kan worden door de WIS ligt het toepassen van de huidige REVI in het geval van zware voorwerpen minder voor de hand. De wagen van de WIS moet (voor)bij het voorwerp staan om het te kunnen inladen, en kan niet op 70 meter afstand in *fend off* staan. De WIS zou dan deze afstand met het voorwerp moeten lopen. In dit geval wordt de tunnel bij aankomst van de WIS op diens verzoek (kort) gesloten om hem de gelegenheid te geven het voorwerp in te laden.
- Als de WIS bij een morsing twijfelt over de aard (en het gevaar) van de vloeistof kan hij de brandweer om assistentie vragen voor nader onderzoek. Ook in dat geval wordt de tunnelbuis afgesloten.

Ondersteun hulpverleningsdiensten in CoPI of in motorkapoverleg (MKO)
- De OVD-RWS of de WIS (zolang de OVD-RWS nog niet aanwezig is) neemt deel aan het CoPI (indien dit is ingesteld) of het motorkapoverleg en levert daar inbreng bij het afwikkelen van het voorval.
- De OVD-RWS/WIS treden op als liaisons tussen de HD en de WVL.
- De OVD-RWS/WIS overleggen met de HD over versnelling van de voortgang van de hulpverlening/ werkzaamheden i.v.m. doorstroming van het verkeer.

Ondersteun HD
- De OVD-RWS/WIS dragen er zorg voor dat de politie ondersteund wordt bij het opvangen van weggebruikers en het werken samen in het controleren van de tunnel en de vluchtroute(s) (Middentunnelkanaal /Veilige Ruimtes)[23] op vluchters.

---

[21] Als geen CoPI wordt ingesteld vindt multidisciplinaire afstemming plaats (of kan dit plaatsvinden) via in te stellen motorkapoverleg (MKO). Zie desgewenst voor informele oriëntatie op motorkapoverleg: https://nl.wikipedia.org/wiki/Motorkapoverleg.

[22] Zolang er geen WIS of OVD-RWS aanwezig is op de plaats van de calamiteit of het incident lopen de opdrachten aan de WVL via de meldkamer (OC).

- De OVD-RWS/WIS hebben namens RWS de coördinatie over het vrijmaken van de rijstroken, uiteraard in afstemming met het aanvalsplan van de HD. In geval er geen HD aanwezig zijn handelen de OVD-RWS/WIS zelfstandig af.

Informeer WVL
- Houd de WVL bij calamiteiten en complexe incidenten op de hoogte van de voortgang van de afhandeling en geef hierbij regelmatig een update van de restduur.

FASE 3: HERSTELLEN NORMALISEREN (stap 6), LOGGEN EN REGISTREREN (stap 7)

Stem voorwaarden vrijgeven ondersteunende buis en (rijstroken) incidentbuis af
- Zodra de hulpverlening is afgelopen is het zaak de normale situatie zo snel mogelijk weer te herstellen. De OVD-RWS of WIS (met toestemming van de OVD-RWS) maakt met de hoogst-leidinggevende van de hulpverleningsdiensten afspraken over de voorwaarden waaronder de ondersteunende buis, rijstroken in de incidentbuis en uiteindelijk de gehele incidentbuis kunnen worden vrijgegeven.

Stem overdracht bevelvoering af
- Zodra de taak van de hulpverleningsdiensten erop zit zal de hoogst-leidinggevende van de HD de bevelvoering overdragen aan RWS (bij calamiteiten zal dit dat aan de OVD-RWS zijn en bij gewone incidenten aan de WIS) en zal debriefing plaatsvinden.

Roep calamiteitenaannemer op/Stem Plan van Aanpak met Berger en Calamiteitenaannemer af
- Bij duidelijke schade aan de tunnel, tunnel technische installaties (TTI), geleiding, wegdek, etc. wordt de betreffende calamiteitenaannemer opgeroepen.
- Organiseer het bergen in afstemming met de berger en de calamiteitenaannemer en houd daarbij rekening met de verschillende bergingskeuzes (normaal/versneld/uitgesteld).

Maak evt. 1 rijstrook vrij
- Probeer zo snel mogelijk een rijstrook vrij te maken. De WVL zal dit - indien mogelijk – ondersteunen met MTM. Voorwaarde is dat dit veilig kan (met afkruising van de incidentstrook en beveiligd door de WIS en een snelheidsmaatregel van 50 km op de ernaast gelegen vrije rijstrook; verder afhandeling incident op voldoende afstand van de aslijn met de vrije rijstrook en conform de gestelde voorwaarden door de hoogst-leidinggevende van de HD). Ook hier moet dus de Richtlijn eerste veiligheidsmaatregelen bij verkeersincidenten (REVI) in acht worden genomen.

Leid het opgesloten verkeer weg
- Organiseer dat weggebruikers die voor de tunnel (c.q. voor het incident in de tunnel) opgesloten zijn, worden weggeleid als vrijmaken van een rijstrook in de tunnel onmogelijk is (zie pagina 13 voor de twee mogelijkheden). (NB: Dit kan overigens al in een eerder stadium als duidelijk is dat de blokkade niet binnen 45 minuten is opgeheven).

Laat noodzakelijke tests TTI uitvoeren
- Organiseer het uitvoeren van reparaties in overleg met de calamiteitenaannemer/ onderhoudsaannemer en evt. het testen van TTI in overleg met de WVL.

Inspecteer Hulpposten
- Inspecteer de hulpposten die (vermoedelijk) gebruikt zijn bij het voorval (laat evt. herstel uitvoeren, aanvullingen verrichten, etc.).

Schouw Tunnelbuis
- Schouw of de tunnelbuizen vrij zijn. Voordat de OVD-RWS of de WIS (bij afwezigheid OVD-RWS) de tunnel kan vrijgeven maakt hij gebruik van de checklist schouwen.

[23] Bij de Gaasperdammertunnel bestaat de vluchtroute tussen de parallel- en hoofdbuis in de richting Diemen resp. Holendrecht uit de drie MTK-compartimenten, de onderdoorgangen bij de toe- en afritten van/naar de S112 in de parallelbuizen en de ondersteunende buis.

Geef tunnel vrij

- Bij voorvallen op coördinatieniveau fase 1 beslist de OVD-RWS over het (al dan niet gefaseerd) weer vrijgeven van de tunnel.

  NB: wanneer is opgeschaald naar coördinatieniveau fase 2 bepaalt de beslisser van het landelijk Crisisteam RWS (CT-RWS) of de tunnel weer open kan. De OVD-RWS blijft in dit geval bij/vanuit RWS verantwoordelijk voor de operationele leiding ter plaatse.
  Bij coördinatieniveau fase 2 zal de OVD-RWS aan de beslisser CT-RWS toestemming moeten vragen om de tunnel weer vrij te geven voor het verkeer. Dit geldt ook in situaties met ernstige storingen waarbij besluitvorming nodig is over openhouden/sluiten indien hersteltermijnen overschreden (dreigen te) worden overschreden. De WVL houdt de OVD-RWS van dit laatste op de hoogte en de OVD-RWS stemt af met CT-RWS. De beslisser van CT-RWS besluit dan dus over het open(houden) of dicht gaan en onder welke voorwaarden en aanvullende compenserende en/of risico reducerende maatregelen.
  Dit proces is (eveneens) weergegeven in bijlage 5 "Schema beslis- en bevoegdheden: Sluiten, openen en open houden tunnels bij falen en calamiteiten".

- Informeer WVL dat de tunnelbuizen vrijgegeven kunnen worden.
- Het is mogelijk dat eerst de ondersteunende tunnelbuis wordt vrijgegeven en later de buis waar de calamiteit heeft plaatsgevonden.

Vul logging aan

- De WVL maakt een logging en deze kan door de OVD-RWS/WIS aangevuld worden met extra informatie.
- De c-WVL zal in overleg met de OVD-RWS/WIS bepalen of een voorval als significant aangemeld moet worden opdat het in aanmerking kan komen voor evaluatie. De evaluatie van significante voorvallen gebeurt door de tunnelbeheerorganisatie RWS WNN.

Overige situaties

Handelingen bij brand in de Verkeerscentrale (VC)

- Bij Brand in de VC worden de tunnels (waar het groepscommando calamiteitenbedrijf zelfstandig werkt) niet afgesloten omdat afsluiten van alle tunnels een verkeersinfarct op het netwerk veroorzaakt.
- Er wordt indien mogelijk (dit is afhankelijk van de eigen veiligheid van het personeel van de VC) een snelheidsmaatregel (70 km/u) in en bij de tunnel getroffen.
- De (c)WVL's en het overig personeel van de VC verlaten de VC (conform het Ontruimingsplan van de VCNWN) en er wordt overgegaan tot lokale bediening van de tunnels. Zolang lokale bediening nog niet is geactiveerd, is er waar mogelijk extra oogtoezicht van weginspecteurs van afdelingen Operationeel Verkeer Randstad van RWS VWM. Bovendien zal, gedurende de tijd dat de WVL's onderweg zijn om lokaal te gaan bedienen, de veiligheid van de weggebruiker ondersteund worden doordat in een aantal incidentsituaties (bijvoorbeeld incident met brand) de Velsertunnel, Coentunnel, Zeeburgertunnel, Schipholtunnel en Gaasperdammertunnel automatisch naar calamiteitenbedrijf zullen schakelen. De Wijkertunnel kent geen automatisch calamiteitenbedrijf, maar deze tunnel ligt op loopafstand van de VC, waardoor lokale bediening binnen zeer korte tijd zal kunnen starten als er voldoende bezetting is.

Beknelling/Valpartij tijdens onderhoud

- Afhandeling van dergelijke incidenten is vastgelegd in het V&G-plan van de onderhoudsaannemer;
- De (c)WVL stemt af met de hulpverleningsdiensten (HD) hoe deze de gewonde(n) het beste kunnen bereiken en stemt de initiële verkeersmaatregelen (indien nodig) en de maatregelen TTI hierop af. De VC schakelt de OVD-RWS in.

Brand met ongeval in de Dienstgang
☐ De medewerkers van de onderhoudsaannemer melden deze situatie aan de VC van RWS en de Meldkamer (OC). De VC schakelt de OVD-RWS in.
Hulpverlening vindt in principe plaats via Dienstgebouw op de tunnel.
☐ De WVL kan gevraagd worden een tunnelbuis af te sluiten indien dit nodig is voor het afvoeren van eventuele slachtoffers.

Tunnel ter beschikking van het bevoegd gezag
- Dit zijn situaties waarbij het bevoegd gezag de tunnel ter beschikking vraagt: bijvoorbeeld in verband met evacuatie van het omliggende gebied, bedreiging door incidenten elders of een benodigde vrije doorgang van hulp- en nooddiensten.
- De (c)WVL beoordeelt of de aanvrager geautoriseerd is;
- De (c)WVL vraagt naar de reden van de ter beschikking stelling i.v.m. eventuele additionele maatregelen;

NB: Er worden in geen enkel geval tunnels gesloten om een aanhouding te laten verrichten door de politie;

Ernstige storing TTI en andere oorzaken technisch falen tunnelveiligheid
De te treffen maatregelen bij Ernstige storing TTI en andere oorzaken van technisch falen tunnelveiligheid zijn in de vigerende versie van het document Regionale Faaldefinities wegtunnels RWS WNN en VCNWN, beschreven op basis van de Faaldefinities uit de LTS (Systeemontwerp RWS Tunnelsysteem).
Het in bijlage 5 opgenomen beslis- en bevoegdhedenschema heeft (tevens) betrekking op tunnelsluiting naar aanleiding van storingen.

Deel IV Afspraken met hulpverleningsdiensten (HD)

Deel IV bevat afspraken met de HD (procedures) specifiek voor wegtunnels in beheer bij RWS WNN.
De afspraken zijn principe-afspraken: op basis van de lokale omstandigheden/inschatting bij afhandeling van een incident kunnen er andere beslissingen worden genomen.

Procedures hulpverleningsdiensten (HD)

Melding van voorvallen
Meldingen van incidenten in de tunnel kunnen op twee manieren binnenkomen bij de gemeenschappelijke meldkamer van de HD (Meldkamer (OC)):
1. via een (c)WVL die vanuit de VC de Meldkamer (OC) belt;
2. via een weggebruiker(s) die direct 112 belt (bellen).

Bij beide manieren van melding vraagt de centralist Meldkamer (OC) naar het type voorval. Deze informatie is van belang voor:
- de centralist Meldkamer (OC) om te bepalen welke eenheden van de HD gealarmeerd en geïnformeerd.
- beeldvorming over het incident door de te alarmeren eenheden en de wegverkeersleider (WVL) in de Verkeerscentrale (VC).

De WVL van de VC informeert de centralist Meldkamer (OC) over:[1]
- exacte locatie: wegnummer, hectometeraanduiding (hm, Li/Re, letter), rijstrook, naam tunnel, tunnelbuis, vluchtdeurnummer (voor verkenning), hulppost.
- aard van het voorval; wat is er gebeurd?: is er sprake van brand, een hoog energetisch ongeval of ander voorval? (classificatie van het voorval conform de standaard indeling bedienprocessen).
- getroffen initiële maatregelen/stroken nog vrij.
- indicatie van mogelijke slachtoffers: doden/gewonden/personen onwel/locatie en aantal letselslachtoffers (w.o. ook in middentunnelkanaal (MTK) /veilige ruimte).*
- indicatie van aantal mensen in incidentvoertuig(en) achtergebleven en (aantal) immobiele slachtoffers.*
- aantal betrokken voertuigen: personenauto's, vrachtauto's, motor, tankwagen(s) wel/niet rolbaar.
- eventueel in de tunnel aanwezig vervoer van gevaarlijke stoffen: bij incident betrokken vrachtauto('s); evt. kenteken, stofnummer, gevaarnummer en of het een elektrisch voertuig betreft;*
- eventuele zichtbare lekkage van (gevaarlijke) vloeistoffen, uit welk voertuig?;*
- gewenste inzet van hulpverleningsdiensten.
- informatie over stremmingen, verkeerssituatie, beste aanrijdroute en opstelplaats, gevarenzone, bereikbaarheid.

* De informatie die de WVL aan de centralist Meldkamer (OC) verstrekt is indicatief: de WVL communiceert wat hij op de camerabeelden ziet.

NB: Het tunnelsysteem van de Gaasperdammertunnel activeert bij brand en/of gevaarlijke stoffen en bij ernstige aanrijding[2] een beveiligde, geautoriseerde beeldverbinding met de MK (verbinding komt automatisch tot stand als de tunnel in calamiteitenbedrijf gaat). Personeel van de Meldkamer (OC) kan dan meekijken met het beeld dat de WVL heeft geactiveerd. Dit beeld wordt ook getoond op het

[1] Deze informatie is vaak niet allemaal tegelijk voorhanden en ontwikkelt zich gedurende de (afhandelings-)tijd in het totaalbeeld. Goede en regelmatige communicatie en afstemming tussen WVL, centralist-MK en de operationele eenheden van de HD en RWS op de weg, in het bijzonder wanneer in eerste instantie gegeven belangrijke informatie wijzigt of er nieuwe informatie beschikbaar komt, is belangrijk. Dit draagt bij aan (het op snelle wijze verkrijgen van) een zo eenduidig mogelijk beeld van het voorval en de effecten ervan en om op kritische punten juist en slagvaardig te kunnen handelen.

[2] Ernstige aanrijding is gedefinieerd als een ongeval met hoog energetisch letsel waarbij de rijbaan is versperd (vermoedelijk is geen slagvaardige hulpverlening mogelijk via de incidentbuis). Een hoog energetisch ongeval is voor de WVL identificeerbaar aan de hand van de schouwkaart IM in combinatie met camerawaarneming. Zie voor Schouwkaart IM: https://www.incidentmanagement.nl/downloadspublicaties/2283182.aspx

Hulpdienstpaneel (HDP) bij de Gaasperdammertunnel.[3] Op verzoek van de Meldkamer (OC) kan deze ook over tunnelbeelden beschikken bij een bommelding of een betoging/vandalisme (de WVL brengt handmatig verbinding tot stand).

Alarmering door Meldkamer (OC) van eenheden en omgevingspartijen

- De Meldkamer (OC) alarmeert de benodigde eenheden voor de eerste inzet op basis van de eigen inzetvoorstellen behorende bij de gegevens van de melding.
- De Meldkamer (OC) informeert/waarschuwt bij een calamiteit/incident in de tunnel met effect(en) op de veiligheid van de omgeving (door bv. brand/rook in de tunnel) omgevingspartijen, zodat deze organisatie specifieke maatregelen kunnen treffen.

Aanrijden

Algemeen

- Het wegennet wordt in de ingestelde rijrichting gebruikt.
- Er wordt zoveel mogelijk gebruik gemaakt van de vastgestelde aanrijdroutes.
- Uitgangspunt bij brand/gevaarlijke stoffen en bij ernstige aanrijding is dat deze via de ondersteunende buis worden benaderd: zie aanrijdmatrix op pagina 3 (figuur 1);
- De Meldkamer (OC) meldt de specifieke inzet van de politie/brandweer en/of ambulance aan de VC.

Bij brand en/of gevaarlijke stoffen en/of bij ernstige aanrijding in de tunnel (bij I en II)[4]

- De HD begeven zich naar de (afgesproken) opstelplaats.
- De bevelvoerder van de verkennende eenheid van de HD[5] ontvangt via de intercom bij de afsluitboom of calamiteitendoorsteek de laatste informatie van de WVL over de situatie/veiligheid in de tunnelbuizen. Bij de Gaasperdammertunnel ontvangt de verkennende eenheid van de brandweer de informatie via het HDP.
  De WVL meldt/herhaalt bij de infovoorziening het nummer van de vluchtdeur in de ondersteunende buis, die de verkennende eenheid van de HD kan gebruiken om de incidentbuis te betreden voor verkenning van de incidentbuis.

Overige situaties in de tunnel (type III en IV)

Bij alle overige situaties gaan de HD (Politie en Ambulance) na contact met de Meldkamer (OC) direct naar Plaats Incident. De (c)WVL kan hierbij adviseren via de Meldkamer (OC) volgens de aanrijdmatrix (zie figuur 1 op pagina 3).

Verkenning

Bij (vermoeden van) brand en/of gevaarlijke stoffen

- Via de vluchtdeur vanuit de ondersteunende tunnelbuis (bovenstrooms van het voorval) voert de verkennende eenheid van de Brandweer de verkenning uit; de verkenning kan ook eerst op afstand plaats vinden via het Hulpdienstpaneel indien de tunnel daarover beschikt.
- Bij vermoeden van brand of de aanwezigheid van gevaarlijke stoffen, als lading van een vrachtauto, kunnen de hulpverleningsdiensten de tunnel alleen met aanvullende maatregelen, zoals ademlucht, veilig betreden. Het kan dan ook voorkomen dat de ondersteunende buis al veilig is voor hulpverleners, maar de incidentbuis nog niet. Alle overige hulpverleningsdiensten wachten tot de bevelvoerder van de verkennende eenheid van de brandweer de incidentbuis heeft verkend via de ondersteunende buis of het hulpdienstpaneel voor de tunnelingang. Nadat de bevelvoerder van de brandweer het "Sein Veilig" heeft afgegeven mogen de overige hulpverleningsdiensten de incidentbuis betreden. Sein Veilig wordt alleen toegepast bij brand en/of gevaarlijke stoffen en wordt altijd per buis afgegeven door de brandweer.

[3] Van de Rijkstunnels die bij RWS WNN in beheer zijn is uitsluitend de Gaasperdammertunnel uitgerust met een beeldverbinding met de Meldkamer (OC) en met Hulpdienstpanelen.

[4] Bij brand/gevaarlijke stoffen drukt de WVL de calamiteitenknop in en activeert hij het evacuatiebedrijf van de tunnel. Bij ernstige aanrijding drukt de WVL de calamiteitenknop in.

[5] Bij brand en/of gevaarlijke stoffen en ernstige aanrijdingen met beknelling zal dit de verkennende eenheid van de brandweer zijn. Bij ernstige aanrijdingen waarbij geen brandweer is ingezet is dit de politie.

Bij ernstige aanrijding (II)

• Bij een ernstige aanrijding kan een gestremde rijbaan ervoor zorgen dat de hulpverlening niet via de incidentbuis bij het incident kan komen en zich 'vastrijdt'. Om dit te voorkomen is de inzet in de incidentbuis via de ondersteunende buis noodzakelijk. De verkenning (m.b.v. het hulpdienstpaneel of ter plaatse via de ondersteunende tunnelbuis) wordt uitgevoerd door de bevelvoerder van de eerst aangekomen eenheid van de brandweer of politie. Ook de weginspecteur of OVD-RWS kan bij een ernstige aanrijding optreden als "verkennende eenheid HD" als Brandweer en Politie nog niet ter plaatse zijn. Deze bevelvoerder/hoogst leidinggevende bepaalt in samenspraak met de overige hulpverleningsdiensten de aanvals- en aanrijdstrategie en geeft de overige diensten toestemming om de incidentbuis te betreden. Als er bij een ernstige aanrijding een rijstrook vrij is gekomen vóórdat de hulpverleningsdiensten de tunnel hebben bereikt, zal de wegverkeersleider in afstemming met de meldkamer van de hulpverleningsdiensten de ernstige aanrijding afschalen. De hulpverleningsdiensten benaderen het incident dan alsnog via de incidentbuis.

NB. Bij brandbestrijding altijd met inachtneming van de blaasrichting van de ventilatoren.
De (c)WVL kan hierbij adviseren via de MK.

Overige situaties m.b.t. doorstroming in de tunnel

- De Politie is coördinerend/leidend bij verstoring van de openbare orde in de tunnel betoging, vandalisme, bommelding, voetgangers/fietsers/dieren (waarbij ook de dierenambulance wordt ingezet) en een ongeval met (vermoeden van) letsel.

Figuur 1. Aanrijdmatrix

Aanrijd matrix	**I**	**II**	**III**	**IV**	**V**
	Tunnelbuizen afsluiten met calamiteitenknop + activeer evacuatiebedrijf	**Tunnelbuizen afsluiten met calamiteitenknop**	**Incidentbuis sluiten**	**Incidentstrook afkruisen + incidentbuis sluiten**	**Incidentstrook afkruisen**
Initieel beide rijrichtingen afgesloten					
Coentunnel **Zeeburgertunnel** **Velsertunnel** **Schipholtunnel** **Wijkertunnel**	ondersteunende buis [A]	ondersteunende buis [A]	incidentbuis	incidentbuis	incidentbuis
Initieel incidentrichting afgesloten					
Gaasperdam-mertunnel PLi, HLi, HRe, Pre	ondersteunende buis [A,B]	ondersteunende buis [A,B]	Incidentbuis [A]	Incidentbuis	incidentbuis
Initieel alle tunnelbuizen afgesloten					
Gaasperdam-mertunnel Wi [6]	HRe	HRe	Incidentbuis [A]	incidentbuis	incidentbuis

[A] **Na toestemming van de politie is tegengesteld aanrijden mogelijk voor de hulpdiensten.**

[B] Bij de Gaasperdammertunnel ligt de ondersteunende buis in de rijrichting van de incidentbuis. Let op! De overige buizen zijn nog in verkeer.

[6] De wisselbuis in de Gaasperdammertunnel is nog niet opengesteld voor het verkeer.

Binnenrijden hulpverleningsdiensten

Naast de normale Incident Management procedures gelden de volgende aanvullende aanbevelingen:

- Vraag voordat de tunnel (incident- of ondersteunende buis) in wordt gegaan indien nodig informatie aan/via de Meldkamer (OC) of (via intercom/HDP) aan de VC over de situatie/veiligheid in de tunnel (*controlemoment*).
- Bij inrijden tunnelbuis zwaailichten aan, sirene uit.
- Rijd langzaam en stel de voertuigen in rechte lijn op, essentieel hierbij is:
  - houd rekening met de mogelijkheid van weggebruikers (voetgangers/vluchters) op de rijbaan;
  - stel de hulpverleningsvoertuigen op aan de zijde van de vluchtdeuren; en
  - zorg dat in de tunnelbuis genoeg ruimte blijft voor het passeren van hulpverleningsvoertuigen en voor afvoer van gewonden.
- Plaats géén voertuigen vóór vluchtdeuren: voorkom dat het gebruik van vluchtdeuren wordt belemmerd voor weggebruikers/vluchters en voor de afvoer van gewonden.
- Bij stilstand voertuig het zwaailicht uit wanneer veiligheid hulpverleners en weggebruikers is geborgd (voorkom hinderlijke reflecties, waaronder reflecties op camera).
- Aan begin tunnel altijd een voertuig in de *fend off* positie positioneren, met de optische signalen aan;
- Motor uitzetten indien mogelijk (voorkom geluidshinder en luchtverontreiniging).
- Bergers wachten op de hiervoor afgesproken locatie (wrakkenplaats) op nadere instructies.

NB: de verbindingsmiddelen van de hulpverleningsdiensten (C2000) worden ondersteund in de tunnels.

Bij (vermoeden van) brand/gevaarlijke stoffen

- Nadat de ter plaatse aanwezige bevelvoerder van de brandweer hiervoor "sein veilig" heeft gegeven mogen de andere hulpverleningsdiensten en de WIS en OVD-RWS de incidentbuis of ondersteunende buis ingaan.
- Sein Veilig wordt afgegeven per buis (incidentbuis en ondersteunende buis).

Bij ernstige aanrijding:

- Ook de weginspecteur of OVD-RWS kan bij een ernstige aanrijding optreden als "verkennende eenheid HD" als Brandweer en Politie nog niet ter plaatse zijn. Deze bevelvoerder/hoogst leidinggevende geeft dan de overige diensten toestemming om de incidentbuis te betreden.

NB: de verbindingsmiddelen van de hulpverleningsdiensten (C2000) worden ondersteund in de tunnels.

Operationele leiding

Algemene afspraken:

- Voor alle incidenten gelden de gangbare IM-procedures over bevelvoering tussen de HD onderling.
- De werkzaamheden van de OVD-RWS en de HD worden uitgevoerd onder het bevel van de hoogst-leidinggevende van de HD.
- De OVD-RWS maakt zich bekend bij de verantwoordelijke hoogst-leidinggevende of bevelvoerder van de HD ter plaatse en houdt contact.
- Alle communicatie tussen HD en Verkeerscentrale en visa versa loopt via de OVD-RWS ter plaatse (of via de weginspecteur als de OVD-RWS niet ter plaatse is). NB: indien of zolang geen RWS medewerkers ter plaatse zijn verloopt de communicatie tussen de HD en de VC via de Meldkamer (OC).
- Er wordt opgeschaald via de GRIP-procedure als een of meer OVD'en van de Brandweer, Politie, Ambulance en/of MK dit nodig achten. Zie ook Regionaal Crisisplan.
- Vanuit RWS neemt de OVD-RWS als liaison deel aan het CoPI.

Aanpassen verlichting, ventilatie, geluidbakens en geautomatiseerde omroepberichten
De ter plaatse aanwezige hoogst-leidinggevende van de HD kan tijdens de afhandeling van het voorval via de Meldkamer (OC) (of via de OVD-RWS/weginspecteur of in uiterste nood via de noodtelefoon bij slechte verbindingen) aan de WVL opdracht geven aanpassingen te verrichten t.a.v. de ventilatie en/of verlichting en/of tot het uitzetten van geluidbakens en geautomatiseerde omroepberichten zodra deze systemen geen functie meer hebben voor de zelfredzaamheid en hulpverlening. De WVL of OVD-RWS of (bij afwezigheid van de OVD-RWS) de weginspecteur (WIS) kan zelf aanpassingen voorstellen aan de hoogst-leidinggevende van de HD. Ventilatie, geluidbakens en geautomatiseerde omroepberichten kunnen zorgen voor geluidshinder. Ventilatie kan ook zorgen voor een lage gevoelstemperatuur of afkoeling.

Ontruiming/Evacuatie weggebruikers/Controle vluchtroutes
Afspraken:
- De politie is procesverantwoordelijke voor opvang van weggebruikers bij de verzamelplaats buiten de tunnel. De WIS faciliteert bij de eerste opvang.
  Opvang en begeleiding van weggebruikers zijn nodig om ervoor te zorgen dat evacuatie ordentelijk verloopt en bepaalde gegevens (door politie) geregistreerd kunnen worden. Bij langdurige opvang wordt het proces "Opvang en Verzorgen" geregeld via de in het Regionaal Crisisplan aangegeven procedure(s).
- Als de Brandweer t.p. van het incident is, is de bevelvoerder van de Brandweer verantwoordelijk voor het proces Verkenning op risico's (schouwen op brand, gevaarlijke stoffen, slachtoffers of gewonden e.d.). Daarbij dient extra aandacht te zijn voor controle van de vluchtroutes (Middentunnelkanaal / Veilige Ruimtes) op eventuele achterblijvers/vluchters;[7]
- Na de incidentbestrijding van de brandweer en goedkeuring om de incidentbuis te betreden, controleren de HD[8] (met eventuele ondersteuning van de OVD/RWS of WIS) of er (niet-gewonde) weggebruikers zijn achtergebleven in het Middentunnelkanaal / Veilige ruimte.[11]
- Als de Meldkamer (OC) bij ernstige aanrijding in voorkomend geval geen Brandweer heeft aangestuurd en ingezet naar het incident, dan spreken de hoogst-leidinggevende van de Politie en de OVD-RWS of (bij afwezigheid van de OVD-RWS) de WIS af wie (welke van) de vluchtroutes/veilige ruimtes controleert op eventueel achtergebleven (niet-gewonde) weggebruikers. [11]
- Bij incidenten waarbij geen HD zijn ingezet, controleert de WIS zo nodig, bijvoorbeeld als gebruik is gemaakt van vluchtdeuren, of er nog (niet-gewonde) weggebruikers/vluchters zijn achtergebleven in de vluchtroutes/veilige ruimte(s). [7]

NB: In het CBP en het Regionaal Crisisplan is het evacueren van mensen met een beperkte mobiliteit en gehandicapten en chronisch zieken niet apart beschreven. De HD zullen in voorkomend geval naar bevinden handelen.

Overdracht bevelvoering
- Wanneer de hoogst-leidinggevende van de HD (brandweer indien ingezet) het voorval heeft afgehandeld, wordt het gezag overgedragen aan de politie (voor eventueel uit te voeren (technisch/forensisch) sporenonderzoek).

Schouwen van de vluchtroutes op achtergebleven slachtoffers of gewonden is de verantwoordelijkheid van de brandweer in situaties waarin ademlucht noodzakelijk is. Anders is het een taak van de politie, met ondersteuning van de OVD-RWS (als er sein veilig is gegeven door de hoogst-leidinggevende van de HD en politie sporenonderzoek heeft verricht). De OVD-RWS kan dit mogelijk meenemen in zijn schouwronde, dan wel de in zijn opdracht door de WIS uit te voeren schouwronde.

Vrijgeven tunnel
- De OVD-RWS maakt met de t.p. aanwezige HD afspraken over de voorwaarden waaronder de rijstroken en tunnelbuizen (eventueel gefaseerd) weer kunnen worden opengesteld voor het verkeer.

[7] Let op: bij de Gaasperdammertunnel bestaat de vluchtroute tussen de parallel- en hoofdbuis in de richting Diemen resp. Holendrecht uit de drie MTK-compartimenten, de onderdoorgangen bij de toe- en afritten van/naar de S112 in de parallelbuizen en de ondersteunende buis.

[8] Indien ademlucht noodzakelijk is, wordt de controle door de brandweer uitgevoerd, in andere gevallen door de politie met ondersteuning van de OVD-RWS.

- De OVD-RWS is verantwoordelijk voor het gehele schouwproces van de tunnel door WIS en WVL. Herstel en test van de uitrusting kan onderdeel uitmaken van de schouw.
- De OVD-RWS beslist over het weer openstellen van de tunnel(buizen) – na eventueel nodig schadeherstel door de calamiteitenaannemer en testen van uitrusting e.d. – voor het verkeer.
- De VC informeert de Meldkamer (OC) over openstelling van de tunnel(buizen).

Nazorg
Bij eerste nazorg zijn zowel medewerkers van de HD als van RWS aanwezig. De overige nazorg is beschreven in plannen van de HD en gemeenten.

Toegang tot de dienstgebouwen
De toegang tot de dienstgebouwen van de verschillende tunnels in de veiligheidsregio Kennemerland is weergegeven op de bereikbaarheidskaarten van de brandweer Kennemerland. Deze bereikbaarheidskaarten zijn opgesteld in afstemming met RWS.
Coentunnel en Gaasperdammertunnel: deze tunnels hebben een sleutelkluis bij het dienstgebouw.

Bijlage: Begrippenlijst

De begrippenlijst op de volgende pagina's is in 2019 is vastgesteld in het NH-brede overleg wegtunnels, met dien verstande dat daarin uitsluitend de bij incidentafhandeling betrokken functionarissen van RWS, inclusief een korte beschrijving van hun functies, zijn opgenomen (en dus niet de uiteenlopende andere benamingen van functionarissen bij de andere wegtunnelbeheerders in Noord-Holland). De begrippenlijst wordt conform afspraak in genoemd overleg beheerd door de brandweer Kennemerland.

Begrippen incidentbestrijding in wegtunnels

Begrippenlijst

Functierollen tunnelbeheerder	
Begrip	**Toelichting**
Verkeerscentrale (VC)	Locatie waar toezicht wordt gehouden op het regionale wegennet in beheer van een wegbeheerder.
Wegverkeersleider (WVL)	Persoon die vanuit de verkeerscentrale toezicht houdt op verkeersdoorstroming, bedienen en bewaken van tunnels, het ondersteunen bij afhandelen van calamiteiten/incidenten en het verzorgen van informatie voor de weggebruikers.
Coördinerend Weg-verkeersleider (C WVL)	Persoon die tijdens een incident de processen en communicatie coördineert in de verkeerscentrale, terwijl de WVL zich richt op het calamiteiten/incident en de handelingen die daarbij nodig zijn.
Weginspecteur (WIS)	De functionaris die toezicht houdt op de weg en calamiteiten/incidenten op het wegennet afhandelt.
OVD-RWS	Bij complexe incidenten en calamiteiten komt de OVD-RWS ter plaatse en treedt op als liaison namens weg/tunnelbeheerder namens RWS.
Locatiebepaling	
Begrip	**Toelichting**
Incident (tunnel)buis	De tunnelbuis waar het incident zich heeft voorgedaan
Ondersteunende (tunnel)buis	De niet-incident tunnelbuis die door de hulpdiensten gebruikt wordt om een verkenning te doen in de incidentbuis.
Voor het incident / locatie	Locatie vanuit de rijrichting gezien voor het incident of specifiek benoemde locatie
Voorbij het incident / locatie	Locatie vanuit de rijrichting gezien na het incident of specifiek benoemde locatie
Bovenwinds / bovenstrooms	Locatie voor het incident met de ventilatierichting / windrichting in de rug
Benedenwinds Benedenstrooms	Locatie voorbij het incident in de tunnel waar rook of emissie gevaarlijke stoffen naar afgevoerd worden.
Middentunnelkanaal	Ruimte tussen de twee tunnelbuizen die dienst doet voor ontvluchting van een tunnelbuis. Ook kunnen hier kabels en leidingen aanwezig zijn.

Voorzieningen t.b.v. incidentbestrijding / - beheersing	
Begrip	**Toelichting**
Calamiteitenbedrijf	Status van tunnel die wordt ingesteld als zich een calamiteit voordoet. Hierdoor worden een aantal standaard geautomatiseerde veiligheidsmaatregelen genomen in de tunnel om de incidentbestrijding te ondersteunen
Evacuatiebedrijf	Status van tunnel die wordt ingesteld bij voorval met brand of gevaarlijke stoffen om ontvluchting mogelijk te maken vanuit de tunnel. Er worden dan een aantal standaard geautomatiseerde maatregelen genomen in de tunnel.
Afsluitboom	Beweegbare slagboom voor afsluiting van rijbanen en dienstwegen
VEVA	Verplaatsbare vangrail of Verrijdbare bermbeveiliging
Rijbaanafsluiters	Gelijk aan VEVA.
CaDo	Calamiteitendoorgang tussen wegvakken in een geleiderail die handmatig of op afstand bediend moet worden.
Hulppost	Elke tunnel bevat kasten die hulpmiddelen bieden voor de weggebruikers om een beginnende brand te blussen (noodtelefoon, brandblusser en/of brandslanghaspel) en de brandweer extra voorzieningen biedt voor de incidentbestrijding (noodtelefoon, brandslanghaspel, afnamepunt blusleiding en/of wandcontactdoos)
Intercom	Directe spreekverbinding met tunneloperator bij afsluitbomen en/of CaDo's.

Vervolg op volgende pagina

Begrippen incidentbestrijding in wegtunnels, Vervolg

Begrippenlijst
Vervolg

Noodtelefoon	Directe spreekverbinding vanuit de tunnel met de tunneloperator zodat alarm geslagen kan worden door weggebruikers en indien nodig voor directe afstemming tussen hulpdiensten met de tunneloperator.
Ventilatie	Primair voor de ontvluchting vanuit de incidentbuis voorbij het incident mogelijk te maken. Secundair om de hulpdiensten te ondersteunen in bestrijding van een brand in de tunnel. De ventilatierichting is altijd met de rijrichting van de incidentbuis mee. De ondersteunende buis heeft de ventilatierichting in dezelfde richting als de incidentbuis.
Vluchtdeur	Nooduitgang die gebruikt wordt om een tunnelbuis te ontvluchten. Tevens toegangsweg van de incidentbuis voor de brandweer voor verkenning.
Veilige ruimte	Ruimte achter vluchtdeur (meestal in het middentunnelkanaal) om vluchtenden tijdelijk op te vangen totdat de ondersteunende tunnelbuis veilig is.
Begrippen bij tunnelbestrijding	
Begrip	**Toelichting**
Calamiteit	Voorval met brand, gevaarlijke stoffen of ernstige aanrijding.
Ernstige aanrijding	Aanrijding met hoog energetisch letsel en rijbaan is versperd.
Hoogst-leidinggevende hulpdiensten	Dit is afhankelijk van de betrokken hulpdiensten: Is de brandweer aanwezig: Brandweer is de leidende discipline. De (H)OVD-B heeft de primaire leiding. Is de brandweer NIET aanwezig: Politie is de leidende discipline, De OVD-P heeft de primaire leiding
Coördinerende eenheid	Eerste eenheid ter plaatse, indien geen of totdat de OVD van de discipline ter plaatse is.
Sein Veilig	Term die wordt gebruikt door hoogst leidinggevende hulpdiensten om aan te geven dat het veilig is voor andere (hulp)diensten om een tunnelbuis te betreden. Dit wordt apart aangegeven voor de ondersteunende buis en de incidentbuis.

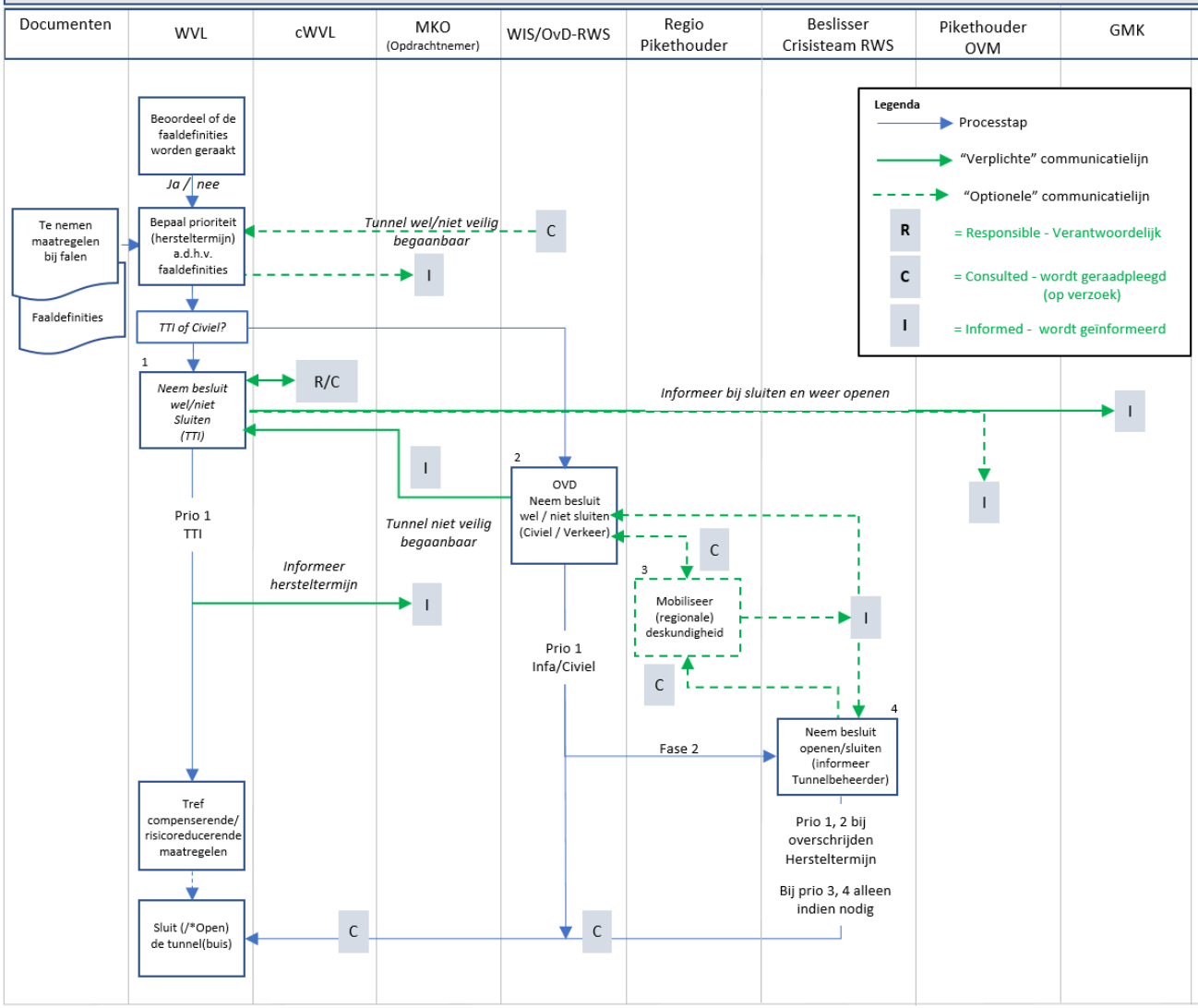
V Afkortingenlijst

B	**BHV**	Bedrijfshulpverlening
	BVB	Bureau Veiligheidsbeambte (Rijkstunnels)
	BT	Beleidsteam
C	**CADO**	Calamiteitendoorsteek
	CBP	Calamiteitenbestrijdingsplan zoals bedoeld in de Warvw
	CCTV	Closed-circuit television
	CMV	Centraal Meldpunt Vrachtautoberging
	CoPI	Commando Plaats Incident
	CT-RWS	(Landelijk) Crisisteam Rijkswaterstaat
	CWVL	Coördinerend Wegverkeersleider VCNWN
D	**DCC**	Departementaal Coördinatiecentrum Crisisbeheersing van het Ministerie van Infrastructuur en Waterstaat
	DRIP	Dynamisch Route Informatie Paneel
	DROC	Dienst Regionaal Operationeel Centrum
G	**GHOR**	Geneeskundige Hulpverleningsorganisatie in de Regio
	GRIP	Gecoördineerde Regionale Incidentbestrijdings Procedure
H	**HD**	Hulpverleningsdiensten
	HID	Hoofdingenieur Directeur
	HIP	Hulpdienst Informatie Paneel
	HPK	Hoofdpompkamer
	HWN	Hoofdwegennet
I	**IM**	Incidentmanagement
L	**LCM**	Landelijk Centraal Meldpunt (voor inschakelen personenautobergers)
M	**MKO**	Motorkapoverleg
	MPK	Middenpomp(en)kamer
	MTK	Middentunnelkanaal
	MTM	Motorway Traffic Management
N	**NCTV**	Nationaal Coördinator Terrorismebestrijding en Veiligheid
O	**OVD-RWS**	Officier van Dienst - Rijkswaterstaat
	OTO	Opleiden, Trainen en Oefenen
	OVM	Operationeel Verkeersmanagement
P	**PvA**	Plan van aanpak
R	**Rarvw**	Regeling aanvullende regels Veiligheid wegtunnels
	RCP	Regionaal Crisisplan
	RDS	Radio Data System
	REVI	Richtlijn eerste veiligheidsmaatregelen bij verkeersincidenten
	ROT	Regionaal Operationeel Team
	RWS	Rijkswaterstaat

T	**TTI**	Tunnel technische installaties
	TVD	Tunnelveiligheidsdossier
U	**UGS**	Uitgangsstelling
	UMS	Uitsluitend materiële schade
	UPP	Uniforme Primaire Processen
V	**VB**	Veiligheidsbeambte
	VBP	Veiligheidsbeheerplan
	VC	Verkeerscentrale
	VCNL	Verkeerscentrum Nederland
	VCNWN	Verkeerscentrale Noordwest Nederland
	V&G plan	Veiligheids- en gezondheidsplan
	VRAA	Veiligheidsregio Amsterdam-Amstelland
	VRI	Verkeersregelinstallatie (verkeerslicht)
	VRK	Veiligheidsregio Kennemerland
	VWM	Landelijke Dienst Verkeer- en Watermanagement van RWS
W	**Warvw**	Wet aanvullende regels Veiligheid wegtunnels
	WIS	Weginspecteur Rijkswaterstaat
	WNN	West-Nederland Noord
	WVL	Wegverkeersleider VCNWN

Rijkswaterstaat
Ministerie van Infrastructuur en Waterstaat

Beslis- en bevoegdhedenschema : Sluiten, openen en open houden tunnels bij falen en calamiteiten



Rolhouder MKO: Bij storingen informeert de WVL de MKO en deze informeert de opdrachtnemer. Indien dit (nog) niet is ingeregeld wordt de opdrachtnemer direct geïnformeerd door de WVL.

1. Bij een storing/falen met herstelprioriteit 1 bepaalt de cWVL dat de tunnel gesloten wordt, of open blijft omdat afdoende compenserende of risico-reducerende maatregelen zijn ingezet. Eerst sluiten, daarna de m compenserende of risico-reducerende maatregelen activeren en daarna weer openen is een mogelijk scenario. Bij oplossing van de storing/falen beslist cWVL over openen tunnel. Indien geen CWVL aanwezig is (nachten / weekenden) komt deze verantwoordelijk bij de WVL te liggen. De WVL heeft de mogelijkheid om de CWVL met binding te bellen en om advies te vragen

2. Bij falen van infrastructuur of de civiele constructie bepaalt de OvD-RWS of de tunnel gesloten wordt of open blijft.

3: (Regionale) deskundigen kunnen op verzoek van OvD-RWS en/of CT-RWS gemobiliseerd worden via de Pikethouder Regio voor advisering over (regio) specifieke zaken m.b.t. de tunnel (techniek, civiel).

4. De beslisser van CT-RWS bepaalt bij het overschrijden van de hersteltermijn (storingen met herstel prioriteit 2, 3 en 4) of de tunnel open blijft of gesloten moet worden.
Bij langere herstelperioden (prio 3 of 4) zal deze beslissing waarschijnlijk tijdig afgestemd zijn met de Regionale Tunnelbeheerder.

CT-RWS besluit ook of een tunnel:
- waarvan een prio 1 storing onvoldoende is hersteld, en
- de compenserende of risico-reducerende maatregelen in onvoldoende mate zijn geoperationaliseerd,
- toch wordt geopend om grotere risico's elders op het netwerk of in de samenleving te voorkomen. *Hier is sprake van uitzonderlijke omstandigheden.

Versie : 20220509
Status: Definitief
Bedrijfsvertrouwelijk

Rijkswaterstaat West Nederland Noord **CBP bijlage 11.** **Overzicht tunnelsystemen** **voor ondersteuning incidentafhandeling** **versie 16 december 2021 (behorende bij CBP d.d. 30 september 2024)**	**Coentunnel buizen Li (Westbuizen)**	**Coentunnel buizen Re (Oostbuizen)**	**Zeeburgertunnel**	**Schipholtunnel**	**Wijkertnnel**	**Velsertunnel**	**Gaasperdammer tunnel**
Automatisch standby na detectie (werkt onafhankelijk van calamiteitenknop en evacuatieknop)	ja	Ja	ja	ja	nee [1]	ja	ja
Geactiveerde systemen onder de calamiteitenknop							
Calamiteitenknop (1 knop per buis)	ja	ja	ja	ja	ja	ja	ja
VRI incidentbuis op rood	ja	ja	ja	ja	ja	ja	ja
VRI ondersteunende buis op rood	ja	ja	ja	ja	ja	ja	ja
Afsluitbomen automatisch neer (incidentbuis en ondersteunende buis)	ja	ja	nee	nee	ja	ja	ja
Langsventilatie incidentbuis in rijrichting	ja	ja	ja	ja	ja	ja	ja
Langsventilatie ondersteunende buis zelfde richting als incidentbuis	ja	ja	ja	ja	ja	ja [2]	ja
Ondersteunende ventilatie omkeerbaar per buis	ja	ja	ja	ja	ja	n.v.t.	ja [3]
Ontgrendeling vluchtdeuren incidentbuis (direct)	ja	ja	n.v.t.	n.v.t.	n.v.t.	ja	ja
Vergrendeling vluchtdeuren ondersteunende buis	ja [4]	nee [5]	n.v.t.	n.v.t.	n.v.t.	ja [6]	ja [7]
Ontgrendeling kopdeuren einde vluchtroute (direct)	n.v.t.	ja	ja	n.v.t.	ja	n.v.t.	n.v.t.
Ontgrendeling einddeuren (laatste vluchtdeuren) einde vluchtroute (met vertraging)	ja [4]	n.v.t.	n.v.t.	n.v.t.	n.v.t.	n.v.t.	ja [7]
Ventilatie vluchtroute middentunnelkanaal en/of dienstgebouwen (overdrukinstallatie)	ja	ja	ja	ja	ja	ja	ja
Verlichting incidentbuis op maximaal (gewenste stand)	ja	ja	ja	ja	ja	ja	ja
Verlichting vluchtroutes	ja	ja	ja	ja	ja	ja	ja
(Dynamische) Vluchtwegaanduiding	ja	ja	ja	ja	ja	ja	ja
Noodstroomaggregaten (indien nodig starten deze op)	ja	ja	ja	ja	ja	ja	ja
Brandbluspompen standby, blussysteem op druk	ja	ja	ja	ja	ja	ja	ja
Vuilwaterpompen in cal. stand	ja	ja	ja	ja	ja	ja	ja
Geactiveerde systemen onder Evacuatiebedrijf (dus aanvullend op het calamiteitenbedrijf)							
Evacuatiebedrijf op MMI	ja	ja	ja	ja	ja	ja	ja
Automatisch evacuatiebericht via omroepinstallatie	ja	ja	nee	nee	ja	ja	ja
Contourverlichting vluchtdeuren	ja	ja	ja	ja	ja	ja	ja
Automatisch evacuatiebericht "UITGANG HIER/EXIT HERE" door geluidsbaken	ja	ja	ja	ja	ja	ja	ja
Automatisch audiobericht in compartiment/MTK bij einddeuren voorafgaand aan ontgrendeling	n.v.t.	n.v.t.	n.v.t.	n.v.t.	n.v.t.	ja	ja
Overige systemen die de afhandeling van calamiteiten ondersteunen en die altijd werken							
	Coentunnel buizen Li (westbuizen)	**Coentunnel buizen Re (oostbuizen)**	**Zeeburgertunnel**	**Schipholtunnel**	**Wijkertnnel**	**Velsertunnel**	**Gaasperdammer Tunnel**
Handmatige omroepberichten door WVL in verkeersbuizen	ja	ja	ja	ja	ja	ja	ja
Omroepsysteem vluchtwegen	ja	ja	ja	ja	ja	ja	ja
HF installatie voor inbreken radiofrequentie	ja	ja	ja	ja	ja	ja	ja
C-2000 versterker tunnelbuizen	ja	ja	ja	ja	ja	ja	ja
C-2000 versterker dienstgebouwen	ja	ja	nee	nee	nee	ja	ja
Verlichting Wrakkenterreinen	ja	ja	nee	n.v.t.	ja	ja	n.v.t.

[1] In de Wijkertunnel wordt de ventilatie aangestuurd ingeval van een alarm van de zicht-rookmeting (rookdetectie) in de verkeersbuis. De ventilatie wordt niet aangestuurd bij het openen van een hulppostkast in combinatie met het uitnemen van een brandhaspel.
[2] In de Velsertunnel is de langsventilatie in de ondersteunende buis zowel in de rijrichting als tegengesteld aan de rijrichting.
[3] Dit geldt niet voor PLi en PRe van de GDT.
[4] In de tunnelbuizen Li (westbuizen) van de Coentunnel wordt de einddeur (laatste vluchtdeur) aan de noordzijde vergrendeld en na 180s ontgrendeld (evacueren naar de ondersteunende buis).
[5] De vluchtdeuren hebben aan de zijde van de vluchtroute (middentunnelkanaal) geen hendel en geen vergrendeling.
[6] In de Velsertunnel worden de vluchtdeuren van de ondersteunende buis na vergrendeling met een vertraging van 120s. weer ontgrendeld.
[7] In de hoofdbuizen en parallelbuizen Li en Re van de Gaasperdammertunnel wordt de einddeur (laatste vluchtdeur) van elke gecompartimenteerde vluchtroute, leidend naar de ondersteunende buis na vergrendeling met een vertraging van 270s weer ontgrendeld (evacueren via de ondersteunende buis). Bij een calamiteit in de wisselbuis worden de vluchtdeuren in de wand tussen Wisselbuis en HLi na vergrendeling met een vertraging van 270s vanaf instellen calamiteitenbedrijf weer ontgrendeld.

Bijlage 12: Formulier Bommelding

Meldingsformulier telefonische bommeldingen

1. **Opname apparatuur inschakelen !**
2. **Telefoon-nr. melder**_____ **(nummerweergave)**
3. **Ontvangst: dag** _____ **datum** _____ **tijdstip** _____
4. **Letterlijke tekst:** _____

_____

_____

_____

_____

5. Vragen:

Tijdstip van ontploffing _____

Lokatie van bom _____

(zichtbaar of verstopt in)

Reden van melding _____

Wie is melder _____

(naam of groepering)

6. Kenmerken van melder:

Stem	**Spraak**	**Taal**
☐ **Man**	☐ **Langzaam**	☐ **Frans**
☐ **Vrouw**	☐ **Normaal**	☐ **Duits**
☐ **Kind**	☐ **Snel**	☐ **Engels**
☐ **Leeftijd ca** _____	☐ **Lijzig**	☐ **Overige nl:** _____
	☐ **Ernstig**	☐ **Accent/ dialect** _____
	☐ **Overig nl:** _____	

7. Achtergrondgeluiden:

☐ **Stemmen** ☐ **Verkeer** ☐ **Muziek** ☐ **Anders nl** _____

Opgenomen door: _____

Bedrijf / Dienst / Instelling _____

Telefoonnummer _____

Bericht doorgeven aan: 112 Alarm-centrale

Berichten bij maatregelpakket I:

Scenario: Ontruiming tunnelbuis	*Van tevoren opgenomen bericht (staat op "bandje")* ***Zit onder evacuatieknop, activeren door WVL*** *Uitzenden via luidsprekers & RDS*	*Frequentie*
<*Gongslag*> Attentie, Attentie. Dit is een noodsituatie. Verlaat uw voertuig, verlaat de tunnel via de vluchtdeur.	<*Gongslag*> Attention, Attention. This is an emergency. Abandon your vehicle and leave the tunnel using the emergency exit. Onderstaand bericht wordt gelijktijdig getoond op het informatie-display (tekstbericht) van de autoradio: Tunnelincident, volg instructies, follow instructions.	1 x per minuut

Scenario: Ontruiming vluchtkanaal	*Van tevoren opgenomen bericht (staat op "bandje")* ***Activeren door WVL*** *Uitzenden via luidsprekers in vluchtkanaal*	*Frequentie*
<*Gongslag*> Attentie, Attentie. Verlaat het vluchtkanaal door de pijlen te volgen en loop door naar de verzamelplaats.	<*Gongslag*> Attention, Attention. Leave the evacuation tunnel. Follow the signs to the safe assembly point.	1 x per minuut

Indien de WVL merkt dat er niet op bericht 1 wordt gereageerd, kan hij ertoe besluiten om het standaardbericht 1 te stoppen en zelf een persoonlijker bericht om te roepen. Hiervoor is het volgende voorbeeld beschikbaar:

Extra bericht: **Scenario: Ontruiming tunnelbuis**	*Niet van tevoren opgenomen bericht, alleen als niet gereageerd wordt op opgenomen bericht.* ***Uitvoering door WVL*** *Uitzenden via luidsprekers*	*Frequentie*
<*Gongslag*> Attentie, Attentie. Dit is een noodsituatie. Iedereen dient de tunnel onmiddellijk te verlaten via de vluchtdeur/ Bestuurder van het … stilstaand voertuig[1] u wordt dringend verzocht de tunnel via de vluchtdeur te verlaten.	<*Gongslag*> Attention, Attention. This is an emergency. Every one has to leave the tunnel immediately using the emergency exit/ Driver of the … vehicle: you are requested to leave the tunnel immediately using the emergency exit	Eenmalig, alleen herhalen als niet gereageerd wordt
[1] *nadere omschrijving voertuig of persoon, te bepalen tijdens incident, bijv. kleur, merk van voertuig.*		

Berichten bij maatregelpakket II, III of IV:

Scenario: Langdurige stremming	*Van tevoren opgenomen bericht (staat op "bandje")* *Uitzenden via luidspreker incidentbuis en gelijktijdig tekstbericht via informatie-display autoradio*	*Frequentie*
<*Gongslag*> Attentie, Attentie. Het verkeer staat voor langere tijd vast. Zet uw voertuig uit, blijf in uw voertuig en wacht op verdere instructies.	<*Gongslag*> Attention, Attention. Traffic has stopped moving. Turn off your engine. Do not leave your vehicle. Await further instructions. Onderstaand tekstbericht wordt gelijktijdig getoond op het informatie-display van de autoradio: Tunnelincident, volg instructies, follow instructions.	1 x per 5 minuten

Bericht bij maatregelpakket III voor tunnels hoogtedetectie

Scenario: Stilstaande vrachtwagen voor tunnel tgv hoogtedetectie.[1]	*Niet van tevoren opgenomen bericht* ***Uit te spreken door WVL.*** *Uitzenden via luidspreker*	*Frequentie*
<*Gongslag*> Attentie, Attentie. De 1e vrachtwagen[2] voor de verkeerlichten, rijdt u door naar de vluchtstrook[3], u bent te hoog. Wij komen zo bij u.	<*Gongslag*> Attention, Attention. The driver of the first truck at the traffic lights, drive to the emergency lane. Your truck is too high. We will come to your assistance in a moment.	Eenmalig, alleen herhalen als niet gereageerd wordt
[1 *dit bericht is afhankelijk van de situatie. Er is gebruik gemaakt van de nu gebruikte berichten in Noord-Holland* *2 Dit kan dus ook de tweede vrachtwagen zijn* 3 *De locatie is afhankelijk van de tunnel nader te specificeren, dus per tunnel vaststellen*		

Berichten bij maatregelpakket IV:

Scenario: Voetgangers/fietsers in de tunnel	*Niet van tevoren opgenomen bericht* ***Activeren door WVL*** *Uitzenden via luidspreker*	*Frequentie*
<*Gongslag*> Attentie, Attentie. Wandelen/fietsen[1] in de tunnel is verboden. U [2] wordt verzocht naar de hulppost te gaan en met de noodtelefoon contact op te nemen met de operator. Loopt u langs de wand met het verkeer mee naar de eerstvolgende hulppost. Pas op voor het verkeer.	<*Gongslag*> Attention, Attention. Walking/cycling in the tunnel is prohibited. Please go to the emergency post and use the emergency phone to get in contact with the operator. Walk close to the wall in the same direction as the traffic to the nearest emergency post. Watch out for traffic.	Eenmalig, alleen herhalen als niet gereageerd wordt
[1] *nadere omschrijving voetganger/fietser, te bepalen tijdens incident,* [2] *nadere omschrijving, aanroepen desbetreffende persoon*		

Scenario: Spookrijder	*Van tevoren opgenomen bericht* ***Activeren door WVL*** *Uitzenden via RDS*	*Frequentie*
<*Gongslag*> Attentie, Attentie. Er is een spookrijder gesignaleerd. Haal niet in, blijf rechts rijden.	<*Gongslag*> Attention, Attention, There is a driver heading in the wrong direction. Do not overtake, keep right. Onderstaand tekstbericht wordt gelijktijdig getoond op het informatie-display van de autoradio: Tunnelincident, volg instructies, follow instructions.	Eenmalig

Berichten bij maatregelpakket V:

Scenario: Waarschuwing incident	*Van tevoren opgenomen bericht (staat op "bandje")* ***Activeren door WVL*** *Uitzenden via autoradio*	*Frequentie*
<*Gongslag*> Attentie, Attentie. Er is een incident in de tunnel. Matig uw snelheid.	<*Gongslag*> Attention, Attention. There is an incident in the tunnel. Please slow down. Onderstaand tekstbericht wordt gelijktijdig getoond op het informatie-display van de autoradio: Tunnelincident, volg instructies, follow instructions.	1 x per minuut

Scenario: Stilstaand voertuig in tunnel	*Niet van tevoren opgenomen bericht* ***Uitvoering door WVL*** *Uitzenden via luidspreker*	*Frequentie*
<*Gongslag*> Attentie, Attentie. De bestuurder van de … *stilstaand voertuig*[1] wordt verzocht naar de hulppost te gaan en met de noodtelefoon contact op te nemen met de operator. Loopt u langs de wand met het verkeer mee naar de eerstvolgende hulppost. Pas op voor het verkeer.	<*Gongslag*> Attention, Attention. The driver of the … vehicle is requested to go to the emergency post and use the emergency phone to get in contact with the operator. Walk close to the wall in the same direction as the traffic to the nearest emergency post. Watch out for traffic.	Eenmalig, alleen herhalen als niet gereageerd wordt
[1] *nadere omschrijving voertuig invullen, te bepalen tijdens incident, bijv. kleur, merk van voertuig.*		

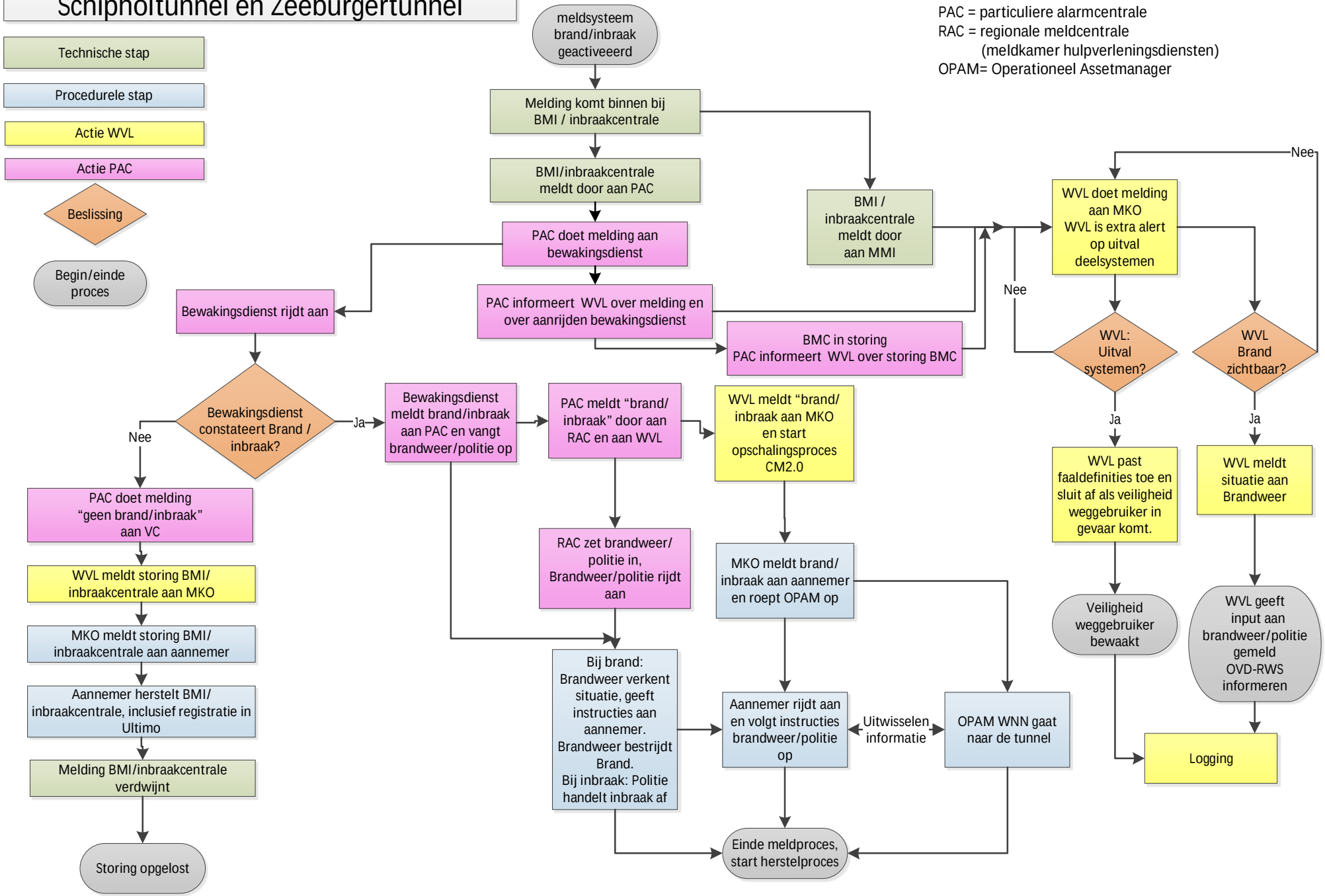
CHECKLIST SCHOUWEN

Vraag	Ja /nee/n.v.t.	gedaan?
1. Is er nog technisch onderzoek nodig waar opruimen en herstel op moet wachten?		
2. Zijn alle benodigde diensten voor opruim- en herstelwerkzaamheden opgeroepen? (b.v. calamiteitenaannemer?) • Is bij schade aan installatie of constructie functioneel beheer gealarmeerd voor aansturing instandhouder?		
3. Is schade geregistreerd (foto's, video)?		
4. Is (zijn) schadeveroorzaker(s) bekend?		
5. Zijn voertuigen weggesleept?		
6. Zijn verloren lading en andere obstakels verwijderd?		
7. Is het wegdek gereinigd?		
8. Is het herstel wegdek aangevangen?		
9. Is het herstel van beschadigde installaties en infrastructuur aangevangen?		
10. Moet de vuilwaterkelder(s) worden afgepompt (in geval van verontreiniging door vloeistof en/of bluswater)?		
11. Moeten hulppostkasten worden bijgevuld?		
12. Is de inspectie van reparaties uitgevoerd?		
13. Is het wegdek geschouwd?		
14. Is het bluswater schoongemaakt en bijgevuld?		
15. Is het MTK geschouwd? (geen achtergebleven goederen, hendels van vluchtdeur op hun plek?)		
16. Kan de tunnel worden vrijgegeven voor verkeer?		

Brand- en inbraakmeldproces Velsertunnel Schipholtunnel en Zeeburgertunnel

Versie 1.7 20231116 def

BMI = brandmeldinstallatie
PAC = particuliere alarmcentrale
RAC = regionale meldcentrale
(meldkamer hulpverleningsdiensten)
OPAM= Operationeel Assetmanager



Behorende bij CBP 30 september 2024

Brandmeldproces dienstgebouwen Wijkertunnel, Coentunnel en Gaasperdammertunnel

Versie 1.0 def 20221221

BMI = brandmeldinstallatie

meldsysteem brand in dienstgebouw geactiveerd

BMI
Ontvangt melding

BMI
meldt door aan ontruimingsinstallatie in dienstgebouw

Aanwezigen in dienstgebouw handelen conform veiligheidsinstructies

Aanwezig personeel ontruimd

BMI
meldt door aan Meldkamer Brandweer

Storing BMI
MK Brandweer meldt aan VC

BMI
meldt door aan MMI

Meldkamer Brandweer
zet brandweer in en belt VC (WVL)

Brandweer
Rijdt aan en verkent.
Brand?

Nee

Ja

Brandweer bestrijdt brand.

Uitwisselen informatie

Aannemer
rijdt aan en volgt instructies brandweer op

Uitwisselen informatie

MKO
meldt brand dienstgebouw aannemer en roept de OPAM WNN op

OPAM WNN gaat naar de tunnel

Uitwisselen informatie

WVL start
opschaling naar crisis management 2.0

Nee

WVL doet melding aan MKO
WVL is extra alert op uitval deelsystemen

WVL:
Uitval systemen?

Ja

WVL
past faaldefinities toe en sluit tunnel af als veiligheid weggebruiker in gevaar komt.

informeren

Veiligheid weggebruiker bewaakt

WVL
Brand zichtbaar?

Nee

Ja

WVL
meldt situatie aan Meldkamer Brandweer

Meldkamer
informeert brandweer over situatie

Brandweer geïnformeerd

Einde meldproces,
brand bestreden,
start herstelproces

Logging

Actie WVL

Actie Brandweer

Technische stap

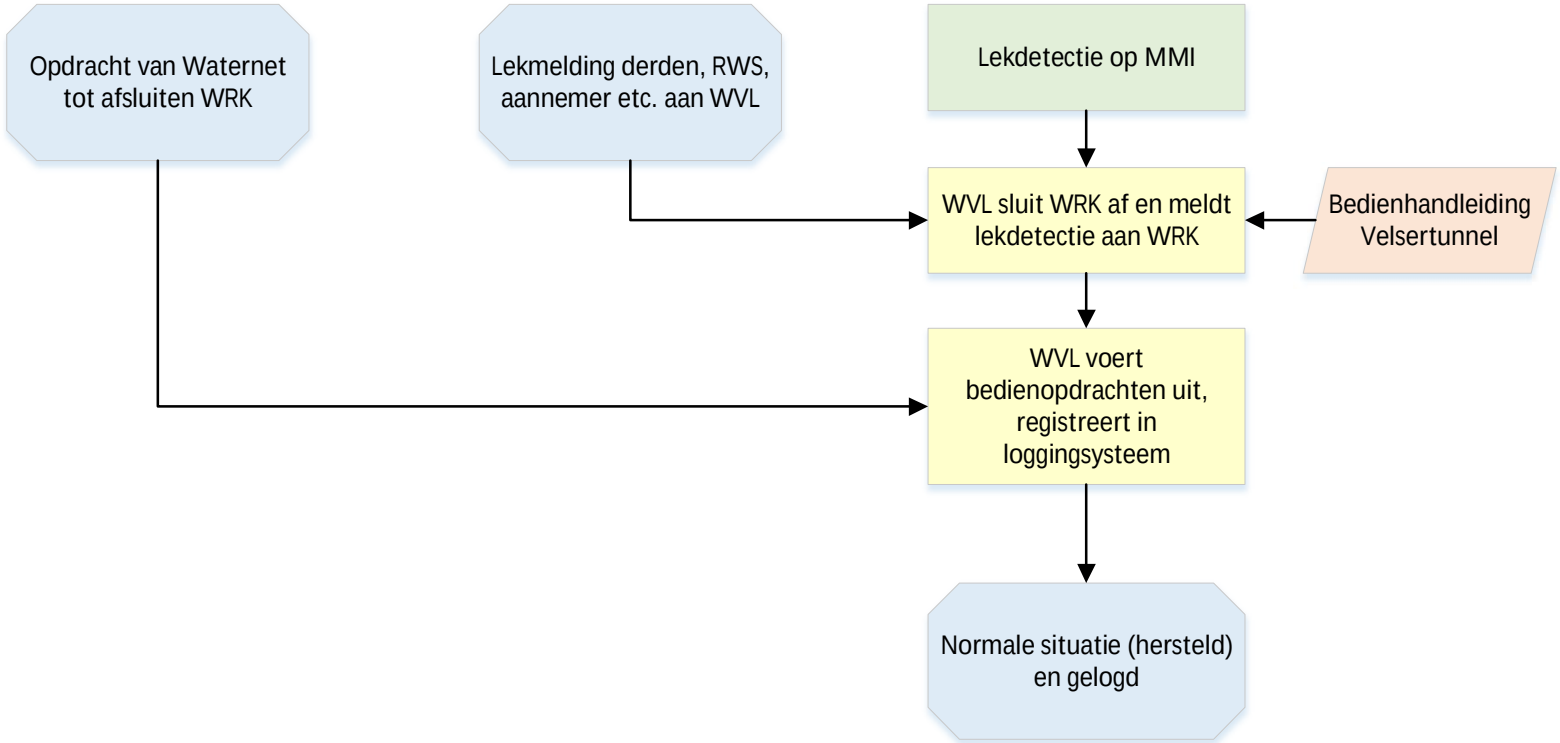
Procedurele stap

Beslissing

Begin/einde proces

Behorende bij CBP 30 september 2024

Proces bediening waterleiding WRK in de Velsertunnel



Behorende bij CBP 30 september 2024

Versie 1.2 28 november 2023

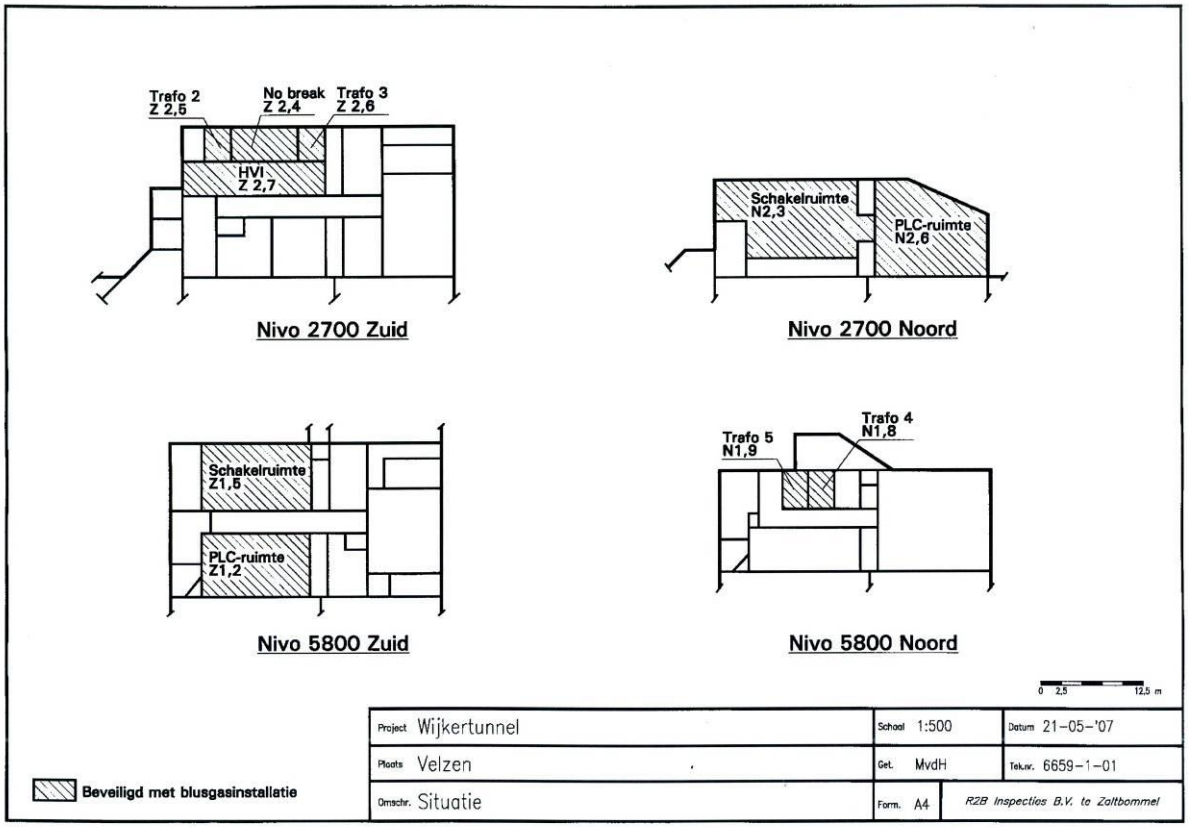
Bijlage 32 Instructie Blusgasinstallatie
Dienstgebouwen Wijkertunnel

Een aantal ruimtes in de dienstgebouwen van de Wijkertunnel is voorzien van een aparte blusgasinstallatie.

Blussysteem	Tyco Integrated systems
Blusgastype:	Novec™ 1230 (producent 3M)
Chemische formule	$CF_3\ CF_2\ C(O)\ CF\ (CF_3)_2$
Omschrijving	Dodecafluoro-2-methylpentan-3-one
Producent	
Kenmerken:	- Geen gevaar voor aanwezigen - Kleurloos - Elektrisch niet geleidend - Niet corrosief - Laat geen residu achter
Bron: Installateur: Tyco Integrated systems	

Ruimtes in dienstgebouwen die zijn voorzien van de blusgasinstallatie

Lokatie	**Niveau**	**Installatie**	**Zaalnummer**
Dienstgebouw zuid	2700	Trafo 2 ruimte	Z 2.5
	2700	Trafo 3 ruimte	Z 2.6
	2700	No breakruimte	Z 2.4
	2700	HVI	Z 2.7
	5800	Schakelruimte	Z 1.5
	5800	PLC ruimte	Z 1.2
Dienstgebouw noord	2700	Schakelruimte	N 2.3
	2700	PLC ruimte	N 2.6
	5800	Trafo 5	N 1.9
	5800	Trafo 4	N 1.8


Trafo 2
Z 2,5
No break
Z 2,4
Trafo 3
Z 2,6
HVI
Z 2,7
Nivo 2700 Zuid
Schakelruimte
N2,3
PLC-ruimte
N2,6
Nivo 2700 Noord
Schakelruimte
Z1,5
PLC-ruimte
Z1,2
Nivo 5800 Zuid
Trafo 4
N1,8
Trafo 5
N1,9
Nivo 5800 Noord
0 2,5 12,5 m
Beveiligd met blusgasinstallatie
Project Wijkertunnel
School 1:500
Datum 21–05–'07
Plaats Velzen
Get. MvdH
Tek.nr. 6659–1–01
Omschr. Situatie
Form. A4
R2B Inspecties B.V. te Zaltbommel

Rijkswaterstaat
Ministerie van Infrastructuur en Waterstaat

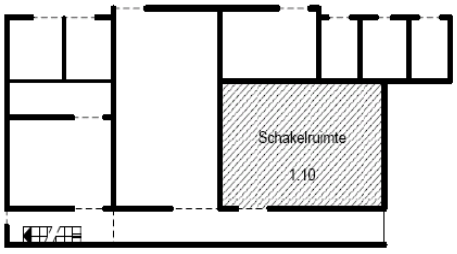
Bijlage 62 Instructie
Blusgasinstallatie Dienstgebouwen
Coentunnel

Een aantal ruimtes in de dienstgebouwen van de Coentunnel is voorzien van een aparte blusgasinstallatie.

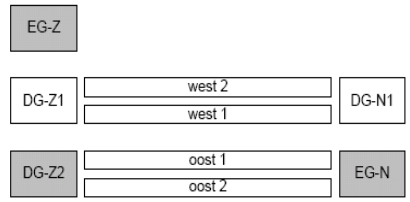
Blussysteem	
Blusgastype:	Argon
Chemische formule	Ar
Omschrijving	
Producent	
Kenmerken:	Kleurloos gas Reukloos Zelfontbrandingstemperatuur: niet van toepassing Geen toxicologische effecten
Bron:	

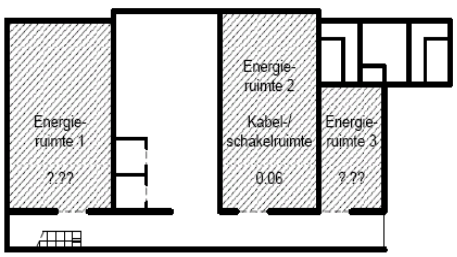
Ruimtes in dienstgebouwen die zijn voorzien van de blusgasinstallatie

Locatie	**Niveau**	**Installatie**	**Zaalnummer**
Energiegebouw noord (EG-N)	-1400	Data en besturing 1	-1.01
	-1800	Energie 1	-1.02
	-1800	Energie 2	-1.03
	-1400	Data en besturing 2	-1.05
	-1800	Energie 3	-1.06
Dienstgebouw zuid (DG-Z2)	-1400	Data en besturing 1	-1.12
	-1800	Energie 1	-1.13
	-1800	Energie 2	-1.14
	-1400	Data en besturing 2	-1.16
	-1800	Energie 3	-1.17
Energiegebouw zuid (EG-Z)	0	Schakelruimte	1.10
	-40	MS-ruimte	
	-2800	Energieruimte 1	
	-2800	Kabel-/schakelruimte Energieruimte 2	0.06
	-2800	Energieruimte 3	

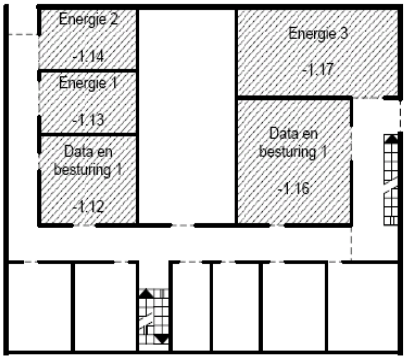


Energiegebouw zuid (EG-Z) beganegrond

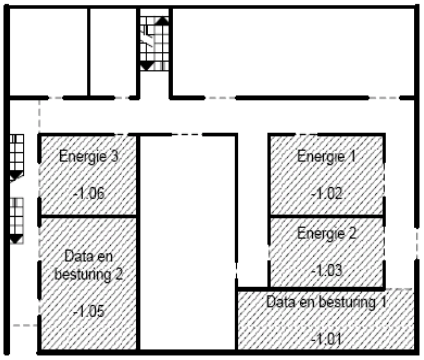




Energiegebouw zuid (EG-Z) kelder



Dienstengebouw zuid (DG-Z2) laag -1



Energiegebouw noord (EG-N) laag -1

Bijlage C Format Risicobeoordeling

Deze Excel spreadsheet is toegevoegd bij “Informatie Opdrachtgever.

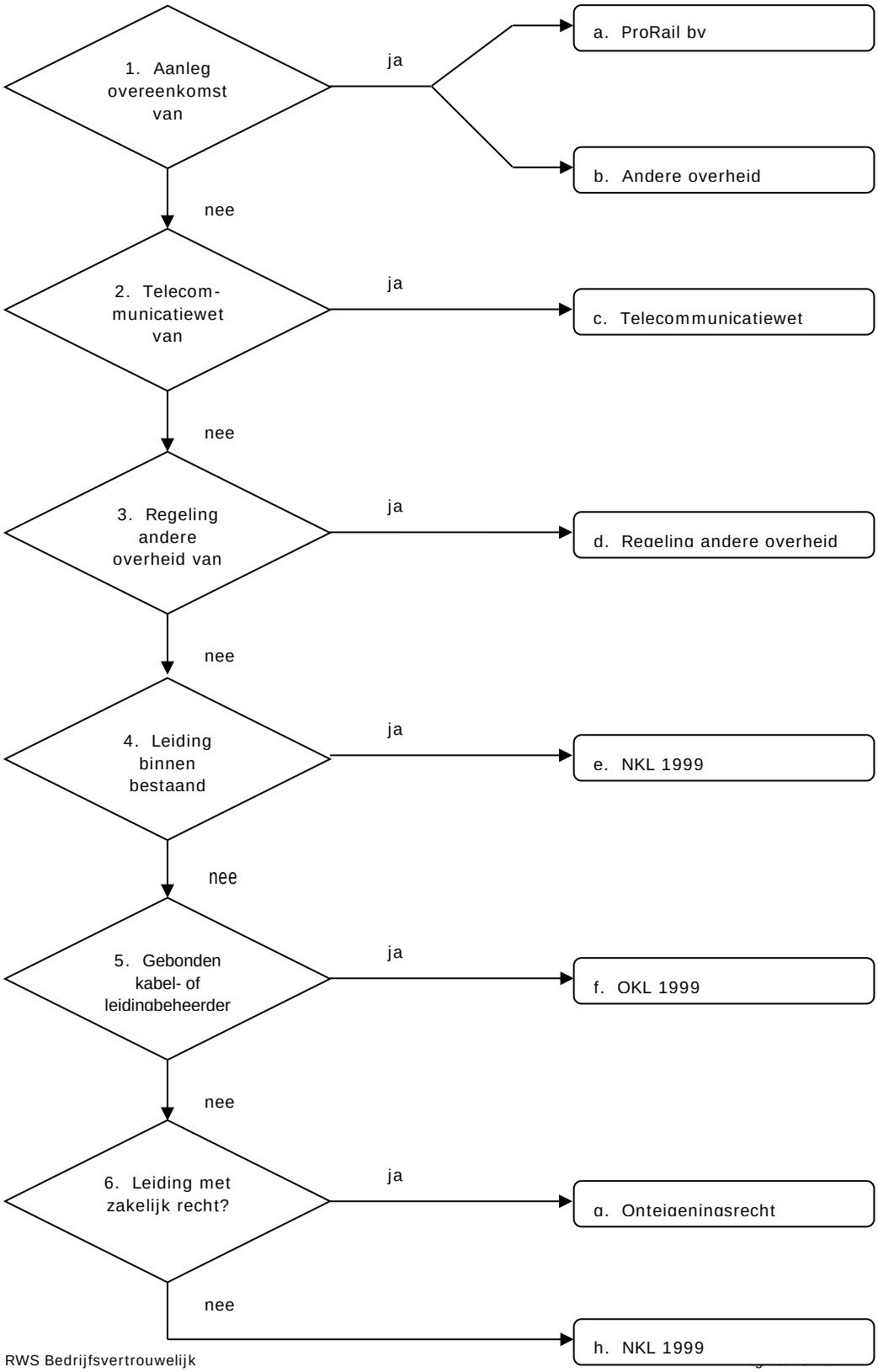
Bijlage D Protocol berekenen en aantonen MKI-waarde

Niet van toepassing.

Bijlage E Kaderrichtlijn Coördinatie uitvoeringsbesluiten op grond van artikel 5.45 lid 2 Omgevingswet

Niet van toepassing.

Bijlage F Regelingenschema Kabels en Leidingen Derden



TOELICHTING REGELINGENSCHEMA

ad a

- ProRail bv = een overeenkomst conform het Samenwerkingsprotocol ProRail – Rijkswaterstaat d.d. 15 december 2011, op grond waarvan de Opdrachtgever alle kosten draagt van het aanpassen van de kabels en leidingen in beheer bij ProRail bv.

ad b

- Andere overheid = een overeenkomst met een andere bij de Werkzaamheden betrokken overheid, op grond waarvan de Opdrachtgever alle kosten draagt van het aanpassen van de kabels en leidingen in beheer bij die overheid.

ad c

- Telecommunicatiewet = de Telecommunicatiewet met bijbehorende Uitvoeringsprotocol Telecom d.d. 13 november 2012, inclusief de bijlagen waaronder de model-Projectovereenstemmingen (nacalculatie, vaste prijs, vereenvoudigd en geschillen) met bijlagen.
- Opmerking: KPN bv verwijdert op eigen kosten de verlaten kabels van het Wegen Telecommunicatie Netwerk, voor zover gelegen buiten het grondgebied van Rijkswaterstaat, conform het Transitieplan WTN d.d. 5 februari 2007 en de Overeenkomst voor onbepaalde tijd inzake beschikking en beheer t.a.v. de functieloze WTN kabels d.d. 22 december 2011.

ad d

- Regeling andere overheid = een vergoedingsregeling van een andere overheid, welke wordt toegepast op een wijziging van aansluitende, kruisende of naastliggende infrastructuur van die overheid.
- Die overheid kan ook ProRail bv zijn (handelt namens de Minister van Infrastructuur en Waterstaat).
- Uitzondering: bij een ligging zonder toestemming van die overheid, dan wel in strijd met de voorschriften van de toestemming, kan het zijn dat er geen recht op vergoeding bestaat.

ad e

- NKL 1999 = de Nadeelcompensatieregeling verleggen kabels en leidingen in en buiten rijkswaterstaatswerken en spoorwegwerken 1999 (Staatscourant 1999, nr 97) met het daarbij behorende Uitvoeringsprotocol schadevergoeding kabels en leidingen (SKL 01-26, 14 september 2001), inclusief de model-Projectovereenstemmingen (vaste prijs en nacalculatie) met bijlagen.
- Het gaat hier om Afdeling 1.2. Recht op vergoeding voor het verleggen van kruisende en/of langsleidingen en de omvang daarvan.
- Uitzondering: bij een ligging zonder vergunning van de Opdrachtgever, dan wel in strijd met de voorschriften van de vergunning, kan het zijn dat er geen recht op vergoeding bestaat.
- Opmerking: de Defensie Pijpleiding Organisatie gaat op eigen kosten over tot het verwijderen van loze leidingen.

ad f

- OKL 1999 = Overeenkomst inzake verleggingen van kabels en leidingen buiten beheersgebied tussen de Minister van Verkeer en Waterstaat (thans Infrastructuur en Waterstaat) en EnergieNed, VELIN en VEWIN (Staatscourant 1999, nr. 97) met het bijbehorende Uitvoeringsprotocol schadevergoeding kabels en leidingen (SKL 01-26, 14 september 2001), inclusief de model-Projectovereenstemmingen (vaste prijs en nacalculatie) met bijlagen.
- Opmerking: de Defensie Pijpleidingen Organisatie gaat op eigen kosten over tot het verwijderen van loze leidingen.

ad g
- Onteigeningsrecht = de Onteigeningswet met de bijbehorende jurisprudentie.
- Afgesproken kan worden de OKL 1999 te volgen, tenzij de kabel- of leidingbeheerder hiervoor alleen kiest in gevallen dat dit voor hem gunstig uitpakt.

ad h
- NKL 1999 = de Nadeelcompensatieregeling verleggen kabels en leidingen in en buiten rijkswaterstaatswerken en spoorwegwerken 1999 (Staatscourant 1999, nr 97) met het daarbij behorende Uitvoeringsprotocol schadevergoeding kabels en leidingen (SKL 01-26, 14 september 2001), inclusief de model-Projectovereenstemmingen (vaste prijs en nacalculatie) met bijlagen.
- Het gaat hier om Afdeling 1.3. Recht op vergoeding voor het verleggen van buitenleidingen en de omvang daarvan.
- Eigenlijk geldt deze afdeling alleen voor een kabel of leiding die valt onder één van de categorieën openbare werken als bedoeld in de Belemmeringenwet Privaatrecht. Dit zou betekenen dat op de overige kabels en leidingen niet de NKL 1999 maar de Beleidsregel nadeelcompensatie Infrastructuur en Milieu 2014 (Staatscourant 2014, nr. 16584) zou moeten worden toegepast. Omdat die regeling echter slechts algemene normen kent, zou naar alle waarschijnlijkheid toch de NKL 1999 inhoudelijk worden gevolgd.
- Er kan een lastige situatie ontstaan als de kabel- of leidingbeheerder weigert aan het Verzoek tot Aanpassing te voldoen en hiertoe ook niet door een derde partij (vaak een andere overheid) kan worden gedwongen. Alsdan zal toch in minnelijk overleg tot een vergelijk moeten worden gekomen. Daarbij kan in uiterste geval een volledige schadeloosstelling (onteigeningsrecht) worden geboden. De kabel- of leidingbeheerder is immers niet verplicht een beroep op de NKL 1999 te doen. Wil deze een nog verdergaande vergoeding van alle huidige en toekomstige kosten, dan lijkt er toch sprake van misbruik van recht (artikel 3:13 BW) c.q. een gedraging in strijd met de zorgvuldigheid die men in het maatschappelijk verkeer tegenover elkaar heeft te betrachten (artikel 6:162 BW). In dat geval dient een kort geding te worden overwogen.

Bijlage G Verkeersmanagement voor rijkswegen

Rijkswaterstaat
Ministerie van Infrastructuur en Waterstaat

Bijlage G Verkeersmanagement voor rijkswegen

Bijlage bij Vraagspecificatie Proces

D&C Vervanging Verlichting Schipholtunnel
Zaaknummer: 31212908

Rijkswaterstaat
Ministerie van Infrastructuur en Waterstaat

Verkeersmanagement voor rijkswegen

Datum	27 februari 2025
Status	definitief

Colofon

Uitgegeven door	Ministerie van Infrastructuur en Waterstaat, Rijkswaterstaat, Verkeer en Watermanagement
Informatie	J. Slenters
Telefoon	06-15060924
E-mail	jacco.slenters@Rijkswaterstaat.nl
Uitgevoerd door	R. van Bemmel
Datum	27 februari 2025
Status	definitief
Versienummer	1.6

Inhoud

1 Inleidende informatie 4
1.1 Regio-indeling Rijkswaterstaat 4
1.2 Regio-indeling verkeerscentrales Rijkswaterstaat 6
1.3 Leeswijzer 6
1.4 Verkeersmaatregelen voor evenementen 6
1.5 Afkortingen en begrippen 7
2 Verkeersmanagement (VM) 9
2.1 Beschrijven verkeersmanagement 9
2.2 Beschrijven fasering verkeersmaatregelen 10
2.3 Slot aanvraag 11
2.4 Beschrijving verkeersmaatregelenplan 12
2.5 Beschrijving verkeersincidentmanagement 13
2.6 Uitgangspunten voor verkeersmanagement 14
2.7 Plaatsen informatieborden 15
2.8 Plaatsen kilometerborden 15
2.9 Aanvragen van een verkeersmaatregel 16
2.10 Aanvragen van een verkeersstop 17
2.11 Annuleren van een verkeersmaatregel 17
3 Richtlijnen, certificaten en ontheffingen voor verkeersmaatregelen (RL) 20

Bijlage G.A Informatievoorziening ter plaatse bij verkeersmaatregelen 23
Bijlage G.B Werkbare Uren (WBU), Venstertijden Afsluitingen (VTA) en werkvensters 26
Bijlage G.C Slot's 27
Bijlage G.D Verkeersmaatregelen 36

1 Inleidende informatie

Dit document is van toepassing wanneer verkeershinder op kan treden als gevolg van de te nemen verkeersmaatregelen bij activiteiten op, langs en/of in de nabijheid van de rijkswegen die in beheer zijn bij Rijkswaterstaat. Een activiteit kan onder andere uit te voeren werkzaamheden op, langs of nabij rijkswegen of een evenement die veel verkeer aantrekt op de rijksweg betreffen.

Verkeersmanagement zit in de DBFM en UAV-GC contracten van de Aanleg en Onderhoudsorganisaties van Rijkswaterstaat (GPO en PPO), maar andere organisatieonderdelen van Rijkswaterstaat en opdrachtgevers buiten Rijkswaterstaat bleken andere, soms verouderde, verkeersmanagementeisen voor rijkswegen toe te passen.

Dit document is opgesteld om voor Rijkswaterstaat een uniforme set van eisen aan het verkeersmanagement voor rijkswegen te stellen. Het document kan worden toegepast bij DBFM, UAV-GC en UAV contracten, ingenieursdienstcontracten en contracten van de Nationale Bewegwijzeringsdienst (NBd).

De terminologie in dit document is op zichzelf staand.

1.1 Regio-indeling Rijkswaterstaat

Rijkswaterstaat is een landelijke organisatie en is in 7 regio's onderverdeeld. In figuur 1 staat de onderverdeling van de regio's met de regionaam.



Figuur 1 RWS Regio-indeling



Figuur 2 RWS districtenindeling

De gegevens van de districten van Rijkswaterstaat zijn te vinden via www.rijkswaterstaat.nl/over-ons/contact/adressen/index.aspx

1.2 Regio-indeling verkeerscentrales Rijkswaterstaat

Rijkswaterstaat heeft 5 verkeerscentrales voor de rijkswegen. De verkeerscentrales zijn:

- Verkeerscentrale Midden-NL;
- Verkeerscentrale Noord-Oost-NL;
- Verkeerscentrale Noord-West-NL;
- Verkeerscentrale Zuid-NL;
- Verkeerscentrale Zuid-West-NL.

De adressen van de verkeerscentrales van Rijkswaterstaat zijn te vinden via www.rijkswaterstaat.nl/over-ons/contact/adressen/index.aspx

1.3 Leeswijzer

De eisen zijn zoveel mogelijk geformuleerd volgens een vast patroon met topeisen en onderliggende eisen. Voor de eenduidigheid zijn eisen voorzien van een ID-nummer bestaande uit twee beginletters die duiden op het proces waarop de eis betrekking heeft en een volgnummer. Deze twee beginletters zijn overigens in de hoofdstuk- en paragraaftitels tussen haakjes vermeld, zodat in de inhoudsopgave het ID-nummer eenvoudig terug te vinden is. Per eis is tevens een relatie aangegeven met één of meer bovenliggende eisen.

ID-nummer	Omschrijving eis / bepaling	Boven-liggende eis
XX100	*De opdrachtnemer dient …*	*XX010*

Naast de eisen zijn bepalingen opgenomen waaruit niet direct een verplichting voortvloeit voor de opdrachtnemer anders dan dat de opdrachtnemer rekening dient te houden met wat is bepaald. Het identificatienummer wordt dan voorafgegaan door "B-" van "Bepaling".

1.4 Verkeersmaatregelen voor evenementen

Wanneer een evenement veel verkeer trekt, dat kan leiden tot verkeershinder op de rijkswegen, dient de organisatie een partij in de hand te nemen die aan de gestelde eisen en bepalingen van dit document kan voldoen. De partij die namens de organisatie verantwoordelijk is voor de verkeersmaatregelen, staat gelijk aan de opdrachtnemer.

Voor de benodigde verkeersmaatregelen in geval van evenementen zijn de volgende eisen van toepassing:

Hoofdstuk of paragraaf	**Omschrijving**	**Eis / bepaling**
2	Richtlijnen, certificaten en ontheffingen voor verkeersmaatregelen	RL100, RL110, RL120, RL130 en RL140
3	Verkeersmanagement	VM010
§3.4	Beschrijving verkeersmaatregelenplan	VM400, VM410, VM420 en VM430
§3.5	Beschrijving incidentmanagement	VM500 en VM510
§3.7	Plaatsen informatieborden	VM700, VM710 en VM720
§3.9	Aanvragen van een verkeersmaatregel	VM900, VM910, B-VM920, B-VM930, VM940 en VM950
§3.11	Annuleren van een verkeersmaatregel	VM1120

Hoofdstuk of paragraaf	Omschrijving	Eis / bepaling
§3.12	Uitvoeren van een verkeersmaatregel	VM1200, B-VM1210, VM1220 en VM1230

1.5 Afkortingen en begrippen

In dit document worden de onderstaande afkortingen gebruikt.

Afkorting	Betekenis
DRIP	Dynamisch Route Informatie Paneel
RWS	Rijkswaterstaat
SPIN	Systeem Planning en Informatie Nederland
VTA	VensterTijden Afsluitingen
WBU	Werkbare Uren

In dit document worden de volgende begrippen toegepast:

Begrippen	Betekenis
Acceptatie	Een verklaring van geen bezwaar van de door de opdrachtnemer ter acceptatie voorgelegde documenten en aanvragen verkeersmaatregelen voor de activiteiten
Bedrijfscertificaat BRL9101	Een schriftelijke verklaring gebaseerd op de BRL9101 voor het gehele bedrijf dat verantwoordelijk is voor de verkeersmaatregelen
Bouwcommunicatie	Het afstemmen van de verkeersmaatregelen met belanghebbenden (weggebruikers, hulpdiensten omwonenden e.d.) en het informeren van weggebruikers voor en tijdens de verkeersmaatregel
Evenement	Een georganiseerde plaatselijke gebeurtenis die veel publiek trekt
Faseringsplan	Een beschrijving van de voorgenomen verkeersmaatregelen in verschillende fases
Go / no go criteria	Besliscriteria of de te plaatsen verkeersmaatregelen op het geplande tijdstip kunnen worden geplaatst
Hindercategorie	Categorie-indeling van het aantal gehinderde verkeersdeelnemers gekoppeld aan de mate van verkeershinder
Hinderklassen	De mate van verkeershinder ingedeeld in klassen
Hulppersonen	Dit kunnen enerzijds werknemers van de opdrachtnemer zijn, anderzijds kan het gaan om zelfstandig hulppersonen
Incidentmanagement	Het proces en de organisatie van de opdrachtnemer hoe en door wie wordt gehandeld bij verkeersincidenten ter plaatse van de verkeersmaatregelen
Informatieborden	Het informeren van de weggebruiker via borden langs de rijksweg
Informatiewagen	Het informeren van de weggebruiker m.b.v. verrijdbare digitale informatiedragers (bijvoorbeeld tekstwagens)
Nevenopdrachtnemer	Een opdrachtnemer van een andere overeenkomst die activiteiten uitvoert op, langs en/of nabij de rijksweg
Opdrachtgever	De natuurlijke of rechtspersoon die de opdrachtnemer opdraagt het werk en/of het activiteiten te verrichten
Opdrachtnemer	De natuurlijke of rechtspersoon, de aannemer, aan wie voor dit document het verkeersmanagement en het plaatsen van de verkeersmaatregelen is opgedragen
Persoonscertificaat	Een persoonsgebonden schriftelijke verklaring

Begrippen	Betekenis
Publiekscommunicatie	Het zichtbaar en herkenbaar neerzetten en op uniforme wijze eenduidige informatie over Rijkswaterstaat, de verkeersmaatregelen en eventuele omleidingsroutes voor de activiteiten en de daardoor veroorzaakte hinder te verstrekken
Rijkswaterstaat	Rijkswaterstaat is een rijksorganisatie die vertegenwoordigd wordt door de wegbeheerder en de verkeerscentrale. Bij werken van Rijkswaterstaat is ook de opdrachtgever een vertegenwoordiger van Rijkswaterstaat
Slot	Een projectspecifieke periode waarbinnen Rijkswaterstaat het acceptabel acht dat capaciteit aan een specifiek gedeelte van de rijksweg wordt onttrokken, waardoor de verkeershinder in een hindercategorie A, B of C valt. Dit geldt ook voor de zogenaamde "reserve" Slot
Venstertijden afsluiting	Zie B-VM620
Verbindingswegen	Het aansluiten van 2 kruisende wegen
Verkeershinder	Het hinderen van wegverkeer dat leidt tot langere reistijd
Verkeersmanagement	Het proces en organisatie van de opdrachtnemer hoe belanghebbenden worden geïnformeerd, hoe te komen tot verkeersmaatregelen om de activiteiten op, langs en/of in de nabijheid van de rijksweg door verkeersmaatregelen op een veilige manier worden afgeschermd en de verkeersveiligheid van de weggebruiker wordt geborgd
Verkeersstop	Het wegverkeer tijdelijk stilzetten (fysiek dan wel d.m.v. een slingermaatregel) voor werkzaamheden op, langs en/of in de nabijheid van de rijksweg waarbij de veiligheid van de wegwerker en/of weggebruiker in gevaar is
Voertuigverliesuren	Extra reistijd voor het aantal gehinderde voertuigen
Wegenverkeersreglement	Reglement verkeersregels en verkeerstekens (RVV 1990)
Werkbare uren	Zie B-VM615
Werkvensters	Zie B-VM630
Zelfstandig hulppersoon	Door de opdrachtnemer in te zetten onderaannemer of ZZP-er

2 Verkeersmanagement (VM)

VM010 De opdrachtnemer dient de werkzaamheden met betrekking tot verkeersmanagement te verrichten, zodanig dat veiligheid en minimale verkeershinder zijn gewaarborgd.

2.1 Beschrijven verkeersmanagement

VM100 Indien verkeersmaatregelen voor activiteiten op, langs en/of in de nabijheid van de rijksweg zullen leiden tot verkeershinder die valt binnen hinderklasse 1 tot en met 4, dan dient de opdrachtnemer een verkeersmanagementplan, waarmee de opdrachtnemer bewerkstelligt dat veiligheid en minimale verkeershinder zijn gewaarborgd, ter acceptatie voor te leggen aan Rijkswaterstaat. VM010

VM110 De opdrachtnemer dient in het verkeersmanagementplan ten minste te beschrijven: VM100

1. het proces verkeersmanagement;
2. een uitwerking van de projectorganisatie met betrekking tot verkeersmanagement;
3. de relatie met de planning;
4. de wijze waarop de verkeersmaatregelen, die voortvloeien uit de activiteiten op, langs en/of in de nabijheid van de rijksweg, in hinderklassen en hindercategorieën worden ingedeeld op basis van tabel 1 “Hindercategoriematrix”;
5. de communicatie met Rijkswaterstaat, gebaseerd op de minimale communicatietermijnen volgens tabel 2 “Communicatietermijnen per hindercategorie”;
6. de communicatie met de doelgroep voor bouwcommunicatie.

Hindercategoriematrix op basis van hinderklasse en aantal gehinderden						
		<1000	<10.000	<100.000	<1.000.000	>1.000.000
Hinderklasse 0: Geen hinder	-					
Hinderklasse 1: Kleine hinder	Geen file: extra vertraging < 5 minuten	E	E	D	C	B
Hinderklasse 2: Matige hinder	5 tot 10 minuten extra vertraging door file en/of omrijden	D	D	C	C	B
Hinderklasse 3: Grote hinder	10 tot 30 minuten extra vertraging door file en/of omrijden	C	C	B	A	A
Hinderklasse 4: Zeer grote hinder	30 tot 60 minuten extra vertraging door file en/of omrijden	C	B	B	A	A

Tabel 1 Hindercategoriematrix

Hindercategorie	Minimale communicatietermijn
A	26 weken
B	13 weken
C	6 weken
D	12 werkdagen
E	n.v.t.

Tabel 2 Communicatietermijnen per hindercategorie

2.2 Beschrijven fasering verkeersmaatregelen

VM200 Indien de opdrachtnemer fasering in verkeersmaatregelen toepast, dan dient de opdrachtnemer voor de hindercategorie A, B en C een faseringplan verkeersmaatregelen, waarmee de opdrachtnemer bewerkstelligt dat met de voorgenomen fasering van de verkeersmaatregelen de veiligheid en minimale verkeershinder zijn gewaarborgd, ter acceptatie voor te leggen aan Rijkswaterstaat. VM010, VM100

VM210 De opdrachtnemer dient in zijn faseringsplan verkeersmaatregelen per fase ten minste te beschrijven: VM200

1. het doel van de fase;
2. op hoofdlijnen van de toe te passen verkeersmaatregelen;
3. globale berekeningen van de extra reistijden en mogelijke vertragingen voor het om te leiden verkeer, waarbij rekening is gehouden met de verkeersintensiteiten en capaciteiten van het wegennet waarop de maatregelen betrekking hebben inclusief omleidingen en adviesroutes (op basis van bruto verkeershinder = zonder flankerende maatregel);
4. een globale risico-inventarisatie met betrekking tot:
   a. verkeersveiligheid;
   b. de doorstroming van het verkeer;
   c. uitloop geplande duur van de activiteiten op, langs en/of in de nabijheid van de rijksweg;
   d. hinderbetrouwbaarheid;
   e. sociale en maatschappelijke overlast;
   f. transport van gevaarlijke stoffen;
   g. bijzonder transport en
   h. de bereikbaarheid voor hulpverleningsdiensten rond afgesloten rijbanen en omleidingsroutes.

   Eén en ander inclusief de bijbehorende maatregelen om de risico's weg te nemen, te beperken of te beheersen;
5. een globale uitwerking van de afstemming ter zake:
   a. te treffen verkeersmaatregelen;
   b. in te stellen omleidingsroutes e.d. met andere Rijkswaterstaatonderdelen;
   c. hulpverleningsdiensten;
   d. ziekenhuizen;
   e. infrabeheerders;
   f. brandstofverkooppunten;
   g. relevante nevenopdrachtnemers en
   h. overige belanghebbenden;
6. berekeningen waaruit blijkt dat bestaande kunstwerken in de tijdelijke situatie ten minste blijven voldoen aan het bestaande constructieve veiligheidsniveau;
7. een globaal inzicht in de aanvoer-, afvoer- en omleidingsroutes (ook voor massa- en volumetransporten en transport gevaarlijke stoffen).

2.3 Slot aanvraag

VM300	Indien de opdrachtnemer één of meerdere Slot's, al dan niet gereserveerd door Rijkswaterstaat, nodig heeft voor zijn activiteiten op, langs en/of in de nabijheid van de rijksweg, dan dient de opdrachtnemer deze gemotiveerd aan te vragen bij en vast te laten stellen door Rijkswaterstaat, zodanig dat Rijkswaterstaat tijdig is geïnformeerd en Rijkswaterstaat Slot's tijdig kan opnemen in de landelijke planning.	VM010, VM100
B-VM310	Een Slot is een projectspecifieke periode waarbinnen Rijkswaterstaat het acceptabel acht dat capaciteit aan een specifiek gedeelte van de rijksweg wordt onttrokken met een hindercategorie A, B of C.	VM300
B-VM320	Indien Rijkswaterstaat Slot's heeft gereserveerd, dan zijn deze opgenomen in een tabel Slot's in Bijlage C "Slot's".	VM300
VM330	De opdrachtnemer dient een Slot zo spoedig mogelijk aan te vragen bij Rijkswaterstaat, doch uiterlijk, in geval van: 1. hindercategorie A: 29 weken voor aanvang verkeersmaatregelen; 2. hindercategorie B: 15 weken voor aanvang verkeersmaatregelen; 3. hindercategorie C: 8 weken voor aanvang verkeersmaatregelen.	VM300
VM340	De opdrachtnemer dient in zijn Slot-aanvraag ten minste te beschrijven: 1. een afweging tussen verkeershinder, de te nemen verkeersmaatregelen en de activiteiten op, langs en/of in de nabijheid van de rijksweg waarom een Slot noodzakelijk wordt geacht; 2. de indeling van de Slot's in hinderklassen en hindercategorieën op basis van de tabel 1 Hindercategoriematrix (op basis van bruto verkeershinder); 3. de begintijd / –datum en de eindtijd / –datum per aangevraagd Slot; 4. de onderbouwde berekeningen van de extra reistijden en mogelijke vertragingen voor het om te leiden verkeer, waarbij rekening is gehouden met de verkeersintensiteiten en capaciteiten van het wegennet waarop de maatregelen betrekking hebben inclusief omleidings- en adviesroutes; 5. een risico-inventarisatie met betrekking tot: a. verkeersveiligheid; b. de doorstroming van het verkeer; c. uitloop geplande duur van de activiteiten op, langs en/of in de nabijheid van de rijksweg; d. hinderbetrouwbaarheid; e. sociale en maatschappelijke overlast; f. transport van gevaarlijke stoffen; g. bijzonder transport en h. de bereikbaarheid voor hulpverleningsdiensten rond afgesloten rijbanen en omleidingsroutes; Eén en ander inclusief de bijbehorende maatregelen om de risico's weg te nemen, te beperken of te beheersen; 6. een uitwerking van de afstemming terzake: a. te treffen verkeersmaatregelen; b. in te stellen omleidingsroutes e.d.; c. met andere Rijkswaterstaatonderdelen; d. hulpverleningsdiensten;	VM330

e. ziekenhuizen;
f. wegbeheerders;
g. brandstofverkooppunten;
h. relevante nevenopdrachtnemers en
7. overige belanghebbenden;
8. het inzicht in de aanvoer-, afvoerroutes en omleidingsroutes (ook voor massa- en volumetransporten en transport gevaarlijke stoffen);
9. de extra adviesroutes.

B-VM350	Rijkswaterstaat verwerkt de vastgestelde Slot's in het programma SPIN. De opdrachtnemer krijgt van Rijkswaterstaat vanuit SPIN één of meerdere fasenummers die de opdrachtnemer dient te gebruiken bij het indienen van een verkeersmaatregelplan en bij het aanvragen van de verkeersmaatregel(en).	VM330

2.4 Beschrijving verkeersmaatregelenplan

VM400	De opdrachtnemer dient een verkeersmaatregelenplan, waarmee de opdrachtnemer bewerkstelligt dat met de te plaatsen verkeersmaatregel de veiligheid en minimale verkeershinder zijn gewaarborgd, ter acceptatie voor te leggen aan Rijkswaterstaat.	VM010
VM410	De opdrachtnemer dient in zijn verkeersmaatregelenplan de verkeersmaatregelen en per verkeersmaatregel ten minste in detail te beschrijven: 1. de toe te passen verkeersmaatregel inclusief het fasenummer dat is verstrekt door Rijkswaterstaat; 2. de afweging tussen de benodigde ruimte voor de werkzaamheden op, langs en/of in de nabijheid van de rijksweg en de resterende verkeersruimte; 3. de beschrijving van de werkzaamheden binnen de verkeersmaatregel; 4. een duidelijke situatietekening in kleur, inclusief alle relevante te plaatsen, aan te passen en/of te verwijderen bebording, bebakening en markering; 5. de tekst op de informatiewagens, omleidingsborden, DRIP's en vooraankondigingsborden; 6. de locaties van de te plaatsen routenummer- en pijlborden; 7. het relevante horizontale en verticale alignement en dwarsprofielen; 8. de in- en uitritten ten behoeve van het werkverkeer; 9. de telefoonnummers betrokken/relevante contactpersonen; 10. de begintijd / –datum en de eindtijd / –datum per aangevraagde verkeersmaatregel en omleiding; 11. de "go / no go"-criteria voor de start van de verkeersmaatregelen; 12. een uitwerking van de bewegwijzering ten behoeve van het aanduiden van omleidingsroutes in verband met afsluitingen; 13. schriftelijke goedkeuringen of verklaringen van geen bezwaar van de betrokken wegbeheerders voor het toepassen van de verkeersmaatregel; 14. een verklaring van geen bezwaar van de hulpverleningsdiensten.	VM400
VM420	Indien de verkeersmaatregelen voor de activiteiten leiden tot verkeershinder die vallen in hindercategorie A, B, C of D, dan dient de opdrachtnemer zijn verkeersmaatregelenplan uiterlijk vóór de termijn	VM400

voor concept verkeersmaatregelenplan volgens tabel 3 "Termijnen verkeersmaatregelenplan per hindercategorie", ter acceptatie voor te leggen aan Rijkswaterstaat.

VM430 Indien verkeersmaatregelen verkeershinder veroorzaken die vallen in hindercategorie A, B, C of D, dan dient de opdrachtnemer te bewerkstelligen dat zijn verkeersmaatregelenplan uiterlijk de termijn voor definitieve verkeersmaatregelenplan volgens tabel 3 "Termijnen verkeersmaatregelenplan per hindercategorie" door Rijkswaterstaat is geaccepteerd. VM420

B-VM440 Indien een beschrijving van een verkeersmaatregel is geaccepteerd, dan behoudt Rijkswaterstaat zich het recht voor, in geval van uitlopende en noodzakelijke activiteiten op het (parallelle) netwerk in hinderklasse 2 of hoger én vanaf hindercategorie C, de acceptatie daarvan in te trekken tot het moment waarop de helft van de in de tabel 1 "Communicatietermijnen per hindercategorie" genoemde minimale communicatietermijn voorafgaande aan de aanvang van de verkeersmaatregel is verstreken. Dit geeft de opdrachtnemer geen recht op bijbetaling of schadevergoeding. Rijkswaterstaat neemt in dat geval het initiatief tot het voorstellen van een nieuwe uitvoeringsperiode. VM430

Hindercategorie	Termijn concept verkeersmaatregelenplan	Termijn definitieve verkeersmaatregelenplan
A	18 weken	6 weken
B	11 weken	6 weken
C	8 weken	6 weken
D	6 weken (als maatregel in SPIN)	4 weken
E	n.v.t.	n.v.t.

Tabel 3 Termijnen verkeersmaatregelenplan per hindercategorie

2.5 Beschrijving verkeersincidentmanagement

VM500 Indien verkeersmaatregelen of de verwachte verkeersdrukte van een evenement vallen in hindercategorie A, B of C, dan dient de opdrachtnemer de beschrijving van de processen met betrekking tot verkeersincidentmanagement ter acceptatie voor te leggen aan Rijkswaterstaat. Met de beschrijving dient de opdrachtnemer te bewerkstelligen dat een drastische verkorting van files, ontstaan door ongelukken en pechgevallen in het verkeer, wordt gerealiseerd met technische maatregelen en door optimale samenwerking met hulpverleningsdiensten. VM010, VM100

VM510 De opdrachtnemer dient ten minste te beschrijven: VM500

1. het coördinatie en opschalingsmodel;
2. de 24 uur bereik- en beschikbaarheid van de contactpersoon voor de verkeersmaatregelen;
3. de bereikbaarheid per wegvak ten behoeve van de hulpverleningsdiensten;
4. de aanvoer- en afvoerroutes van de hulpverleningsdiensten;
5. de informatie voor de weggebruiker (inzet extra informatiewagens en teksten op DRIP's).

2.6 Uitgangspunten voor verkeersmanagement

VM600	De opdrachtnemer mag geen capaciteit aan het wegennet onttrekken buiten de vastgestelde werkbare uren (WBU), venstertijden afsluitingen (VTA), werkvensters en/of Slot's. Het opbouwen of afbreken van een verkeersmaatregel wordt ook gezien als het onttrekken van capaciteit.	VM010
VM605	Indien de opdrachtnemer mogelijkheid ziet de uitgangspunten ten aanzien van verkeersmanagement te verbeteren, dan dient de opdrachtnemer gemotiveerde voorstellen tot wijziging welke strekken tot een totale vermindering van de totale verkeershinder (waaronder hinderbeleving) ter acceptatie voor te leggen aan Rijkswaterstaat. Ten aanzien van de door Rijkswaterstaat vastgestelde WBU, VTA, werkvensters en Slot's kan vroegtijdig een voorstel tot wijziging worden ingediend als daardoor verkeershinder geminimaliseerd kan worden. Het afwijzen van voorstellen tot wijziging geeft de opdrachtnemer geen recht op bijbetaling of schadevergoeding.	VM600
B-VM610	Rijkswaterstaat heeft WBU, VTA en werkvensters vastgesteld welke zijn opgenomen in een tabel WBU, VTA en werkvensters in Bijlage AB "Werkbare Uren (WBU), Venstertijden Afsluitingen (VTA) en werkvensters".	VM600
B-VM615	De WBU zijn door Rijkswaterstaat vooraf bepaalde periodes (momenten/tijdstippen) waarin tussen bepaalde begin- en eindpunten rij- en/of vluchtstroken aan het wegennet kunnen worden onttrokken, waarbij maximaal hinderklasse 1 kan ontstaan.	B-VM610
B-VM620	De VTA zijn door Rijkswaterstaat, onafhankelijk van een specifiek project, bepaalde en tussen aangegeven begin- en eindpunten vastgestelde periodes, waarbinnen Rijkswaterstaat het acceptabel acht dat een specifiek weggedeelte (zoals toe- en afritten, verbindingswegen en tunnels) wordt afgesloten. De VTA vallen ten hoogste in hindercategorie D.	B-VM610
B-VM630	Werkvensters zijn door Rijkswaterstaat vooraf bepaalde periodes (momenten/tijdstippen), aansluitend aan de voor dat weggedeelte vastgestelde WBU, waarin tussen bepaalde begin- en eindpunten de wegcapaciteit kan worden teruggebracht tot één rijstrook en waarbij maximaal 15 minuten vertraging optreedt. Deze maatregelen worden qua flankerende maatregelen altijd als hinderklasse 1 beschouwd, maar moeten in de aanvraag van de verkeersmaatregel wel als hinderklasse 2 worden aangevraagd.	B-VM610
VM640	De opdrachtnemer mag alleen werkvensters gebruiken als het totale aantal WBU dat erop volgt wordt benut voor de te verrichten werkzaamheden op, langs en/of in de nabijheid van de rijksweg.	VM600
VM650	De opdrachtnemer mag tijdens de werkvensters geen rijdende afzettingen toepassen.	VM640
B-VM660	De WBU, VTA en werkvensters worden jaarlijks geactualiseerd en per 1 oktober voor het volgend kalenderjaar vastgesteld en aan de opdrachtnemer verstrekt.	B-VM610
VM670	De opdrachtnemer dient bij langjarige contracten rekening te houden	B-VM660

met een jaarlijkse gemiddelde afname van de WBU, VTA en werkvensters, vermeld in bijlage B "Werkbare Uren (WBU), Venstertijden Afsluitingen (VTA) en werkvensters".

VM680	Wijzigingen van de WBU, VTA en werkvensters geven de opdrachtnemer in beginsel geen recht op bijbetaling of schadevergoeding tenzij de opdrachtnemer aantoont dat de afname van de WBU en/of werkvensters meer bedraagt dan het in Bijlage B "Werkbare Uren (WBU), Venstertijden Afsluitingen (VTA) en werkvensters" genoemde percentage. In dat geval dient de opdrachtnemer uiterlijk binnen 2 maanden na publicatie van de WBU een motivering voor een kostenvergoeding in te dienen bij de opdrachtgever.	VM670
B-VM690	Indien de opdrachtnemer buiten de overeengekomen WBU, VTA, werkvensters en Slot's toch capaciteit aan het wegennet onttrekt, dan zal per geval en per 15 minuten een boete worden opgelegd van € 10.000,=.	VM600

2.7 Plaatsen informatieborden

VM700	De opdrachtnemer dient, bij afsluiting van een rijbaan of verbindingsweg (toe- of afrit) en bij een fasering vanaf hinderklasse 2, 2 weken voorafgaande aan de geplande verkeersmaatregelen, vooraankondigingsborden te plaatsen en deze gelijktijdig met de verkeersmaatregelen te verwijderen.	VM010
VM710	Indien sprake is van de volgende situaties: 1. het niet zichtbaar voor de weggebruiker verrichten van activiteiten op, langs en/of in de nabijheid van de rijksweg, of; 2. een vertraging voor de weggebruiker van meer dan 15 minuten, of; 3. kans op file op voor de weggebruiker onverwachte locatie, dan dient de opdrachtnemer direct voorafgaande aan de verkeersmaatregelen, ter plaatse van elke verkeersmaatregel , informatiewagens en/of informatieborden te plaatsen en deze gelijktijdig met de verkeersmaatregelen te verwijderen:	VM010
VM720	Indien de opdrachtnemer een informatiewagen toepast, dan dient de informatiewagen uitsluitend één beeldstand te tonen.	VM710

2.8 Plaatsen kilometerborden

VM800	Indien de verkeersmaatregel er toe leidt dat er: 1. geen vluchtstrook aanwezig is, of; 2. een afname van het aantal rijstroken is, of; 3. een snelheidsbeperking van 70 of 90 km/u is, dan dient de opdrachtnemer bij een verkeersmaatregel met een lengte van ten minste 3 km en een tijdsduur van ten minste 24 uur, voor de duur van die verkeersmaatregel kilometerborden te plaatsen.	VM010
VM810	De opdrachtnemer dient ter hoogte van het nulpunt in de verkeersmaatregel een kilometerbord te plaatsen met daarop de totale lengte van de verkeersmaatregel, afgerond op hele kilometers.	VM800

VM820	De opdrachtnemer dient aan het einde van de verkeersmaatregel een kilometerbord “bord einde werkzaamheden Rijkswaterstaat” te plaatsen.	VM800
VM830	Indien bovengenoemde verkeersmaatregel langer duurt dan 14 dagen, dan dient de opdrachtnemer iedere 3 km, gezien vanaf het einde van de verkeersmaatregel eveneens kilometerborden te plaatsen met daarop de resterende lengte van de verkeersmaatregel, afgerond op hele kilometers.	VM800
VM840	De opdrachtnemer dient de kilometerborden aan één zijde van de rijbaan te plaatsen.	VM800
VM850	Het ontwerp van de kilometerborden dient te voldoen aan de vigerende “Huisstijlrichtlijnen bouwborden Rijkswaterstaat”, zoals gepubliceerd op de site www.rws.nl/bouwborden dan wel een daarvoor in de plaats tredende site.	VM800

2.9 Aanvragen van een verkeersmaatregel

VM900	De opdrachtnemer dient de te treffen verkeersmaatregelen aan te vragen bij het verkeersloket van Rijkswaterstaat met behulp van het programma SPIN. Indien verkeersmaatregelen voor fasering vallen in hindercategorie A, B en C, dan kan de opdrachtnemer de verkeersmaatregelen inclusief het fasenummer pas aanvragen nadat het verkeersmaatregelplan is geaccepteerd. De opdrachtnemer kan toegang krijgen tot het programma SPIN door een verzoek in te dienen bij Rijkswaterstaat. De opdrachtnemer ontvangt vervolgens van Rijkswaterstaat de handreiking SPIN.	VM010, VM400
VM910	De opdrachtnemer dient uiterlijk 12 werkdagen vóór de week van uitvoering de verkeersmaatregelen in SPIN te hebben aangevraagd.	VM900
B-VM920	De opdrachtnemer ontvangt uiterlijk de tweede vrijdag vóór de week van uitvoering bericht of toestemming wordt verleend voor de te treffen verkeersmaatregelen inclusief het betreffende aanvraagnummer uit SPIN van Rijkswaterstaat. Rijkswaterstaat stemt voorts intern af met de verkeerscentrale van Rijkswaterstaat.	VM910
B-VM930	Een aanvraag voor een verkeersmaatregel wordt binnen de totale verkeersmaatregelenplanning voor de rijksweg beoordeeld op te verwachten hinder voor de weggebruiker. Zo kunnen door omleidingsroutes, evenementen, overige verkeersmaatregelen, vakantieperioden etc. de intensiteiten op specifieke locaties tijdelijk sterk afwijken van de intensiteiten op basis waarvan de WBU en werkvensters zijn berekend.	B-VM920
VM940	Indien er sprake is van niet voorziene verkeersonveilige omstandigheden, dan kan de opdrachtnemer, in aanvulling op en in afwijking van hetgeen is bepaald, direct een urgente verkeersmaatregel aanvragen bij de verkeerscentrale van Rijkswaterstaat. De opdrachtnemer dient voor het plaatsen daarvan toestemming te vragen bij de voor de regio verantwoordelijke verkeerscentrale van Rijkswaterstaat (zie §1.2). Het niet instemmen door de verkeerscentrale van Rijkswaterstaat met een aangevraagde urgente verkeersmaatregel geeft de opdrachtnemer	VM010

geen recht op bijbetaling of schadevergoeding.

VM950	Indien een urgente verkeersmaatregel wordt getroffen, dan dient de opdrachtnemer dit aan Rijkswaterstaat te melden.	VM940

2.10 Aanvragen van een verkeersstop

VM1000	Indien de opdrachtnemer een verkeersstop wenst aan te vragen, dan dient dit te geschieden via het programma SPIN.	VM010, VM400, VM900
VM1010	De opdrachtnemer dient bij het aanvragen van een verkeersstop te motiveren waarom de verkeersstop noodzakelijk is.	VM1000
B-VM1020	Een verkeersstop is niet toegestaan, tenzij: 1. een verkeersmaatregel waarbij het verkeer uiterst links rijdt omgezet moet worden naar uiterst rechts, of vice versa en waarbij tevens òf: a. deels losliggend materiaal binnen de verkeersmaatregel niet voor het omzetten van het verkeer kan worden verwijderd; òf b. een rijstrook vanwege verrichte activiteiten nog niet bereden mag worden; 2. activiteiten aan een object (boven de rijbaan) zodanig moeten worden verricht dat de veiligheid van de weggebruiker/wegwerker in het geding is; 3. de file van de vorige verkeersstop op het traject voor de locatie van de verkeersstop is opgelost; 4. de verwachte file is opgelost voor het einde van de vastgestelde WBU.	VM1000
B-VM1030	Een verkeersstop mag alleen worden uitgevoerd door de politie of een weginspecteur van Rijkswaterstaat die daarvoor bevoegd is.	VM1000
B-VM1040	Een verkeersstop mag in geen geval langer duren dan 15 minuten. Bij uitloop van activiteiten op, langs en/of in de nabijheid van de rijksweg waarbij de genoemde termijn van 15 minuten wordt overschreden, is Rijkswaterstaat gerechtigd de verkeersstop te beëindigen. De opdrachtnemer kan hieraan geen recht op bijbetaling of schadevergoeding ontlenen.	VM1000
VM1050	De opdrachtnemer dient er rekening mee te houden dat een aangevraagde verkeersstop door bijzondere omstandigheden te laat of niet kan plaatsvinden. De opdrachtnemer kan hieraan geen recht op bijbetaling of schadevergoeding ontlenen.	VM1000

2.11 Annuleren van een verkeersmaatregel

VM1100	Indien de opdrachtnemer de door hem aangevraagde en door Rijkswaterstaat toegestane verkeersmaatregelen wenst te annuleren, dan dient de opdrachtnemer het verzoek voorzien van een deugdelijke motivering uiterlijk om 14.00 uur op de dag voorafgaand aan het begintijdstip van de geplande verkeersmaatregelen voor te leggen aan Rijkswaterstaat. In geval van weekendwerkzaamheden vanaf hindercategorie C geldt een tijdstip van uiterlijk donderdag om 12.00 uur.	VM900

B-VM1110	In geval van annulering van de verkeersmaatregelen zullen de door Rijkswaterstaat gemaakte kosten ten aanzien van (de communicatie van) de geannuleerde verkeersmaatregelen alsmede extra gemaakte kosten worden verhaald, tenzij de opdrachtnemer aantoont dat er sprake is van aan hem niet verwijtbare oorzaken die ten grondslag liggen aan het verzoek tot annulering.	VM1100
VM1120	Indien de activiteiten op, langs en/of in de nabijheid van de rijksweg waarvoor de verkeersmaatregelen zijn aangevraagd worden afgelast/uitgesteld, dan dient de opdrachtnemer de afgelasting/ het uitstel onmiddellijk te melden aan de belanghebbenden en in SPIN de maatregelen terug te trekken. Indien het een Slot betreft, dan dient de opdrachtnemer aan Rijkswaterstaat te melden dat de fases van een Slot worden ingetrokken.	VM1100

2.12 Uitvoeren van een verkeersmaatregel

VM1200	De opdrachtnemer dient ten aanzien van elke te plaatsen verkeersmaatregel direct voor aanvang de begintijd en direct na beëindiging de eindtijd telefonisch te melden aan de voor de regio verantwoordelijke verkeerscentrale van Rijkswaterstaat (zie §1.2) onder vermelding van het betreffende aanvraagnummer uit SPIN.	VM010, VM400
B-VM1210	Als begintijd voor de verkeersmaatregel wordt het tijdstip van aanvang van het plaatsen van de verkeersmaatregel op de rijksweg genomen en als eindtijd het tijdstip waarop alle met de betreffende verkeersmaatregel verband houdende materialen en hulpmiddelen van de rijksweg zijn verwijderd en de rijksweg volledig beschikbaar is voor het verkeer.	VM1200
VM1220	Indien de opdrachtnemer voorziet dat de geplande eindtijd van de verkeersmaatregel zal worden overschreden, dan dient de opdrachtnemer dit, ten behoeve van publiekscommunicatie door Rijkswaterstaat, terstond te melden aan de verkeerscentrale van Rijkswaterstaat.	VM1200
VM1230	De opdrachtnemer dient tijdens het aan- en/of afmelden van een verkeersmaatregel de nummerherkenning van de telefoon van de opdrachtnemer aan te hebben staan.	VM1200
B-VM1240	Rijkswaterstaat behoudt zich het recht voor het tijdstip van aanvang van het plaatsen van een verkeersmaatregel bij te stellen en om een verleende toestemming voor plaatsen en/of verwijderen van verkeersmaatregelen in te trekken afhankelijk van de actuele verkeersintensiteit en weersomstandigheden.	VM1200
VM1250	De opdrachtnemer dient het plaatsen van een (niet geplande) tijdelijke snelheidsbeperkende maatregel terstond te melden aan de verkeerscentrale van Rijkswaterstaat. Een snelheidsbeperkende maatregel kan niet eerder worden opgeheven dan met toestemming van de verkeerscentrale van Rijkswaterstaat.	VM010
VM1260	Zodra de (niet geplande) tijdelijke snelheidsbeperkende maatregel is opgeheven, dient de opdrachtnemer dit terstond te melden aan de verkeerscentrale van Rijkswaterstaat.	VM1250

B-VM1270	Rijkswaterstaat zal, voor aanmelding van de verkeersmaatregelen binnen de WBU, VTA en werkvensters voor wegvakken waarop signalering aanwezig is, alleen toestemming tot het treffen van de verkeersmaatregelen verlenen indien op dat moment de gemiddelde snelheid van het verkeer op het betreffende wegvak hoger is dan 70 kilometer per uur en indien het onttrekken van rijstroken aan het betreffende wegvak niet leidt tot een hogere verkeersintensiteit dan de in Bijlage B “Werkbare Uren (WBU), Venstertijden Afsluitingen (VTA) en werkvensters” aangegeven aantal motorvoertuigen per uur op elk van de overgebleven rijstroken.	VM1200 B-VM1240
B-VM1280	Rijkswaterstaat zal, voor de aanmelding van de verkeersmaatregelen binnen de werkvensters, voor wegvakken waarop signalering aanwezig is, alleen toestemming tot het treffen van (een) verkeersmaatregel(en) verlenen indien op dat moment de gemiddelde snelheid van het verkeer op het betreffende wegvak hoger is dan 70 kilometer per uur.	VM1200 VM1250

3 Richtlijnen, certificaten en ontheffingen voor verkeersmaatregelen (RL)

RL100	De opdrachtnemer dient bij het plannen en toepassen (waaronder ontwerpen, plaatsen, in stand houden, verwijderen) van verkeersmaatregelen te voldoen aan: 1. de CROW-publicatie "Beleid en proces, Werk in Uitvoering 96a/96b - 2020" inclusief erratum, de CROW-publicatie "Specificaties voor Materiaal en Materieel, Werk in Uitvoering 96a/96b - 2020" inclusief erratum; 2. bij autosnelwegen: de CROW-publicatie "Werken op autosnelwegen, Werk in Uitvoering 96a - 2020" inclusief erratum, de CROW-publicatie "Standaardmaatregelen op autosnelwegen, Werk in Uitvoering 96a - 2020" inclusief erratum; 3. bij overige (rijks)wegen: de CROW-publicatie "Werken op niet-autosnelwegen, Werk in Uitvoering 96b - 2020" inclusief erratum, de CROW-publicatie "Standaardmaatregelen op niet-autosnelwegen, Werk in Uitvoering 96b - 2020" inclusief erratum; 4. Bijlage A "Informatievoorziening ter plaatse bij verkeersmaatregelen"; 5. de richtlijnen en eisen van overige wegbeheerders met betrekking tot verkeersmanagement op het onderliggende wegennet.	VM010
RL101	Indien instandhouding van het areaal tot de opdracht behoort, dan dient de opdrachtnemer op verzoek van de Weginspecteur bij een verkeersincident veiligheidsmaatregelen te treffen en te voldoen aan de richtlijn "Aanvullende Veiligheidsmaatregelen bij langdurige Incidenten versie 1_0_5".	VM010
RL110	De opdrachtnemer, dan wel zelfstandige hulppersoon die belast is met werkzaamheden met betrekking tot verkeersmaatregelen of veiligheidsmaatregelen, dient in het bezit te zijn van een BRL9101 procescertificaat, of gelijkwaardig, ten aanzien van de aan te wenden kennis en kunde inzake het toepassen van verkeersmaatregelen bij activiteiten op, langs en/of in de nabijheid van de rijksweg.	RL100
RL120	Indien de opdrachtnemer, dan wel zelfstandig hulppersoon, geen rijstroken hoeft af te sluiten voor het verkeer, dan volstaat voor alle hulppersonen, die belast zijn met werkzaamheden met betrekking tot verkeersmaatregelen, een persoonsgebonden certificaat zoals beschreven in de "BRL9101" of een gelijkwaardig certificaat. De bedoelde persoonsgebonden certificaten, conform de vigerende BRL9101 zijn: 1. medewerker tijdelijke verkeersmaatregelen; 2. vakman tijdelijke verkeersmaatregelen; 3. specialist tijdelijke verkeersmaatregelen (aanvrager SPIN-maatregel conform VM900).	RL110
RL130	De opdrachtnemer dient bij een persoonscertificaat aan te geven hoe in te zetten kennis en kunde gewaarborgd worden tijdens de ontwerp- en de uitvoeringswerkzaamheden met betrekking tot de verkeersmaatregelen.	RL120
RL140	De opdrachtnemer dient zorg te dragen dat hulppersonen, die betrokken zijn bij de activiteiten op, langs en/of in de nabijheid van de	RL100 VM010

	rijksweg, in het bezit zijn van een geldige, door Rijkswaterstaat te verstrekken, verklaring. Met deze verklaring wordt ontheffing verleend van artikelen van het Wegenverkeersreglement en het "Reglement verkeersregels en verkeerstekens", voor zover noodzakelijk voor de activiteiten op, langs en/of in de nabijheid van de rijksweg.	
RL150	De opdrachtnemer dient het in te zetten materieel, beschreven in de CROW-publicatie "Specificaties voor Materiaal en Materieel, Werk in Uitvoering 96a/96b - 2020", iedere 12 maanden te keuren door een onafhankelijk (zelfstandig) hulppersoon met een persoonsgebonden certificaat keuren materieel.	RL100
RL160	Een onafhankelijk keurende instelling dient de bevindingen te vermelden in een keuringsrapport en te registreren.	RL150

Referentielijst

Onderstaande referentielijst geeft een overzicht van de documenten waarnaar vanuit eisen wordt verwezen en die niet als bijlage bij dit document zijn gevoegd.

Omschrijving referentie	**Eis / bepaling**
CROW-publicatie "Beleid en proces, Werk in Uitvoering 96a/96b - 2020", Artikelnummer 526 d.d. 1 juli 2020 en erratum van 9 oktober 2024 ISBN 9789066286795	RL100
CROW-publicatie "Specificaties voor Materiaal en Materieel, Werk in Uitvoering 96a/96b - 2020", Artikelnummer 525 d.d. 1 juli 2020 en erratum van 9 oktober 2024 ISBN 9789066286788	RL100
CROW-Publicatie "Werken op autosnelwegen, Werk in Uitvoering 96a - 2020", Artikelnummer 529 d.d. 1 juli 2020 en erratum van 9 oktober 2024 ISBN 9789066286818	RL100
CROW-Publicatie "Standaardmaatregelen op autosnelwegen, Werk in Uitvoering 96a - 2020", Artikelnummer 530a d.d. 1 juli 2020 en erratum van 9 oktober 2024 ISBN 9789066286825	RL100
CROW-publicatie "Werken op niet-autosnelwegen, Werk in Uitvoering 96b - 2020", Artikelnummer 527 d.d. 1 juli 2020 en erratum van 9 oktober 2024 ISBN 9789066286801	RL100
CROW-publicatie "Standaardmaatregelen op niet-autosnelwegen, Werk in Uitvoering 96b - 2020", Artikelnummer 530b d.d. 1 juli 2020 en erratum van 9 oktober 2024 ISBN 9789066286832	RL100
Aanvullende Veiligheidsmaatregelen bij langdurige Incidenten versie 1_0_5 https://werkwijzerrws.intranet.rws.nl/link/standaard/5878	RL101

Bijlage G.A Informatievoorziening ter plaatse bij verkeersmaatregelen

Omschrijving	**Standaardtekst**
Aanleg werkzaamheden	Aanleg…
Specifiek object niet bereikbaar	... niet bereikbaar
Eén rijstrook dicht na afrit …	1 rijstrook dicht na afrit ...
Calamiteit / ongeval / Rijksweg dicht	A… dicht volg …..
Aanbrengen figuratie	Aanbrengen wegmarkering
Afrit afgesloten	Afrit .. dicht, draaien bij afrit ..
Na asfalteren	Asfalt koelt af
Tijdens asfalteringswerkzaamheden	Asfalt werkzaamheden
Maai- en opruimwerk	Bermen maaien ….. km
Einde verkeersmaatregel	Dank voor uw begrip
Korte invoegstrook	Korte invoegstrook
Korte uitvoegstrook	Korte uitvoegstrook
Ontbrekende markering	Markering ontbreekt
Omleiding	Omleiding volg ….
Onderhoud brug	Onderhoud brug
Onderhoudswerkzaamheden dijk	Onderhoud dijk
Onderhoud portaal	Onderhoudswerkzaamheden
Putten zuigen	Onderhoud riolering ….. km
Onderhoudswerkzaamheden sluizen	Onderhoud sluizen
Onderhoud verlichting	Onderhoud verlichting
Onderhoud tunnel	Onderhoud tunnel
Onderhoud viaduct	Onderhoud viaduct
Verschoven rijstroken	Ook vluchtstrook gebruiken
Wegafzetting wordt opgebouwd	Opbouwen wegafzetting
Parkeerplaats dicht	Parkeerplaats dicht
Repareren geleiderail	Repareren vangrail
Reparatie wegdek	Repareren wegdek
Vullen rijsporen	Repareren wegdek
Ongeval/omleiding	Richting ... volg …
Onderhoud / storing signalering	Filewaarschuwing buiten gebruik
Gewijzigde situatie	Situatie gewijzigd
Slecht wegdek	Slecht wegdek
Aanbrengen belijning	Strepen trekken
Tankstation niet bereikbaar	Tankstation niet bereikbaar
Oprit afgesloten	Oprit dicht volg …..
Rijstroken zijn versmald	Versmalde rijstroken
Wegafzetting wordt verwijderd	Verwijderen wegafzetting
Meetwerkzaamheden over grotere afstand dan 2 km	Metingen wegdek
Beperkt aantal rijstroken beschikbaar	.. rijstroken beschikbaar
Duur van het werk (periode)	Werkzaamheden 12/7 – 18/7
Duur van het werk	Werkzaamheden tot 12/6 12h

Bij onvoorziene omstandigheid

Onvoorziene omstandigheid	Standaard tekst
Calamiteit / ongeval / Rijksweg gestremd	… dicht volg ….. … dicht
	
Afgevallen lading	Afgevallen lading
Afrit afgesloten	Afrit dicht volg …..
Olie op de weg	Olie op de weg 
Calamiteit / ongeval *Icm J34 – Ongeval*	Ongeval op A… volg … Ongeval: ook vluchtstrook gebruiken Ongeval: … rijstroken dicht Ongeval: rijstrook dicht Ongeval: A… dicht 
Reinigen wegdek (m.u.v. olie)	Reinigen wegdek
Calamiteit / ongeval / omleiding	Richting ... volg …
Slecht wegdek	Slecht wegdek 
Technisch onderzoek ongeval	Technisch onderzoek ongeval
Oprit afgesloten	Oprit dicht volg …..
Verkeerslichten knipperen of zijn gedoofd	Verkeerslichten buiten werking
Spitsstrook afgesloten wegens omstandigheden	Spitsstrook dicht i.v.m. …
Kans op file	Filevorming 

Prioriteitsvolgorde te tonen teksten
Indien meerdere teksten mogelijk zijn, wordt op basis van de volgende prioriteitsvolgorde een tekst gekozen:
1. acuut gevaar;
2. omleidingen / afsluitingen;
3. waarschuwen over verkeerssituatie;
4. informatie over de verkeersmaatregelen;
5. informatie over de feitelijke werkzaamheden.

Bijlage G.B Werkbare Uren (WBU), Venstertijden Afsluitingen (VTA) en werkvensters

De tabel met WBU, VTA en werkvensters voor Schipholtunnel:

Tunnelbuis	Tijdvak van	Tijdvak tot
Oost 1	23.00 uur	5.00 uur
Oost 2	21.00 uur	5.00 uur
West 1	23.00 uur	5.00 uur
West 2	21.00 uur	5.00 uur

NB: Deze werkbare uren waren in 2025 van kracht. Deze kunnen jaarlijks worden bijgesteld aan de hand van het verkeersaanbod.

Bijlage G.C Slot's

De door Rijkswaterstaat bepaalde Slot’s voor de Schipholtunnel.

Tunnelbuis en periode
West 2 (parallelbaan): maandag 14 juni 2027 21.00 uur tot/met dinsdag 22 juni 2027 5.00 uur
West 1 (hoofdrijbaan): maandag 26 juli 2027 23.00 uur tot/met maandag 2 augustus 2027 23.59 uur
Oost 2 (parallelbaan): dinsdag 3 augustus 2027 0.00 uur tot/met maandag 9 augustus 2027 23.59 uur
Oost 1 (hoofdrijbaan): dinsdag 10 augustus 2027 0.00 uur tot/met dinsdag 17 augustus 2027 5.00 uur

Slotaanvraagformulier RWS West-Nederland Noord

In te vullen door Opdrachtnemer
In te vullen door Opdrachtgever

De opdrachtnemer dient bij mailverkeer richting douwe.de.vries@rws.nl en WNN-minderhinder@rws.nl in het onderwerp te starten met het contractnummer gevolgd door locatie.

Algemene informatie

versie 1-12-2018

Algemene informatie slotaanvraag hinder (vaar)wegen				
Registratienummer viewer	*27- _ _ _*			
ID-nummer RTT	*RWS006860 west, RWS006861 oost*			
Spinnummer	Volgt na akkoord RWS			
Datum aanvraag	21-03-2025			
Projectbenaming	Vervangen verlichting Schipholtunnel			
Contractnummer	31206777			
Contractnaam	Groot onderhoud en update tunnels GOUT			
Status	Nog aan te besteden			
Aanbestedingsdatum	01-09-2026			
Uitvoeringsdatum van/tot	14-06-2027 t/m 17-08-2027			
Opdrachtnemer	*Nog onbekend*			
Contactgegevens Opdrachtnemer				
Omgevingsmanager	Nog onbekend			
Projectmanager	Nog onbekend			
Technisch manager	Nog onbekend			
Contractmanager	Nog onbekend			
Contactgegevens Opdrachtgever				
Omgevingsmanager	*Ed Nijman, 06-15169364, ed.nijman@rws.nl*			
Projectmanager	*Jeroen Papenhuijzen, 06-11840801, jeroen.papenhuijzen@rws.nl*			
Technisch manager	*Martijn Heemink, 06-50197295, martijn.heemink@rws.nl*			
Contractmanager	*Dennis Kuiper, 06- 11526204, dennis.kuijper@rws.nl*			
Verkeersmanager district	*Douwe de Vries, 06-52077254, douwe.de.vries@rws.nl*			
Mijlpalen				
Verwachte ingebruikname	16 augustus 2027			
Hinderdata				
Hinderperiode	startdatum	14-06-2027	einddatum	17-08-2027
Hinderperiode alternatief*	startdatum	2028	einddatum	2028
Schiphol Airport is schriftelijk akkoord met het buis na buis afsluiten van de Schipholtunnel voor het vervangen van de verlichting. De duur van de afsluiting per buis is maximaal een week. In een overleg op 21 februari 2025 hebben we gezamenlijk de volgorde en de tijdsperiode bepaald en daar zijn onderstaande afsluitingen uit voortgekomen. De wens van Schiphol Airport om een doorsteek te realiseren van de parallelbaan naar de hoofdrijbaan Oost heeft TBO en VM gehonoreerd en deze kunnen we in 2025/2026 realiseren. In het bestuurlijk overleg van 6 mei 2025 tussen Schiphol Airport en Rijkswaterstaat wordt de afsluiting toegelicht.				
Datum slotaanvraag ontvangen				
Datum slotaanvraag goedgekeurd				

Hinderinformatie

Hinderplanning wegen* (hoofdfasering)				
Korte werkomschrijving	**Schipholtunnel afsluiting westbuis 2 week 24/25 ivm vervangen van de verlichting**			*Omschrijving werkzaamheden: bv onderhoud/vervanging object of traject*
Locatieaanduiding				
Traject, wegnummer	Wegnummer(s)	A4		
	Wegbeheerder(s)	West Nederland Noord District Zuid		
Traject, hmp	Van hmp/knp.	Km. 5,30	Tot hmp/knp.	Km. 7,70
Rijrichting	HRR/HRL/beide	PRR		
Hinderperiode hoofdfasering	Startdatum: Tijd:	14-06-2027 21:00	Einddatum: Tijd:	22-06-2027 5:00
Dagdeel	*Permanent*		*Weekend/nacht/permanent*	
Verkeersmaatregel	*Afsluiting*		*type CROW-fig of afsluiting*	
Verwachte hinderklasse	*3*		*0,1,2,3,4 (afsluiting is min. hkl. 2)*	
Vertragingstijd	*30-60 minuten*		*Werkvak +evt. file of omrijdtijd*	
Hindercategorie	*A*		*A/B/C/D*	
Aantal gehinderden	*552.000*		*Mvt tijdens periode*	
Max. snelheid werkvak	*70*		*Km/uur*	
Reductie	*100*		*0-100 (100+volledige afsluiting)*	
Omleidingsroutes (indien van toepassing)				
Route 1	Het verkeer wordt omgeleid via de hoofdrijbaan west 1. Schiphol is bereikbaar via de doorsteek ter hoogte van km 7.8.			*Wegnummer+knooppunt*
Route 2				*Wegnummer+knooppunt*
OV en hulpdiensten				
Busroute	Omleiding volgen.		*Afspraak met busmaatschappij*	
Hulpdiensten	Nood/hulpdiensten met prio 1 kunnen op gepaste snelheid door het werkvak.		*Afspraak met hulpdiensten*	
Informatie t.b.v. Van A naar Beter				
Wat	Vervangen van de verlichting van de Schipholtunnel.		*Korte omschrijving bv aanleg spitsstrook*	
Waarom	Groot onderhoud is nodig om de werking te garanderen. Doordat LED wordt aangebracht levert dit een flinke energiebesparing op.		*Korte omschrijving waarom de werkzaamheden worden uitgevoerd*	
Welke hinder	Schipholtunnel westelijke parallelbuis is afgesloten, verkeer via de westelijke hoofdrijbaan.		*Omschrijving van de hinder tbv weggebruiker*	

Toelichting:
Berekening op basis van cijfers van 2024. De hinderberekening is lastig te maken. Er is te veel verkeer voor één korte slinger naar West 2 (2100 mvt/u met capaciteit van 1700 mvt/u). Hierdoor ontstaat hinder op de hoofdrijbaan. FOSIM komt uit op 5+ kilometer langzaam rijdend verkeer (10-30 km/u). We passen verkeersmanagement, mobiliteitsmaatregelen en publiekscommunicatie toe om het aantal gehinderden te verminderen, conform de Hinderaanpak.

Hinderinformatie

Hinderplanning wegen* (hoofdfasering)				
Korte werkomschrijving	**Schipholtunnel afsluiting westbuis 1 week 30/31 ivm vervangen van de verlichting**			*Omschrijving werkzaamheden: bv onderhoud/vervanging object of traject*
Locatieaanduiding				
Traject, wegnummer	Wegnummer(s)	A4		
	Wegbeheerder(s)	West Nederland Noord District Zuid		
Traject, hmp	Van hmp/knp.	Km. 5,30	Tot hmp/knp.	Km. 8,14
Rijrichting	HRR/HRL/beide	HRR		
Hinderperiode hoofdfasering	Startdatum: Tijd:	26-07-2027 23:00	Einddatum: Tijd:	02-08-2027 24:00
Dagdeel	*Permanent*		*Weekend/nacht/permanent*	
Verkeersmaatregel	*Afsluiting*		*type CROW-fig of afsluiting*	
Verwachte hinderklasse	*4*		*0,1,2,3,4 (afsluiting is min. hkl. 2)*	
Vertragingstijd	*60+*		*Werkvak +evt. file of omrijdtijd*	
Hindercategorie	*A*		*A/B/C/D*	
Aantal gehinderden	*470.000*		*Mvt tijdens periode*	
Max. snelheid werkvak	*70*		*Km/uur*	
Reductie	*100*		*0-100 (100+volledige afsluiting)*	
Omleidingsroutes (indien van toepassing)				
Route 1	Het verkeer wordt omgeleid via rijksweg 9 en vervolgens rijksweg 5. Schiphol is bereikbaar via de west 2 parallelbuis.			*Wegnummer+knooppunt*
Route 2				*Wegnummer+knooppunt*
OV en hulpdiensten				
Busroute	Omleiding volgen.		*Afspraak met busmaatschappij*	
Hulpdiensten	Nood/hulpdiensten met prio 1 kunnen op gepaste snelheid door het werkvak.		*Afspraak met hulpdiensten*	
Informatie t.b.v. Van A naar Beter				
Wat	Vervangen van de verlichting van de Schipholtunnel.		*Korte omschrijving bv aanleg spitsstrook*	
Waarom	Groot onderhoud is nodig om de werking te garanderen. Doordat LED wordt aangebracht levert dit een flinke energiebesparing op.		*Korte omschrijving waarom de werkzaamheden worden uitgevoerd*	
Welke hinder	Schipholtunnel westelijke hoofrijbaan is afgesloten, verkeer via rijksweg 5.		*Omschrijving van de hinder tbv weggebruiker*	

Toelichting:

Het ingevulde aantal gehinderden is puur A4, maar feitelijk worden ook nog alle voertuigen op de A9 gehinderd. De A4 wordt waarschijnlijk al bij Badhoevedorp afgesloten.
Verkeer richting Schiphol komt al in de file voor Badhoevedorp en wordt gehinderd door "sluipverkeer" die de enkele rijstrook gebruiken om door te rijden.
Verkeer via A9-A5 wordt op knp. Badhoevedorp geknepen naar 1 rijstrook.
Als alternatief zal men gaan sluipen via de A9 en de N232.

Ochtendspits:
Ca. 3600 voertuigen/uur om te leiden.
Ca. 1800 voertuigen/uur via West 2.
Ca. 800 voertuigen/uur via A9 A5.
Restant: 1000 voertuigen/uur in de file/sluipen.

Avondspits:
Ca. 5200 voertuigen/uur om te leiden.
Ca. 1800 voertuigen/uur via West 2.
Ca. 0 voertuigen/uur via A9 A5 (boog zit in de avond al vol!).
Restant: 3400 voertuigen/uur in de file/sluipen.

We passen verkeersmanagement, mobiliteitsmaatregelen en publiekscommunicatie toe om het aantal gehinderden te verminderen, conform de Hinderaanpak.

Hinderinformatie

Hinderplanning wegen* (hoofdfasering)				
Korte werkomschrijving	**Schipholtunnel afsluiting oostbuis 2 week 31/32 ivm vervangen van de verlichting**			*Omschrijving werkzaamheden: bv onderhoud/vervanging object of traject*
Locatieaanduiding				
Traject, wegnummer	Wegnummer(s)	A4		
	Wegbeheerder(s)	West Nederland Noord District Zuid		
Traject, hmp	Van hmp/knp.	Km. 8,10 f & d	Tot hmp/knp.	Km. 6,20 f
Rijrichting	HRR/HRL/beide	PRL		
Hinderperiode hoofdfasering	Startdatum: Tijd:	03-08-2027 0:00	Einddatum: Tijd:	09-08-2027 24:00
Dagdeel	*Permanent*		*Weekend/nacht/permanent*	
Verkeersmaatregel	*Afsluiting*		*type CROW-fig of afsluiting*	
Verwachte hinderklasse	*3*		*0,1,2,3,4 (afsluiting is min. hkl. 2)*	
Vertragingstijd	*10-30 minuten*		*Werkvak +evt. file of omrijdtijd*	
Hindercategorie	*A*		*A/B/C/D*	
Aantal gehinderden	*475.000*		*Mvt tijdens periode*	
Max. snelheid werkvak	*70*		*Km/uur*	
Reductie	*100*		*0-100 (100+volledige afsluiting)*	
Omleidingsroutes (indien van toepassing)				
Route 1	Verkeer vanaf Schiphol richting Amsterdam wordt via een doorsteek omgeleid naar de hoofdrijbaan.			Route 1
Route 2				Route 2
OV en hulpdiensten				
Busroute	Omleiding volgen.		Busroute	
Hulpdiensten	Nood/hulpdiensten met prio 1 kunnen op gepaste snelheid door het werkvak.		Hulpdiensten	
Informatie t.b.v. Van A naar Beter				
Wat	Vervangen van de verlichting van de Schipholtunnel.		**Wat**	
Waarom	Groot onderhoud is nodig om de werking te garanderen. Doordat LED wordt aangebracht levert dit een flinke energiebesparing op.		**Waarom**	
Welke hinder	Schipholtunnel oostelijke parallelbuis is afgesloten, verkeer via rijksweg 5.		**Welke hinder**	

Toelichting:

Er wordt op de hoofdrijbaan één rijstrook afgesloten. Hierop kan het verkeer vanaf Schiphol rijden via de doorsteek. Mogelijk is deze enkele rijstrook niet voldoende voor Schiphol, waardoor er een kleine vertraging kan ontstaan op het Schipholterrein. Het alternatief (2 rijstroken doorsteek en 2 rijstroken op de hoofdrijbaan) zorgt voor te veel hinder.

We passen verkeersmanagement, mobiliteitsmaatregelen en publiekscommunicatie toe om het aantal gehinderden te verminderen, conform de Hinderaanpak.

Hinderinformatie

Hinderplanning wegen* (hoofdfasering)				
Korte werkomschrijving	**Schipholtunnel afsluiting oostbuis 1 week 32/33 ivm vervangen van de verlichting**			*Omschrijving werkzaamheden: bv onderhoud/vervanging object of traject*
Locatieaanduiding				
Traject, wegnummer	Wegnummer(s)	A4		
	Wegbeheerder(s)	West Nederland Noord District Zuid		
Traject, hmp	Van hmp/knp.	Km. 9,20	Tot hmp/knp.	Km. 8,14
Rijrichting	HRR/HRL/beide	HRL		
Hinderperiode hoofdfasering	Startdatum: Tijd:	10-08-2027 0:00	Einddatum: Tijd:	17-08-2027 5:00
Dagdeel	*Permanent*		*Weekend/nacht/permanent*	
Verkeersmaatregel	*Afsluiting*		*type CROW-fig of afsluiting*	
Verwachte hinderklasse	*4*		*0,1,2,3,4 (afsluiting is min. hkl. 2)*	
Vertragingstijd	*60+*		*Werkvak +evt. file of omrijdtijd*	
Hindercategorie	*A*		*A/B/C/D*	
Aantal gehinderden	*475.000*		*Mvt tijdens periode*	
Max. snelheid werkvak	*70*		*Km/uur*	
Reductie	*100*		*0-100 (100+volledige afsluiting)*	
Omleidingsroutes (indien van toepassing)				
Route 1	Het verkeer wordt deels omgeleid via rijksweg 5, deels via de doorsteek van de hoofdrijbaan naar de parallelbaan. Verkeer richting Schiphol wordt niet belemmerd.			Route 1
Route 2				
OV en hulpdiensten				
Busroute	Omleiding volgen.			Busroute
Hulpdiensten	Nood/hulpdiensten met prio 1 kunnen op gepaste snelheid door het werkvak.			Hulpdiensten
Informatie t.b.v. Van A naar Beter				
Wat	Vervangen van de verlichting van de Schipholtunnel.			**Wat**
Waarom	Groot onderhoud is nodig om de werking te garanderen. Doordat LED wordt aangebracht levert dit een flinke energiebesparing op.			**Waarom**
Welke hinder	Schipholtunnel oostelijke hoofdrijbaan is afgesloten, verkeer via rijksweg 5.			**Welke hinder**

Toelichting:

Naast het verkeer op de A4 in de Oost 1 wordt ook het verkeer op Oost 2 en op de A5 gehinderd. In de berekening is puur de doorsnede van de A4 meegenomen.
Een deel van het verkeer zal proberen te sluipen via het Schipholterrein, met alle gevolgen van dien.

In de ochtendspits telt het drukste uur 5200 voertuigen per uur.
Over de hoofdrijbaan kunnen nog 1700 voertuigen per uur middels de doorsteek naar de Oost 2. De verbindingsboog van de A4 Links naar de A5 Rechts kan nog ca. 1400 voertuigen verwerken.
Zoals benoemd: De rest van het verkeer (ca. 2100 voertuigen per uur) kan kiezen tussen sluipen over het Schipholterrein, de N201 of in de file staan. Dit zorgt voor een file met een vertraging van ca. een uur.

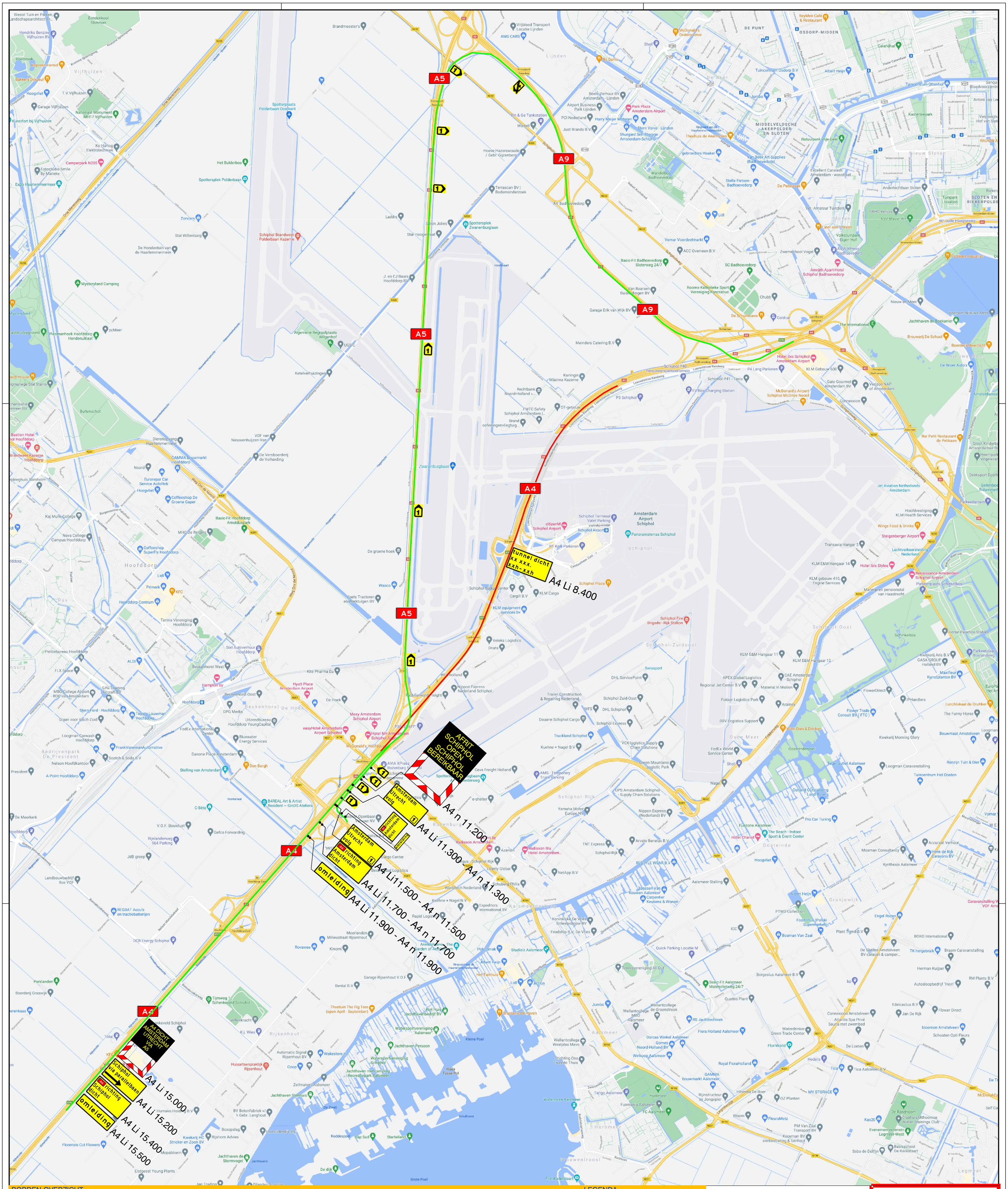
In de avondspits telt het drukste uur 4200 voertuigen per uur.
Over de hoofdrijbaan kunnen nog 1700 voertuigen per uur middels de doorsteek naar Oost 2. De verbindingsboog van de A4 Links naar de A5 Rechts kan nog ca. 600 voertuigen verwerken.
Hierdoor blijven er nog ca. 1900 voertuigen per uur over. Ook hier geldt dat de file een vertraging oplevert van ca. een uur.

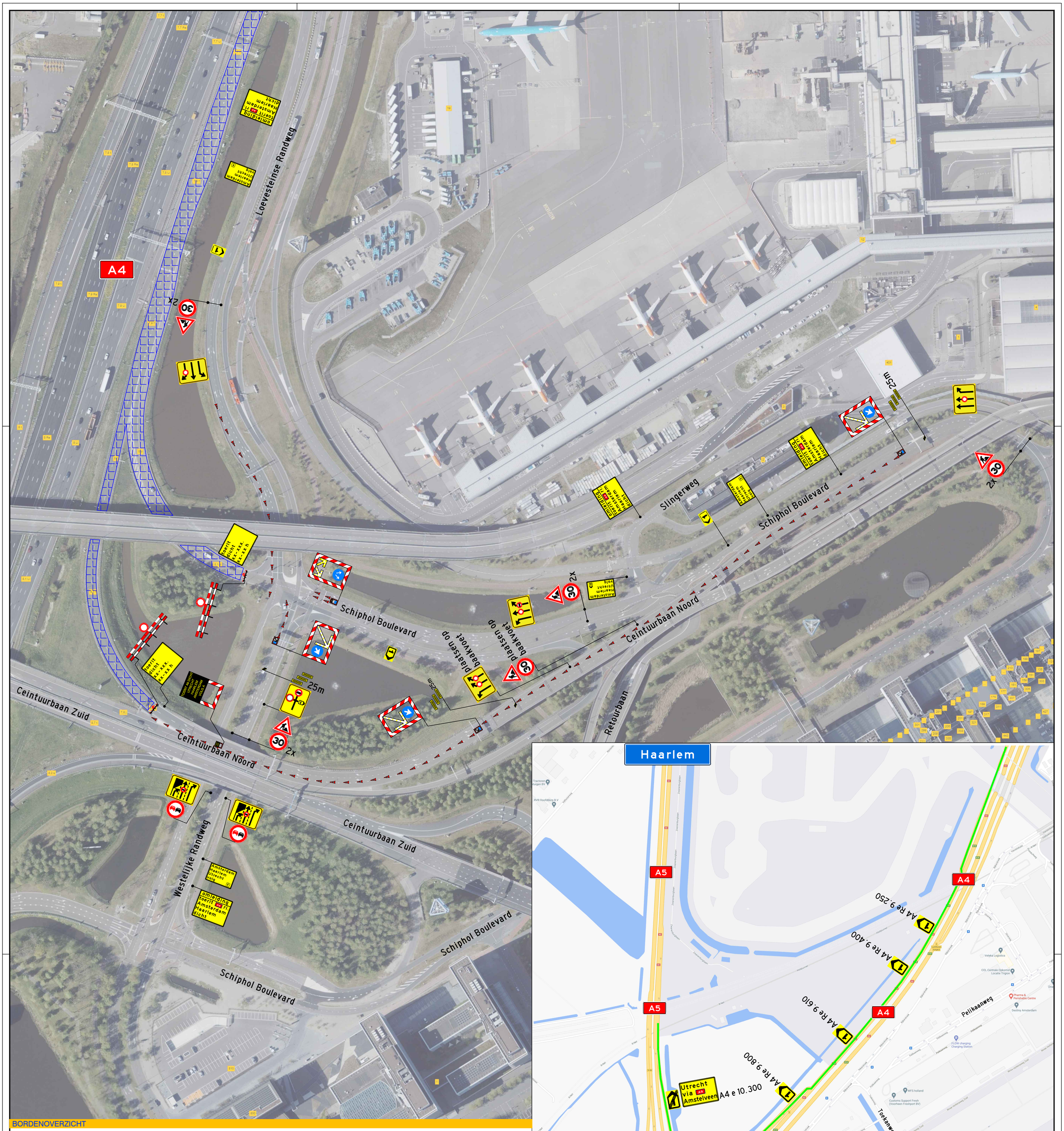
We passen verkeersmanagement, mobiliteitsmaatregelen en publiekscommunicatie toe om het aantal gehinderden te verminderen, conform de Hinderaanpak.

Bijlage G.D Verkeersmaatregelen

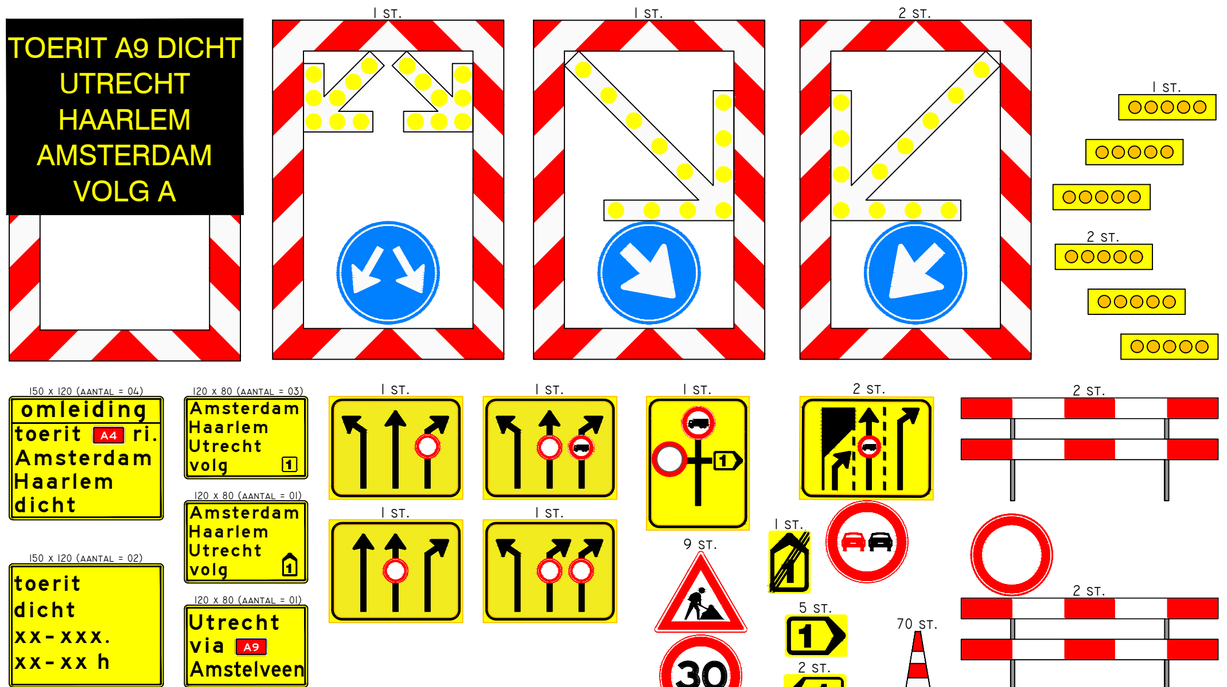
Huidige verkeersmaatregelenplannen (2025):

- Afsluiting Schipholtunnel Oostbuis 1
- Afsluiting Schipholtunnel Oostbuis 2
- Afsluiting Schipholtunnel Westbuis 1 – omleiding A9 A5
- Afsluiting Schipholtunnel Westbuis 2 – afsluiting boog A9 A4
- Afsluiting Schipholtunnel Westbuis 1 en 2


A5
A9
A4
A5
A9
A4
A5
A4
tunnel dicht
xx xxx.
xxh-xxh
A4 Li 8.400
AFRIT SCHIPHOL OPEN SCHIPHOL BEREIKBAAR
A4 n 11.200
Amsterdam Utrecht volg
A4 Li 11.300 - A4 n 11.300
richting Amsterdam dicht
A4 Li 11.500 - A4 n 11.500
omleiding
A4 Li 11.700 - A4 n 11.700
A4 Li 11.900 - A4 n 11.900
A4 DICHT AMSTERDAM UTRECHT VIA A5
Schiphol via parallelbaan
A4 Li 15.000
A4 Li 15.200
A4 Li 15.400
A4 Li 15.500
omleiding
Schiphol Terminal Valet Parking
citizenM Schiphol Airport
Schiphol Airport
P1 Kort Parkeren
Amsterdam Airport Schiphol
Panoramaterras Schiphol
Schiphol Plaza
Schiphol Badge Center
Cargill B.V
KLM Cargo
KLM equipment services bv
Schiphol Fire Brigade - Rijk Station
Schiphol-Oost
Schiphol-Zuidoost
Schiphol-Rijk
Schiphol
Oude Meer
Hornmeer
Rijsenhout
Aalsmeer
Aalsmeerderbrug
Oosteinde
Oranjewijk
Nieuw Sloten
Sloten
Nieuwe Meer
Legmeer
Vrouwentroost
Rozenburg
Hoofddorp
Beukenhorst
De Hoek
Buitenschot
Vijfhuizen
Lijnden
De Akker
DE PUNT
OSDORP-MIDDEN
MIDDELVELDSCHE AKERPOLDER EN SLOTEN
Grote Poel
De dijk
Koddespoel
Cap Sud
Starteiland
Fort Kudelstaart
Schinkelbos
Zwanenburgbaan
Hoofdvaart
Ringvaart van de Haarlemmermeerpolder
Ringvaart van de Haarlemmermeerpolder
Ringvaart van de Haarlemmermeerpolder



BORDENOVERZICHT



LEGENDA

ondergronden omleidingen
bron:
// google maps.nl
// streetsmart.cyclomedia.com

werkvak

Omleiding route 1

Vooraankondiging plaatsen 2 weken voor aanvang werkzaamheden.
De locatie van de borden is een indicatie, exacte locatie wordt in het werk bepaald

Uitvoering:
- xx xxx. xx-xxh

Plaatsen bebording:
- Medio week xx
Verwijderen bebording:
- Medio week xx

ENGIE

Goedgekeurd

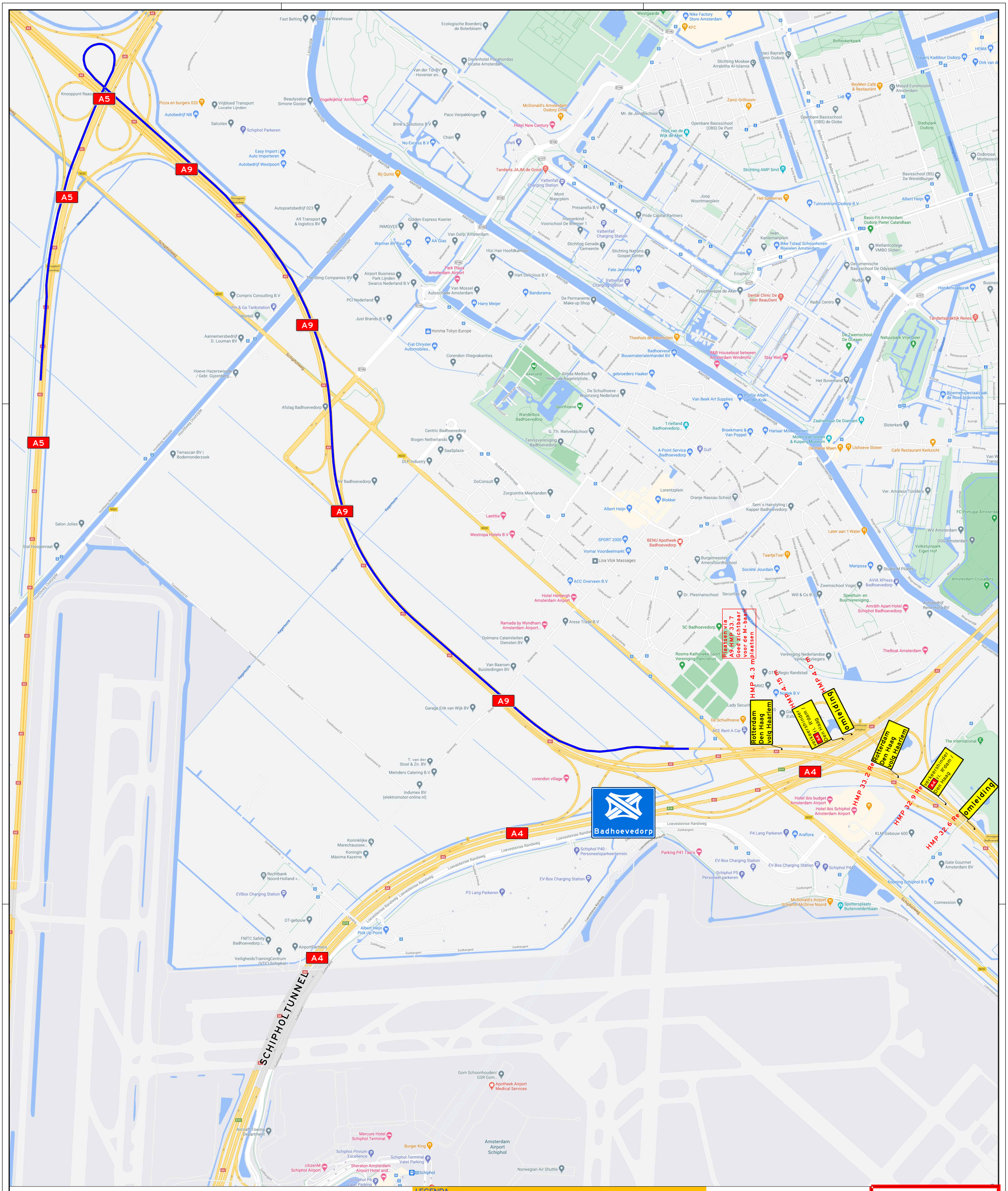
Vermeulen Groep | Wegbeheerder.

5					
4					
3					
2	02-03-2022	OMLEIDING VAN A NAAR I GEWIJZIGD	DBI	WHA	RWS
1	16-07-2021	CONCEPT	WHA	DBI	
STATUS	DATUM	WIJZIGING	GET.	CHCK.	VRIJ.

VERMEULEN GROEP
Hoogeveenseweg 4a
2391 NR
Hazerswoude-Dorp
Tel. : +31(0)79 331 94 54
Fax. : +31(0)79 331 94 76
E-mail : vmr@vermeulengroep.com
Website : www.vermeulengroep.com

Omleiding - Afzetting AFSL Schipholtunnel Oostbuis 2	Opdrachtgever	ENGIE
	Schaal	N.V.T
	Formaat	A1
	Dossiernr.	A0517021
	Tekeningnr.	AFSL Schipholtunnel Oostbuis 2-VKP01

I:\A5 Traffic\Database tekeningen\1. Wegen Rijkswaterstaat\WNN-Z\Schipholtunnel\ACAD\AFSL Schipholtunnel Oostbuis 2v2.dwg 3/2/2022 12:43



LEGENDA

200 x 60 (AANTAL = 02)

omleiding

200 x 100 (AANTAL = 02)

Rotterdam
Den Haag
volg Haarlem

200 x 100 (AANTAL = 02)

verkeershinder
A4 ri. R'dam /
Den Haag

Omleidingsroute

A4 A5 A9 Badhoevedorp

Goedgekeurd

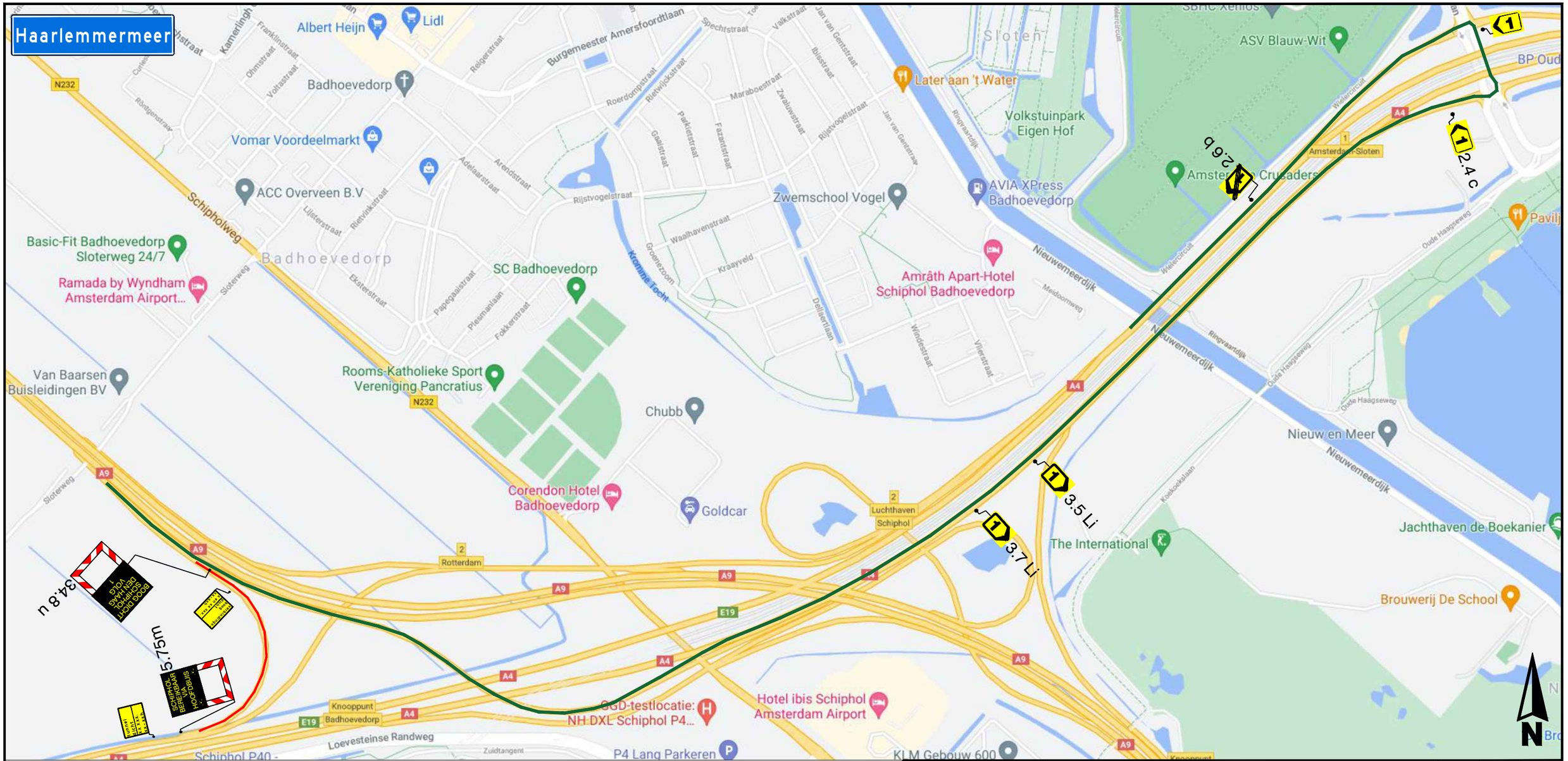
Vermeulen Groep | Wegbeheerder.

5					
4					
3	20-05-21	TEKST BORDEN GEWIJZIGD	DBI	KHE	RWS
2	19-05-21	OML GEWORDEN	DBI	RST	
1	15-10-2020	VERKEERSHINDER A4 ADVIESROUTE A9 / A5	JLU	RST	
STATUS	DATUM	WIJZIGING	GET.	CHCK.	VRIJ.

VERMEULEN GROEP
Hoogeveenseweg 4a
2391 NR
Hazerswoude-Dorp
Tel. : +31(0)79 331 94 54
Fax. : +31(0)79 331 94 76
E-mail : vmr@vermeulengroep.com
Website : www.vermeulengroep.com

Omleiding West 1 dicht verkeer via A9 -A5 Schipholtunnel	Opdrachtgever	00000
	Schaal	N.V.T
	Formaat	A1
	Dossiernr.	A0500000
	Tekeningnr.	A0500000

I:\A5 Traffic\Projecten 2017\A0517 001 - A0517 100\A0517021 Top Tunnels\Top Tunnels 2021\A0517021-SHT21\10. Tekeningen\Tekeningen\Adviesroute Schipholtunnel\ACAD\Verkeershinder A4 adviesroute A9 A5.dwg 5/20/2021 10:23



1 st.



1 st.



1 st.



2 st.



2 st.



1 st.



Omleiding t.b.v. verbindingsboog afsluiting van A9 ri. A4

5					
4					
3	02-03-2022	OMLEIDING GEWIJZIGD VAN A NAAR I	DBI	WHA	RWS
2	12-8-2021	TEKENING UPDATE	AOZ	DBI	DBI
1	03-08-2017	CONCEPT	NLE	MST	RHO
STATUS	DATUM	WIJZIGING	GET.	CHCK.	VRIJ.

VERMEULEN GROEP

Hoogeveenseweg 4a
2391 NR
Hazerswoude-Dorp

Tel. : +31(0)79 331 94 54
Fax. : +31(0)79 331 94 76
E-mail : vmr@vermeulengroep.com
Website : www.vermeulengroep.com

Omleiding West 2 afsluiting	
Opdrachtgever	ENGIE
Schaal	N.V.T
Formaat	A3
Dossiernr.	A0517021-SHT
Tekeningnr.	A0517021-SHT OML. W2

I:\A5 Traffic\Projecten 2017\A0517 001 - A0517 100\A0517021 Top Tunnels\Top Tunnels 2017\A0517021-SHT\10. Tekeningen\Westbuis Schematisch Week 15\A0517021-SHT Westbuisv2.dwg 8/26/2024 8:50

Overzicht borden

200 x 100 (AANTAL = 01)

Rotterdam A4
Den Haag
volg
2

200 x 100 (AANTAL = 03)

A4 dicht
onderhoud
Schipholtunnel

200 x 100 (AANTAL = 03)

Schiphol
volg
1

200 x 100 (AANTAL = 02)

Rotterdam A4
Den Haag
volg
2

200 x 60 (AANTAL = 04)

omleiding

OML KLEIN (AANTAL = 03)

omleiding

11 ST.

1

200 x 100 (AANTAL = 03)

tunnel dicht
xx xxx
xxh-xxh

120 x 80 (AANTAL = 01)

Schiphol
volg
1
Rotterdam A4
volg
2

1 ST.

1

6 ST.

2

120 x 80 (AANTAL = 03)

A4 dicht
onderhoud
Schipholtunnel

3 ST.

1

120 x 80 (AANTAL = 02)

Schiphol
volg
1
Rotterdam A4
volg
2

7 ST.

2

13 ST.

1

1 ST.

1

1 ST.

2

A4 DICHT
SCHIPHOL
VOLG 1
ROTTERDAM
VOLG 2

TUNNEL DICHT
SCHIPHOL
DEN HAAG
VOLG
1

LEGENDA

ondergronden omleidingen
bron:
// google maps.nl
// streetsmart.cyclomedia.com

werkvak

Omleiding route 2 1

Omleiding route 1

Afsluiting

Goedgekeurd

Vermeulen Groep | Wegbeheerder.

5					
4					
3					
2					
1	04-03-2022	CONCEPT		DBI	NVE
STATUS	DATUM	WIJZIGING		GET.	CHCK. VRIJ.

VERMEULEN GROEP
Hoogeveenseweg 4a
2391 NR
Hazerswoude-Dorp
Tel. : +31(0)79 331 94 54
Fax. : +31(0)79 331 94 76
E-mail : vmt@vermeulengroep.com
Website : www.vermeulengroep.com

Omleiding Afsluiting A4 Schipholtunnel Westbuis 1 en 2	Opdrachtgever	00000
	Schaal	N.V.T
	Formaat	A0
	Dossiernr.	A0500000
	Tekeningnr.	AFSL Schipholtunnel-OML-W1-2

© Tekening Uitsluitend voorbereid door Vermeulen Groep voor Contract/Traffic - Afgeleverd - Documenteerbaar Database Intellectuele Eigendom - Wegen Tijdelijke Verkeersmaatregelen (TVM) Schipholtunnel/A4/A9/A5/N232 - Schipholtunnel WEST 1 + 2.dwg

Bijlage H Scheepvaartverkeersmanagement voor rijksvaarwegen

Niet van toepassing.

Bijlage I Rijkswaterstaat Brede Afspraak Archeologie

Niet van toepassing.

Bijlage J Programma van Eisen voor uitvoerend archeologisch onderzoek

Niet van toepassing.

Bijlage K Rijkswaterstaat Brede Afspraak Maatschappelijk Verantwoord Inkopen

Rijkswaterstaat
Ministerie van Infrastructuur en Waterstaat

Bijlage K Rijkswaterstaat Brede Afspraak Maatschappelijk Verantwoord inkopen

Bijlage bij Vraagspecificatie Proces

D&C Vervanging Verlichting Schipholtunnel
Zaaknummer: 31212908

Rijkswaterstaat
Ministerie van Infrastructuur en Waterstaat

Rijkswaterstaat Brede Afspraak Maatschappelijk Verantwoord Inkopen (RBA MVI)

Toepassing van criteria voor Maatschappelijk Verantwoord Inkopen (MVI) binnen het cluster GWW voor Rijkswaterstaat

Datum april 2025
Status Definitief

RWS INFORMATIE

Colofon

Uitgegeven door	Rijkswaterstaat, Grote Projecten en Onderhoud
Informatie	Niek Schoenmaekers
Telefoon	0630703897
E-mail	niek.schoenmaekers.nl
Vastgesteld door	“Programma Duurzaam Aanleg & Onderhoud” en Redactieraad contractenbuffet GPO Inkoopcentrum GWW (ICG)
Datum	November 2024
Status	Definitief
Versienummer	3.0

1 Inhoud

2 Inleiding 6

3 Verplichtingen van de opdrachtnemer 7

4 MVI-eisen GWW 8
4.1 Civiele constructies 9
4.1.1 Duurzaam ontwerp houten constructie 9
4.1.2 Duurzaam ontwerp staalconstructie 9
4.1.3 Duurzaam hout 9
4.1.4 Civiele constructies / Minder milieubelastende smeeroliën, hydraulische vloeistoffen en vetten 10
4.1.5 Duurzaamheidseisen voor betonmortel voor civiele constructies 10
4.1.6 Duurzaamheidseis voor nieuw te leveren keerwanden 11
4.1.7 Duurzaamheidseisen voor nieuw te leveren stelbeton 11
4.1.8 Duurzaamheidseisen voor nieuw te leveren betonnen stapelblokken 11
4.1.9 Civiele constructies / Duurzaamheidseisen voor kanaalplaatvloeren 11
4.1.10 Duurzaamheidseisen voor betonmortel toegepast als verhardingslaag van een infrastructureel project 11
4.1.11 Duurzaamheidseisen voor betonnen breedplaatvloeren 12
4.1.12 Maximale milieukosten waterbouw asfalt 12
4.2 Conserveringswerken 13
4.2.1 Toepassen oplosmiddelarme conserveringssystemen 13
4.2.2 Producten met lood- of chromaathoudende pigmenten 14
4.2.3 Leveren beheer- en onderhoudsplan 14
4.2.4 Milieumanagementsysteem 15
4.3 Openbare verlichting (OVL) 15
4.3.1 Ledverlichting 15
4.3.2 Levensduur ledsysteem 15
4.3.3 Dimbare OVL-installatie 16
4.3.4 Lichthinder wordt beperkt 16
4.4 Riolering 16
4.4.1 Duurzaamheidseis voor nieuw te leveren betonnen rioleringsbuizen tot 1.000 mm 16
4.4.2 Duurzaamheidseis voor nieuw te leveren betonnen inspectieputten 16
4.4.3 Duurzaamheidseis voor betonnen kolken 17
4.5 Straatmeubilair 17
4.5.1 Straatmeubilair (m.u.v. Speeltoestellen): meer dan 5% kunststof 17
4.5.2 Straatmeubilair (incl. Speeltoestellen): verven 18
4.5.3 Duurzaam hout 18
4.5.4 Recycling kunststoffen 19

4.5.5 Circulaire materialen voor verkeersborden en bewegwijzeringsborden 19
4.6 Wegen 21
4.6.1 Duurzaamheidseis voor een fietspad van gestort beton 21
4.6.2 Duurzaamheidseis voor nieuw te leveren stelbeton 21
4.6.3 Duurzaamheidseis voor nieuw te leveren betonstraatstenen 21
4.6.4 Duurzaamheidseis voor betontegels 22
4.6.5 Duurzaamheidseis voor nieuw te leveren grasbetontegels 22
4.6.6 Duurzaamheidseis voor nieuw te leveren industrieplaten 22
4.6.7 Duurzaamheidseis voor nieuw te leveren betonbanden 22
4.6.8 Maximale milieukosten asfaltdeklagen 22
4.6.9 Maximale milieukosten asfalt tussen- en onderlaag 23
4.6.10 Duurzaamheidseisen voor nieuw te leveren straatbakstenen 23
4.7 Gemalen 23
4.7.1 Energierendement van systeem 23
4.7.2 Energierendement van systeemdelen 24
4.7.3 Gemalen / Minder milieubelastende smeeroliën, hydraulische vloeistoffen en vetten 25
4.8 Waterzuiveringsinstallaties en slibbehandeling 25
4.8.1 Ecotoxiciteit chemicaliën 25
4.9 Dooimiddelen 25
4.9.1 Inkoop uitvoering gladheidbestrijding op basis van CROW 353 26
4.10 Mobiele werktuigen uitbesteding 26
4.10.1 Emissie-eisen mobiele dieselwerktuigen met variabel toerental 26
4.10.2 Het nieuwe draaien 26
4.10.3 Onderhoud gebruikte mobiele werktuigen 27
4.10.4 Minder milieubelastende smeeroliën, hydraulische vloeistoffen en vetten 27
4.10.5 Mobiele werktuigen en Bouwlogistiek - Uitbesteding / Voertuigen voldoen tenminste aan basiseisen voor emissies 28
4.10.6 Verplichte training 'Het Nieuwe Rijden' voor chauffeurs met B-rijbewijs 28
4.11 Verkeersregelinstallaties 29
4.11.1 Diminrichting in regeltoestel 29
4.11.2 Energiezuinige lichtbronnen 29
4.11.3 Energiezuinige lampen voor scheepvaartseinen 29
4.11.4 Levenscycluskosten 30
4.11.5 Minimale levensduur en garantie 30
4.12 Groenvoorzieningen 30
4.12.1 Verwerven van bloembollen 30
4.12.2 Boomkwekerijproducten van een genetische kwaliteit (buitenstedelijk) 32
4.12.3 Meststoffen en bodemverbeteraars bij aanleg en onderhoud van openbaar groen (incl. sport- en speelvelden) 32
4.12.4 Ongewenste kruiden, ziekten en plagen (excl. sport- en speelvelden) 32

4.12.5 Duurzaam ontwerp groenvoorziening 33
4.12.6 Eisen aan compost 33
4.12.7 Geen invasieve exoten 34
4.13 Reiniging openbare ruimte 34
4.13.1 Verwijderen van graffiti met hogedrukwaterreiniger 34
4.13.2 Milieu-impact onkruidbestrijding op verhardingen 34
4.13.3 Vermindering van PM10 straatstof 35
4.13.4 Milieukeur voor buitenschoonmaakmiddelen 35
4.14 Vaartuigen 36
4.14.1 Voorzieningen voor afvalwater 36
4.14.2 Minder milieubelastende smeeroliën, hydraulische vloeistoffen en vetten 36
4.14.3 Vaartuigen / Varend materieel voldoet aan basiseisen voor emissies 37
4.14.4 Maximaal energieverbruik vaartuig 37
4.14.5 Varend materieel gebruikt tenminste een basis aandeel duurzame energiedragers 37

2 Inleiding

Rijkswaterstaat heeft zich gecommitteerd, in overeenstemming met het Rijksbeleid, om 100% maatschappelijk verantwoord in te kopen (voorheen ‘duurzaam in te kopen’). Dit houdt in dat bij alle aanbestedingen / inkopen de minimumeisen van het betreffende cluster van de MVI-criteriatool van toepassing zijn. Eén van deze clusters is bijvoorbeeld het cluster ‘Grond-, weg- en waterbouw’. [1]

De eisen zijn vastgelegd in de MVI-criteriatool[2] op ambitieniveau 1 (voorheen de ‘Criteriadocumenten Maatschappelijk Verantwoord Inkopen’, en daarvoor de ‘Criteriadocumenten Duurzaam Inkopen’). De eisen worden periodiek geactualiseerd onder de verantwoordelijkheid van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties en het Ministerie van Infrastructuur en Waterstaat.
De voor het werk[3] vigerende eisen zijn de eisen zoals opgenomen in hoofdstuk 3 van deze versie van de RBA MVI. In het contract van waaruit naar deze RBA MVI verwezen wordt, staat aangegeven welke versie van deze RBA MVI van toepassing is.
In deze RBA MVI kunnen eisen opgenomen zijn in aanvulling op de eisen uit de MVI-criteriatool.
De in de MVI-criteriatool opgenomen eisen ten aanzien van social return zijn niet overgenomen in de RBA MVI. Rijkswaterstaat geeft hier op een andere wijze met behulp van de Groeituin Social Return[4] invulling aan.
De in de MVI-criteriatool opgenomen eisen ten aanzien van Gladheidbestrijding zijn niet overgenomen in de RBA MVI. Deze maken al deel uit van de “Eisen wegenzout Rijkswaterstaat”.

[1] Rijkswaterstaat heeft een verdergaande ambitie dan het opnemen van de minimumeisen voor maatschappelijk verantwoord inkopen. Voor meer informatie over hoe Rijkswaterstaat invulling geeft aan maatschappelijk verantwoord inkopen bij de aanbesteding en realisatie van werken, zie www.rijkswaterstaat.nl/duurzaaminkopen.
[2] Zie https://www.mvicriteria.nl/nl
[3] Daar waar in deze RBA de term ‘werk’ staat, wordt tevens Meerjarig Onderhoud bedoeld.
[4] Rijkswaterstaat heeft een set contractbepalingen in de GWW-contractmodellen opgenomen, waarmee social return met behulp van de Groeituin uniform wordt uitgevraagd. Deze contractbepalingen zijn door ICG gepubliceerd op het Contractenbuffet: Design en Construct (rws.nl), Algemeen (rws.nl), Wegen (rws.nl), Droog (rws.nl), Rivieren en Kanalen (rws.nl). Meer informatie tref je aan op onze intranetpagina: Social return in GWW-opdrachten van Rijkswaterstaat (rws.nl).

3 Verplichtingen van de opdrachtnemer

Van toepassing zijnde criteria

1. De opdrachtnemer dient voor alle door hem uit te voeren werkzaamheden te bepalen welke productgroepen met MVI-criteria zoals vastgelegd in hoofdstuk 3 van dit document van toepassing zijn op het onderhavige werk.
2. Wanneer het werk onderdeel is van het cluster ‘Grond-, weg- en waterbouw’, dan zijn de van toepassing zijnde eisen opgenomen in hoofdstuk 3 van dit document.
3. De opdrachtnemer dient invulling te geven aan de van toepassing zijnde eisen opgenomen in hoofdstuk 3 van dit document en aan de expliciete en impliciete doelstellingen die daarbij in de toelichting zijn verwoord.
4. De opdrachtnemer dient aan te tonen dat voldaan wordt aan de van toepassing zijnde eisen opgenomen in hoofdstuk 3 van dit document en aan de expliciete en impliciete doelstellingen die daarbij in de toelichting zijn verwoord.

Bewijsmiddelen

5. De opdrachtnemer dient aan te tonen dat aan de eisen voldaan is overeenkomstig de vereisten aan zijn kwaliteitsmanagementsysteem zoals gesteld in het contract.

4 MVI-eisen GWW

Voor de GWW-werken van Rijkswaterstaat zijn de eisen op Ambitieniveau 1 uit de MVI-criteriatool (www.mvicriteria.nl) onder het cluster ‘Grond-, Weg- en Waterbouw’ van toepassing. Het betreft de productgroepen:

1. Civiele constructies
2. Conserveringswerken
3. Openbare verlichting
4. Riolering
5. Straatmeubilair
6. Wegen
7. Gemalen
8. Waterzuiveringsinstallaties en slibbehandeling
9. Dooimiddelen
10. Mobiele werktuigen uitbesteding
11. Verkeersregelinstallaties
12. Groenvoorzieningen
13. Reiniging openbare ruimte
14. Vaartuigen

Voor de GWW-werken van Rijkswaterstaat zijn de eisen op Ambitieniveau 1 uit de MVI-criteriatool (www.mvicriteria.nl) onder het cluster “Grond-, Weg- en Waterbouw” geselecteerd en op de volgende pagina’s opgenomen. De eisen zijn van toepassing op alle GWW-werken van Rijkswaterstaat.

Indien een van toepassing zijnde eis uit de MVI-tool is opgenomen in de Vraagspecificatie en de inhoud hiervan gelijk is aan de eis uit de MVI-tool, dan wordt bij de desbetreffende eis de volgende tekst opgenomen: Deze eis uit de RBA is opgenomen in de Vraagspecificatie.

4.1 Civiele constructies

4.1.1 Duurzaam ontwerp houten constructie

- Ambitieniveau: 1
- Criteriumtype: EIS;
- Criteriumcode: 029.001

Eis
Constructies met hout die worden blootgesteld aan weer en wind) zijn zo ontworpen dat geen (hemel)water kan blijven staan en/of geen capillair vocht in kan trekken.

Bovenbeschreven beginsel staat o.a. weergegeven in het CUR-rapport 213 'Hout in de GWW-sector duurzaam detailleren'.

Door goed te detailleren en gebruik te maken van de geschikte houtsoorten, kunnen constructies gemaakt worden met een hoge levensduur. In het rapport worden algemene regels gegeven voor het goed detailleren.

Een nadere bepaling van het beginsel kan zijn:
- Kopse vlakken van hout zijn afgeschermd van vocht;
- Bij de toepassing van een houten vlak tegen een ander vlak wordt een afstand tussen deze vlakken aangehouden van minimaal 8 mm (met uitzondering van gevingerlast hout).

Meer informatie over toe te passen houtsoorten en detaillering van houten constructies is te vinden op de website van Houtdatabase.

4.1.2 Duurzaam ontwerp staalconstructie

- Ambitieniveau: 1
- Criteriumtype: EIS
- Criteriumcode: 029.002

Deze eis uit de RBA is opgenomen in de Vraagspecificatie.

4.1.3 Duurzaam hout

- Ambitieniveau: 1
- Criteriumtype: EIS
- Criteriumcode: 029.007

Eis
Te leveren hout of hout verwerkt in te leveren (hout)producten dient te voldoen aan de "Dutch Procurement Criteria for Timber" ten aanzien van duurzaam bosbeheer en de handelsketen, inclusief de bijbehorende beoordelingsmethode.

Hout dat onder een certificeringsysteem wordt geleverd, dient vergezeld te gaan van de op de levering betrekking hebbende factuur en/of pakbon van de opdrachtnemer. Facturen dienen te zijn voorzien van:
- naam en adresgegevens van de opdrachtgever en de opdrachtnemer;

- datum uitgifte;
- houtsoort en/of productbeschrijving;
- volume of aantal van het geleverd product;
- de naam van het certificeringssysteem, de claim (bijv. FSC 100% of PEFC gecertificeerd);
- Chain-of-Custody certificaatnummer van de leverancier.

Verificatie
- Certificaat van de voor dit dossier verantwoordelijke staatssecretaris toegelaten certificeringssystemen, geldend op datum van aankondiging. Voor alle goedgekeurde certificeringssystemen, zie de rechterkolom van de tabel judgements;
- Alternatief en verifieerbaar bewijs waaruit blijkt dat aan de gestelde eis wordt voldaan. Als hulpmiddel bij het leveren van alternatief bewijs kan de opdrachtnemer gebruik maken van Documents for Category B evidence.

4.1.4 Civiele constructies / Minder milieubelastende smeeroliën, hydraulische vloeistoffen en vetten

- Ambitieniveau: 1
- Criterium type: EIS
- Criterium code: 029.012

Eis:
Smeerolie, hydraulische vloeistoffen en vetten dienen te voldoen aan de criteria 1 t/m 4 voor de toekenning van de EU-milieukeur voor smeermiddelen Besluit (EU) 2018/1702.
Als bij gebruik van smeermiddelen met accidenteel verlies het vereiste smeermiddel afwijkt van de voorgeschreven specificaties van de leverancier (van de voer- en/of werktuigen) dan dient de opdrachtnemer in overleg met de leverancier het toe te passen smeermiddel bepalen.
Besluit (EU) 2018/1702 maakt onderscheid in:
- smeermiddel met volledig verlies: een smeermiddel dat tijdens het gebruik volledig in het milieu vrijkomt;
- smeermiddel met gedeeltelijk verlies: een smeermiddel dat tijdens het gebruik gedeeltelijk in het milieu vrijkomt en waarvan het niet-vrijgekomen gedeelte voor herverwerking, recyclage of verwijdering kan worden teruggewonnen;
- smeermiddel met accidenteel verlies: een smeermiddel dat in een gesloten systeem wordt gebruikt, enkel accidenteel in het milieu kan vrijkomen en na gebruik voor herverwerking, recyclage of verwijdering kan worden teruggewonnen.

Verificatie
- Technische productspecificaties of andere documentatie waaruit blijkt dat aan dit criterium is voldaan.
- (Geldig) certificaat van een ISO type I milieukeurmerk, waarvan de eisen overeenkomen met de in dit criterium gestelde eisen, of een gelijkwaardig certificaat. Meer informatie over ISO type I milieukeurmerk is te vinden op de website van PIANOo. Producten met het Europese Ecolabel voldoen aan de gestelde eisen 1 t/m 4. Op de website van de Europese Commissie is een lijst beschikbaar van oliën en vetten die voldoen aan de eisen van het Europese Ecolabel.

4.1.5 Duurzaamheidseisen voor betonmortel voor civiele constructies

- Ambitieniveau: 1

- Criterium type: Eis
- Criterium code: 029.018

Deze eis uit de RBA is opgenomen in de Vraagspecificatie.

4.1.6 Duurzaamheidseis voor nieuw te leveren keerwanden

- Ambitieniveau: 1
- Criterium type: Eis
- Criterium code: 029.019

Deze eis uit de RBA is opgenomen in de Vraagspecificatie.

4.1.7 Duurzaamheidseisen voor nieuw te leveren stelbeton

- Ambitieniveau: 1
- Criterium type: Eis
- Criterium code: 029.020

Deze eis uit de RBA is opgenomen in de Vraagspecificatie.

4.1.8 Duurzaamheidseisen voor nieuw te leveren betonnen stapelblokken

- Ambitieniveau: 1
- Criterium type: Eis
- Criterium code: 029.021

Deze eis uit de RBA is opgenomen in de Vraagspecificatie.

4.1.9 Civiele constructies / Duurzaamheidseisen voor kanaalplaatvloeren

- Ambitieniveau: 1
- Criterium type: Minimumeis
- Criterium code: 029.022

Deze eis uit de RBA is opgenomen in de Vraagspecificatie.

4.1.10 Duurzaamheidseisen voor betonmortel toegepast als verhardingslaag van een infrastructureel project

- Ambitieniveau: 1
- Criterium type: Eoostis
- Criterium code: 029.023
- Onderwerp: Verhardingslaag - gestort

Deze eis uit de RBA is opgenomen in de Vraagspecificatie.

4.1.11 Duurzaamheidseisen voor betonnen breedplaatvloeren

- Ambitieniveau: 1
- Criterium type: Eis
- Criterium code: 029.025

Deze eis uit de RBA is opgenomen in de Vraagspecificatie.

4.1.12 Maximale milieukosten waterbouw asfalt

- Ambitieniveau: 1
- Criterium type: Eis
- Criterium code: 029.024
- Onderwerp: Waterbouw asfalt

De MKI-waarde van het waterbouw asfalt van mengseltype [X] mag niet hoger zijn dan [Y], uitgedrukt in euro's per ton asfalt.
Toelichting voor de inkopende organisatie
Toelichting eis:

- De inkopende organisatie dient X (mengseltype) en Y (MKI-waarde) nader te specificeren door de naam van het mengsel en de MKI-waarde in te vullen. Zoek daartoe het betreffende asfaltmengsel in onderstaande tabel, en neem die waarde [Y] en de naam van het mengsel [X] over in de eis-tekst.
- Deze eis voorziet in een maximale MKI-waarde voor de productiefase van asfalt (fase A1 t/m A3).
- Gebruik deze eis als u het toe te passen asfaltmengsel voorschrijft. Indien u de keuze voor het mengsel vrijlaat aan de aannemer, gebruik dan het gunningscriterium milieuprestatie GWW werken.
- De waarden in onderstaande tabel zijn 10% lager dan de branchemiddelde waarde zoals geregistreerd in het LCA-achtergrondrapport voor Branche representatieve Nederlandse Asfaltmengsels door TNO, versie 22-09-2020. De MKI-waarde moet zijn berekend volgens de PCR Asfalt, versie 1.0, over de levensfases A1 t/m A3.
- Als het door de inkopende organisatie voorgeschreven mengsel niet in onderstaande tabel staat, kies dan indien mogelijk het meest overeenkomende mengsel. Als dit niet mogelijk is, kan deze eis beter niet toegepast worden.

mengsel	maximaal toegestaan MKI per ton asfalt A1-A3 (10% onder branchegemiddelde)
WB asfaltbeton	10,47
Open steenasfalt	8,06
WB gietasfalt	14,01
WB asfaltmastiek	18,63

Toelichting Levenscyclusanalyse (LCA) en Milieukostenindicator (MKI):

- Een levenscyclusanalyse (LCA) berekent de milieueffecten van een product gedurende een gehele of gedeeltelijke levenscyclus. De uitkomsten hiervan kunnen worden omgerekend tot één score, de Milieukostenindicator (MKI). Deze MKI-waarde is bruikbaar bij aanbestedingen. Voor meer informatie zie de handreiking Inkopen met de Milieukostenindicator van PIANOo.
- Indien u wilt gunnen op zo laag mogelijke milieukosten (MKI-waarde) voor het hele project, gebruik dan het gunningscriterium Milieuprestatie GWW werken uit de MVI Criteria Tool, onderdeel Wegen.

Verificatie

- Een geverifieerde Environmental Product Declaration (EPD), op basis van de vigerende PCR, met volledige mengselsamenstelling.
- Een geverifieerd categorie 1 LCA rapport op basis van de vigerende PCR.
    - NB: Beide voorafgaande mogelijke bewijsmiddelen dienen getoetst en akkoord bevonden te zijn door een Erkende LCA- deskundige die op het moment van toetsen voorkomt op de 'Lijst van LCA- deskundigen die door de Stichting NMD als toetser erkend zijn voor het toetsen van categorie 1 en 2 data ten behoeve van opname in de Nationale Milieudatabase' zoals vastgesteld door Stichting NMD.
- Of gelijkwaardig

4.2 Conserveringswerken

4.2.1 Toepassen oplosmiddelarme conserveringssystemen

- Ambitieniveau: 1
- Criteriumtype: EIS
- Criteriumcode: 030.001

Eis

Het samengestelde conserveringssysteem moet worden opgebouwd met conserveringsproducten waarvan het aandeel vluchtige organische stoffen (VOS) onderstaande grenswaarden per liter conserveringsproduct niet overschrijdt.

Onder conserveringssysteem wordt verstaan: het samenstel van bij de conserveringsopdracht te gebruiken conserveringsproducten en de toepassing daarvan bij de conserveringswerkzaamheden.
Maximale grenswaarden voor het VOS gehalte van verven en vernissen:

*Productsubcategorie-	*Type-	*g/l (*)
*a- Matte coatings voor wanden en plafonds (glans ≤ 25°-60°)	WG	30
	SG	30
*b- Glanzende coatings voor wanden en plafonds (glans > 25°-60°)	WG	100
	SG	100

*Productsubcategorie-	*Type-	*g/l (*)
*c- Buitenmuren minerale ondergrond	WG	40
	SG	430
*d- Hout- en metaalverven voor binnen- en buitendecoratie en voor interieur- en gevelbekleding	WG	130
	SG	300
*e- Vernissen en houtbeitsen voor houtwerk binnen en buiten, inclusief dekkende houtbeitsen	WG	130
	SG	400
*f- Houtbeitsen met minimale laagdikte voor binnen en buiten	WG	130
	SG	700
*g- Primers	WG	30
	SG	350
*h- Hechtprimers	WG	30
	SG	750
*i- Performante eencomponentcoatings	WG	140
	SG	500
*j- Performante tweecomponentcoatings voor specifiek eindgebruik zoals vloeren	WG	140
	SG	500
*k- Meerkleurige coatings	WG	100
	SG	100
*l- Coatings met decoratieve effecten	WG	200
	SG	200

(*) g/l = gebruiksklaar product
(**) WG: Watergedragen, SG: Solvent gedragen

Verificatie
- productdata en -bladen waaruit blijkt dat aan bovenstaande eisen wordt voldaan;
- of gelijkwaardig.

4.2.2 Producten met lood- of chromaathoudende pigmenten

- Ambitieniveau: 1
- Criteriumtype: EIS
- Criteriumcode: 030.002

Eis
In toe te passen conserveringsproducten mag geen pigment met lood of chroom-6 zijn verwerkt.

Verificatie
- analyse en/of productdata en -bladen waaruit blijkt dat aan bovenstaande eis wordt voldaan;
- of gelijkwaardig.

4.2.3 Leveren beheer- en onderhoudsplan

- Ambitieniveau: 1
- Criteriumtype: Eis
- Criteriumcode: 030.004

De eis uit de RBA is opgenomen in de Vraagspecificatie.

4.2.4 Milieumanagementsysteem

- Ambitieniveau: 1
- Criteriumtype: GE
- Criteriumcode: 030.007

Eis
De opdrachtnemer beschikt voor dat deel/die delen van de organisatie dat/die betrokken is/zijn bij de uitvoering van de opdracht over een managementsysteem waarin ten minste de volgende onderwerpen zijn geregeld:

- milieubeleidsuitgangspunten van de organisatie;
- concrete maatregelen die de opdrachtnemer heeft getroffen of gaat treffen om de milieubelasting van de bedrijfsprocessen die verband houden met de uitvoering van de opdracht te verminderen of te voorkomen, in elk geval ten aanzien van [x];
- hoe bovenstaande milieuaspecten van de organisatie worden gemonitord en geherwaardeerd als basis voor continue verbetering met specifieke aandacht voor de in deze criteria opgenomen milieuaspecten;
- hoe aandacht wordt besteed aan de bewustwording en de competentie van medewerker(s) en toeleverancier(s) ten aanzien van het omgaan met de voor deze opdracht relevante milieuaspecten; dat naleving van de op de verlangde prestatie(s) geldende milieuwetgeving is geborgd.

Verificatie

- ISO 14001-certificaat, EMAS-certificaat, of een gelijkwaardig certificaat;
- verklaring dat de milieuzorg een structureel onderdeel uitmaakt van de dagelijkse bedrijfsvoering, van een onafhankelijke auditor, accountant of (geaccrediteerde) certificatie-instelling met aantoonbare kennis van zaken;
- of gelijkwaardig.

4.3 Openbare verlichting (OVL)

4.3.1 Ledverlichting

- Ambitieniveau: 1
- Criteriumtype: EIS
- Criteriumcode: 033.001

Deze eis uit de RBA is opgenomen in de Vraagspecificatie.

4.3.2 Levensduur ledsysteem

- Ambitieniveau: 1
- Criteriumtype: EIS
- Criteriumcode: 033.002

Deze eis uit de RBA is opgenomen in de Vraagspecificatie.

4.3.3 Dimbare OVL-installatie

- Ambitieniveau: 1
- Criteriumtype: EIS
- Criteriumcode: 033.003

Deze eis uit de RBA is opgenomen in de Vraagspecificatie.

4.3.4 Lichthinder wordt beperkt

- Ambitieniveau: 1
- Criteriumtype: EIS
- Criteriumcode: 033.004

Eis
De lichtuitstraling van de OVL-installatie moet vallen binnen de grenswaarden als gesteld in de Richtlijn Lichthinder 2020 van de Nederlandse Stichting voor Verlichtingskunde (NSVV).
Aan de Richtlijn Lichthinder dient te worden voldaan voor zover deze van toepassing is verklaard in de Vraagspecificatie.

Toelichting
De richtlijn lichthinder geeft grenswaarden voor lichtuitstraling. Als lichthinder wordt bedoeld het ten gevolge van lichtuitstraling van de OVL-installatie optreden van overlast bij mens, plant of dier. De Richtlijn Lichthinder 2020 kan gevonden worden op de. website van de NSVV.

Verificatie
De opdrachtnemer kan worden gevraagd om documenten te overleggen waaruit blijkt dat aan deze eis is voldaan en dat dit op een valide wijze is bepaald.

4.4 Riolering

4.4.1 Duurzaamheidseis voor nieuw te leveren betonnen rioleringsbuizen tot 1.000 mm

- Ambitieniveau: 1
- Criteriumtype: EIS
- Criteriumcode: 034.012

Deze eis uit de RBA is opgenomen in de Vraagspecificatie.

4.4.2 Duurzaamheidseis voor nieuw te leveren betonnen inspectieputten

- Ambitieniveau: 1
- Criteriumtype: EIS
- Criteriumcode: 034.013

Deze eis uit de RBA is opgenomen in de Vraagspecificatie.

4.4.3 Duurzaamheidseis voor betonnen kolken

- Ambitieniveau: 1
- Criteriumtype: EIS
- Criteriumcode: 034.014

Deze eis uit de RBA is opgenomen in de Vraagspecificatie.

4.5 Straatmeubilair

4.5.1 Straatmeubilair (m.u.v. Speeltoestellen): meer dan 5% kunststof

- Ambitieniveau: 1
- Criteriumtype: EIS
- Criteriumcode: 035.001

Eis
Voor straatmeubilair waarvan meer dan 5% van de massa van het eindproduct uit kunststoffen bestaat, dient van de totale hoeveelheid kunststoffen ten minste 90% (gewichtsprocenten binnen een product) gerecycled materiaal te zijn. Voor straatmeubilair is dit post-consumer materiaal, bij speeltoestellen mag ook pre-consumer materiaal gebruikt worden.

Definitie gerecycled of secundair materiaal :

Materiaal dat verkregen is via opwerking van afvalmateriaal. Dit kan een afvalstroom in een productieproces zijn (pre-consumer fase) of afkomstig van producten die al een eerdere gebruiksfunctie hebben vervuld, zoals consumentenafval (post-consumer fase).

- Pre-consumer materiaal (of: postindustrieel restmateriaal) is restmateriaal dat geen afval wordt in een productieproces. Uitgesloten is hergebruik zoals nabewerking en schroot, dat gegenereerd wordt in een proces en kan worden teruggewonnen binnen hetzelfde proces. Het gaat om materiaal gegenereerd door de industrie en niet is gebruikt door de consument;

- Post-consumer materiaal is restmateriaal dat door eindgebruikers van producten wordt geproduceerd bij afdanking van deze producten, als de eindgebruiker het product niet langer voor het beoogde doel kan gebruiken. Eindgebruikers zijn onder andere huishoudens, commerciële partijen en industriële partijen. Afdanking omvat het retouren van materiaal uit de distributieketen.
  Het gaat om materiaal afkomstig uit eerder gebruik of uit reststromen en dat primaire materialen vervangt. Het materiaal kan afkomstig zijn van zowel soortgelijke als andersoortige producten dan het doelproduct. Kenmerkend voor recycling is dat het materiaal gescheiden wordt tot een zo zuiver mogelijke grondstof en aan het begin van een productieproces wordt heringevoerd. Op voorhand van het recyclingproces is doorgaans niet bekend in welk eindproduct het materiaal terecht komt. Er is een bewerking nodig om de materialen opnieuw in te kunnen zetten in de oorspronkelijke of andere toepassing.

Deze eis geldt niet:
- Indien de opdrachtnemer hergebruikte of refurbished producten levert.

Definitie hergebruikte (of refurbished) producten of onderdelen:
Producten of onderdelen die al in gebruik zijn geweest, toegepast in eenzelfde nieuw of ander product. Ook het reviseren (refurbishen), oftewel het herstellen en aanpassen van een bestaand product, met behoud of verbetering van de functionaliteit en het herfabriceren (opknappen, herbestemmen) waarbij een nieuw

product wordt gemaakt uit onderdelen, componenten en of materialen van afgedankte producten, wordt gezien als 'hergebruik'. Gerecyclede grondstoffen vallen niet onder deze definitie, aangezien deze via een omvormproces zijn verkregen; bij recycling wordt de oorspronkelijke vorm van het product niet behouden.

- Voor de toepassing van:
    - kunststoffen in touw en vezel versterkte kunststoffen;
    - transparante of gekleurde overkappingen (vanwege vertroebeling).

Verificatie

- Certificaat waaruit blijkt dat aan het vereiste aandeel gerecycled kunststof wordt voldaan, zoals: QA-CER-certificaat, Plastica Seconda Vita
- Documentatie over de samenstelling en gebruikte grondstoffen/materialen voor (de onderdelen van) de geleverde producten.
- Of gelijkwaardig.

4.5.2 Straatmeubilair (incl. Speeltoestellen): verven

- Ambitieniveau: 1
- Criteriumtype: EIS
- Criteriumcode: 035.003

Eis

Het vluchtige organische verbinding (VOS) gehalte (excl. water) voor verven met een spreidend vermogen van ten minste 15 m^2/l en voor vernissen die worden toegepast op hout, dient maximaal 250 g/l (met een dekkracht van 98%) te bedragen. Voor de overige verfproducten (vernissen, houtbeitsen, vloercoatings, vloerverven en verwante producten) is dat maximaal 180 g/l.

Een VOS is een organische verbinding die, onder normale druk, een kookpunt (of beginkookpunt) heeft dat lager is dan of gelijk aan 250°C.

Verificatie

- Europees Ecolabel voor verven en vernissen, of een gelijkwaardig keurmerk;
- Of gelijkwaardig.

4.5.3 Duurzaam hout

- Ambitieniveau: 1
- Criteriumtype: EIS
- Criteriumcode: 035.005

Eis

Te leveren hout of hout verwerkt in te leveren (hout)producten dient te voldoen aan de ‘Dutch Procurement Criteria for Timber’ ten aanzien van duurzaam bosbeheer en de handelsketen, inclusief de bijbehorende beoordelingsmethode.

Hout dat onder een certificeringsysteem wordt geleverd, dient vergezeld te gaan van de op de levering betrekking hebbende factuur en/of pakbon van de opdrachtnemer. Facturen moeten zijn voorzien van:

- naam en adresgegevens van de opdrachtgever en de opdrachtnemer;
- datum uitgifte;
- houtsoort en/of productbeschrijving;
- volume of aantal van het geleverd product;
- naam van het certificeringssysteem en de claim (bijv. FSC 100% of PEFC gecertificeerd);

- Chain-of-Custody certificaatnummer van de leverancier.

Verificatie
- Certificaat van de voor dit dossier verantwoordelijke staatssecretaris toegelaten certificeringssystemen, geldend op de datum van aankondiging. Voor alle goedgekeurde certificeringssystemen, zie de rechterkolom van de tabel judgements;
- Alternatief en verifieerbaar bewijs waaruit blijkt dat aan de gestelde eis wordt voldaan. Als hulpmiddel bij het leveren van alternatief bewijs kan de opdrachtnemer gebruik maken van Documents for Category B evidence.

4.5.4 Recycling kunststoffen

- Ambitieniveau: 1
- Criteriumtype: EIS
- Criteriumcode: 035.010

Eis
Voor speeltoestellen waarvan meer dan 25% van de massa van het eindproduct uit kunststoffen bestaat, dient van de totale hoeveelheid kunststoffen ten minste 50% (gewichtsprocenten binnen een product) gerecycled materiaal te zijn. Naast post-consumer materiaal mag ook pre-consumer materiaal gebruikt worden.

Definitie gerecycled of secundair materiaal :
Materiaal dat verkregen is via opwerking van afvalmateriaal. Dit kan een afvalstroom in een productieproces zijn (pre-consumer fase) of afkomstig van producten die al een eerdere gebruiksfunctie hebben vervuld, zoals consumentenafval (post-consumer fase).
- Pre-consumer materiaal (of: postindustrieel restmateriaal) is restmateriaal dat geen afval wordt in een productieproces. Uitgesloten is hergebruik zoals nabewerking en schroot, dat gegenereerd wordt in een proces en kan worden teruggewonnen binnen hetzelfde proces. Het gaat om materiaal gegenereerd door de industrie en niet is gebruikt door de consument;

- Post-consumer materiaal is restmateriaal dat door eindgebruikers van producten wordt geproduceerd bij afdanking van deze producten, als de eindgebruiker het product niet langer voor het beoogde doel kan gebruiken. Eindgebruikers zijn onder andere huishoudens, commerciële partijen en industriële partijen. Afdanking omvat het retouren van materiaal uit de distributieketen. Het gaat om materiaal afkomstig uit eerder gebruik of uit reststromen en dat primaire materialen vervangt. Het materiaal kan afkomstig zijn van zowel soortgelijke als andersoortige producten dan het doelproduct. Kenmerkend voor recycling is dat het materiaal gescheiden wordt tot een zo zuiver mogelijke grondstof en aan het begin van een productieproces wordt heringevoerd. Op voorhand van het recyclingproces is doorgaans niet bekend in welk eindproduct het materiaal terecht komt. Er is een bewerking nodig om de materialen opnieuw in te kunnen zetten in de oorspronkelijke of andere toepassing.

- Deze eis geldt niet:
Indien de opdrachtnemer hergebruikte of refurbished producten levert

Deze eis geldt niet voor de toepassing van kunststoffen in:
- touw en vezelversterkte kunststoffen;
- transparante of gekleurde overkappingen, vanwege vertroebeling.

4.5.5 Circulaire materialen voor verkeersborden en bewegwijzeringsborden

- Ambitieniveau: 1
- Criterium type: Eis
- Criterium code: 035.016

Te leveren, aan te brengen of te vervangen verkeers- en bewegwijzeringsborden (borden) dienen eerder gebruikt te zijn (hergebruik). Voor zover niet in eerder gebruikte borden kan worden voorzien, dienen de borden biobased te zijn of hebben een hoog recyceld content. In voorkomende gevallen wordt onderbouwd waarom (deels) niet eerder gebruikte borden worden geleverd of aangebracht.

Definitie hergebruik

- Bij het opnieuw gebruiken (hergebruik) van borden of onderdelen van borden die al eerder in gebruik zijn geweest behouden zij hun oorspronkelijke vorm. Ook het voorafgaand aan herplaatsing reviseren (refurbishen), oftewel het uitvoeren van kleine reparaties van borden en het vernieuwen van de signface, wordt gezien als 'hergebruik'.

Definitie en eisen biobased

- Een grondstof, materiaal of object(onderdeel) is biobased wanneer sprake is van niet-fossiel materiaal dat is gewonnen en geproduceerd op basis van hernieuwbare grondstoffen. Een hernieuwbare grondstof is een grondstof van biologische oorsprong, exclusief grondstoffen uit geologische afzetting of fossiele grondstoffen, die wordt beheerd en/of geteeld en die na winning binnen 100 jaar terug groeit zonder het betreffende ecosysteem uit te putten.
- Voor biobased borden geldt een aantoonbaar biobased content van tenminste 70% (massa).
- Biobased borden moeten zijn gemaakt van secundaire en/of tertiaire reststromen uit de Europese Unie. Ook geteelde biogrondstoffen kunnen worden toegepast, bij voorkeur uit de Europese Unie, zo mogelijk uit Nederland. Borden gemaakt van teeltproducten (niet zijnde reststoffen) van buiten de EU mogen alleen worden toegepast als de teeltproducten voldoen aan duurzaamheids- en kwaliteitscriteria opgesteld in het kader van de Green Deal Groencertificaten (https://greendealgroencertificaten.nl/).
- Bij gebruik van hout geldt: hout voldoet aan de "Dutch Procurement Criteria for Timber" ten aanzien van duurzaam bosbeheer en de handelsketen, zie criterium '(Verwerkt) Hout dient aan duurzaamheidseisen te voldoen'.

Eisen hoog recyceld content

- Voor metalen borden geldt voor aluminium een aantoonbaar recyceld content van tenminste 70% (massa) borden en voor stalen borden van tenminste 40% (massa).

Toelichting voor de inkopende organisatie
Deze eis kan van toepassing zijn op leveringen van borden en op diensten waarbij borden worden aangebracht en/of vervangen.

Verificatie
Voor wat betreft gebruikte borden

- Documentatie waaruit blijkt hoe invulling wordt gegeven aan de voorkeur voor eerder gebruikte borden. Met in voorkomende gevallen een onderbouwing waarom geen eerder gebruikte borden worden geleverd of aangebracht.
- Of gelijkwaardig

Voor wat betreft biobased content

- Certificaat waaruit blijkt dát en welk aandeel biobased grondstoffen zijn gebruikt, zoals 'OK biobased'-certificaat, 'DIN Geprüft Bio-based'-certificaat, of een gelijkwaardig certificaat.

- 'Groencertificaat', waarmee voor bepaalde productiemethoden, de biomassafractie van een biobased product rekenkundig kan worden bepaald via een gecertificeerde massabalans, of een gelijkwaardig certificaat.
- Rapport dat is opgesteld door een onafhankelijke derde, dat aantoont dat het gebruikte materiaal biobased is. Methodes die kunnen worden gebruikt om de biobased content te bepalen zijn:
    - de ASTM D6866 methode of gelijkwaardig;
    - een methode genoemd in [het Rapport 16721:2014 van CEN](European Committee for Standardization), dat een overzicht geeft van verschillende beschikbare methoden om de biobased fractie te bepalen.
- Of gelijkwaardig

Voor wat betreft duurzaamheid teeltproducten van buiten de EU

- Bewijsmateriaal waaruit blijkt dat wordt voldaan aan de duurzaamheids- en kwaliteitscriteria opgesteld in het kader van de Green Deal Groencertificaten. Mogelijke bewijsmiddelen zijn een ISCC/ISCC+, RSB, Bonsucro, Rainforest Alliance (SAN), RSPO, Better Biomass of gelijkwaardig certificaat.
- NTA 8080 certificaat, dat aantoont dat de biomassa die is gebruikt van duurzame herkomst is, of een gelijkwaardig certificaat.
- Of gelijkwaardig.

Voor wat betreft recyceld content metalen borden

- Technische documentatie van de leverancier waaruit het aandeel recyceld content blijkt van metalen borden en de omvang/hoogte daarvan.
- Of gelijkwaardig.

4.6 Wegen

4.6.1 Duurzaamheidseis voor een fietspad van gestort beton

- Ambitieniveau: 1
- Criteriumtype: EIS
- Criteriumcode: 036.29

Deze eis uit de RBA is opgenomen in de Vraagspecificatie.

4.6.2 Duurzaamheidseis voor nieuw te leveren stelbeton

- Ambitieniveau: 1
- Criteriumtype: EIS
- Criteriumcode: 036.30

Deze eis uit de RBA is opgenomen in de Vraagspecificatie.

4.6.3 Duurzaamheidseis voor nieuw te leveren betonstraatstenen

- Ambitieniveau: 1

- Criteriumtype: EIS
- Criteriumcode: 036.31

Deze eis uit de RBA is opgenomen in de Vraagspecificatie.

4.6.4 Duurzaamheidseis voor betontegels

- Ambitieniveau: 1
- Criteriumtype: EIS
- Criteriumcode: 036.32

Deze eis uit de RBA is opgenomen in de Vraagspecificatie.

4.6.5 Duurzaamheidseis voor nieuw te leveren grasbetontegels

- Ambitieniveau: 1
- Criteriumtype: EIS
- Criteriumcode: 036.33

Deze eis uit de RBA is opgenomen in de Vraagspecificatie.

4.6.6 Duurzaamheidseis voor nieuw te leveren industrieplaten

- Ambitieniveau: 1
- Criteriumtype: EIS
- Criteriumcode: 036.34

Deze eis uit de RBA is opgenomen in de Vraagspecificatie.

4.6.7 Duurzaamheidseis voor nieuw te leveren betonbanden

- Ambitieniveau: 1
- Criteriumtype: EIS
- Criteriumcode: 036.35

Deze eis uit de RBA is opgenomen in de Vraagspecificatie.

4.6.8 Maximale milieukosten asfaltdeklagen

- Ambitieniveau: 1
- Criteriumtype: EIS
- Criteriumcode: 036.37

Deze eis uit de RBA is opgenomen in de Vraagspecificatie.

4.6.9 Maximale milieukosten asfalt tussen- en onderlaag

- Ambitieniveau: 1
- Criteriumtype: EIS
- Criteriumcode: 036.38

Deze eis uit de RBA is opgenomen in de Vraagspecificatie

4.6.10 Duurzaamheidseisen voor nieuw te leveren straatbakstenen

- Ambitieniveau: 1
- Criterium type: Eis
- Criterium code: 036.041

De MKI-waarde voor nieuw te leveren straatbakstenen is maximaal 9,5 €/ton. De MKI-waarde moet berekend zijn volgens de laatste versie van de 'Bepalingsmethode Milieuprestatie Bouwwerken' (EN15804+A2) van de Nationale Milieudatabase. Voor de actuele versie, zie de website van de Nationale Milieudatabase. De MKI-waarde betreft de levenscyclusfasen A t/m D.

Uitgezonderd van bovenstaande eisen zijn straatbakstenen met toeslagstof chroomoxide (grijze straatbakstenen) en gesmoorde stenen (smoren is een extra bakproces waardoor het ijzeroxide in de stenen verkleurt naar grijstinten).

Toelichting voor de inkopende organisatie
Straatbakstenen bestaan volledig uit klei, eventueel voorzien van toeslagstoffen. De waarde voor de MKI is gebaseerd op de productbladen van BouwCirculair. De productbladen voor de GWW zijn te vinden op www.moederbestek.nl.

Verificatie

- Een categorie 1 LCA rapport.
- Een Environmental Product Declaration (EPD)
    - NB Beide documenten dienen getoetst en akkoord zijn bevonden door een erkende LCA-deskundige die op het moment van toetsen voorkomt op de 'Lijst van LCA- deskundigen die door de Stichting NMD als toetser erkend zijn voor het toetsen van categorie 1 en 2 data ten behoeve van opname in de Nationale Milieudatabase' zoals vastgesteld door Stichting NMD.
- Of gelijkwaardig.

4.7 Gemalen

4.7.1 Energierendement van systeem

- Ambitieniveau: 1
- Criteriumtype: EIS
- Criteriumcode: 037.001

Eis
Het systeem moet een energierendement hebben van minimaal [x]% in het bedrijfspunt/de bedrijfspunten [x] en een opvoerhoogte van [x] meterwaterkolom (mwk) gedurende een periode van [x] jaar gemeten volgens methode ISO 9906.
Onder het systeem wordt verstaan: [x] .

Voor het bepalen van het minimum rendement [X] van het systeem moet de inkopende organisatie uitgaan van de laatste stand van de techniek (best available technology). Met de laatste stand van de techniek wordt hier bedoeld: 'een (branche)gemiddelde van de best leverbare energiebesparende technieken en beste energiebesparende ontwerpoplossingen die binnen gangbare risico- en betrouwbaarheidsparameters kunnen worden toegepast'. Informatie over de laatste stand van de techniek kan bijvoorbeeld door een marktconsultatie worden opgehaald.
De inkopende organisatie eist het energierendement van het totale systeem bij vooraf bepaalde bedrijfspunt(en). De bedrijfspunten worden bepaald op basis van het gebruiksprofiel. Bij rioolgemalen zijn dit vaak 'Droog weer afvoer' (DWA) [X] in m^3/h gedurende [X] uren/jaar, 'Regen weer afvoer' (RWA), gedurende [X] uren/jaar en eventueel een verhoogd DWA [X] m^3/h gedurende [X] uren/jaar. En over een bepaalde periode (X jaren) gemeten. Overige systeemkenmerken zijn de opvoerhoogte (minimaal/maximaal) [mwk (meterwaterkolom)] en indien aanwezig bij een rioolgemaal de 'weerstand persleiding' [mwk].
In sommige gevallen kan er sprake zijn van een spanningsveld tussen een harde rendementseis en andere duurzaamheidsaspecten, bijvoorbeeld wanneer de acceptatie van iets hoger energieverbruik bij langere levensduur en grotere mate van circulariteit (herbruikbaarheid van onderdelen, losmaakbaarheid etc.) in de weg staat. Indien dit het geval is dient de inkopende organisatie hierin een afweging te maken en kan ze ervoor kiezen om de rendementseis naar beneden bij te stellen om ook andere duurzaamheidsdoelen te kunnen behalen.

Verificatie
- Bij de controle van de opgave van het rendement kan gebruik gemaakt worden van een pomptest, garantiemeting, of een gelijkwaardige methode.

Boetebepaling
Bij oplevering wordt het rendement van de pomp + elektromotoren + (indien aanwezig) frequentieregelaar gemeten volgens methode ISO 9906.
Mocht blijken dat het gemeten rendement lager uitvalt dan in de aanbieding is opgegeven, dan betaalt de leverende partij over elke procent lager rendement een boete [x].

4.7.2 Energierendement van systeemdelen

- Ambitieniveau: 1
- Criteriumtype: EIS
- Criteriumcode: 037.003

Eisen
Een te leveren pomp, elektromotor en/of ventilatiesysteem dient te voldoen aan de volgende eisen:
1. Het hydraulisch rendement van de pomp is minimaal [x]% bij het bedrijfspunt [x] m3/min en statische opvoerhoogte van [x] mwk.

2. Het rendement van een droog opgestelde elektromotor van een pompinstallatie gemeten volgens IEC 60034-2-1:2014 dient groter te zijn dan 95%. Voor elektromotoren tot 90kW moet minimaal een klasse IE3 motor worden toegepast.

3. Het ventilatiesysteem voldoet ten minste aan klasse SFP 2 volgens NEN-EN 16798-3:2017.

Boetebepaling
Bij oplevering wordt het rendement van de pomp + elektromotoren + (indien aanwezig) frequentieregelaar gemeten volgens methode ISO 9906.
Mocht blijken dat het gemeten rendement lager uitvalt dan in de aanbieding is opgegeven, dan betaalt de leverende partij over elke procent lager rendement een boete [x].

4.7.3 Gemalen / Minder milieubelastende smeeroliën, hydraulische vloeistoffen en vetten

- Ambitieniveau: 1
- Criterium type: EIS
- Criterium code: 037.004

Smeerolie, hydraulische vloeistoffen en vetten dienen te voldoen aan de criteria 1 t/m 4 voor de toekenning van de EU-milieukeur voor smeermiddelen Besluit (EU) 2018/1702.
Als bij gebruik van smeermiddelen met accidenteel verlies het vereiste smeermiddel afwijkt van de voorgeschreven specificaties van de leverancier (van de voer- en/of werktuigen) dan dient de opdrachtnemer in overleg met de leverancier het toe te passen smeermiddel bepalen.
Besluit (EU) 2018/1702 maakt onderscheid in:

- smeermiddel met volledig verlies: een smeermiddel dat tijdens het gebruik volledig in het milieu vrijkomt;
- smeermiddel met gedeeltelijk verlies: een smeermiddel dat tijdens het gebruik gedeeltelijk in het milieu vrijkomt en waarvan het niet-vrijgekomen gedeelte voor herverwerking, recyclage of verwijdering kan worden teruggewonnen;
- smeermiddel met accidenteel verlies: een smeermiddel dat in een gesloten systeem wordt gebruikt, enkel accidenteel in het milieu kan vrijkomen en na gebruik voor herverwerking, recyclage of verwijdering kan worden teruggewonnen.

Verificatie

- Technische productspecificaties of andere documentatie waaruit blijkt dat aan dit criterium is voldaan.
- (Geldig) certificaat van een ISO type I milieukeurmerk, waarvan de eisen overeenkomen met de in dit criterium gestelde eisen, of een gelijkwaardig certificaat. Meer informatie over ISO type I milieukeurmerk is te vinden op de website van PIANOo. Producten met het Europese Ecolabel voldoen aan de gestelde eisen 1 t/m 4. Op de website van de Europese Commissie is een lijst beschikbaar van oliën en vetten die voldoen aan de eisen van het Europese Ecolabel.

4.8 Waterzuiveringsinstallaties en slibbehandeling

4.8.1 Ecotoxiciteit chemicaliën

- Ambitieniveau: 1
- Criteriumtype: EIS
- Criteriumcode: 038.001

Eis
De toe te passen chemicaliën waarop de ABM-klassenindeling van toepassing is, dienen te voldoen aan ABM-klasse B of C.

4.9 Dooimiddelen

4.9.1 Inkoop uitvoering gladheidbestrijding op basis van CROW 353

- Ambitieniveau: 1
- Criterium type: Eis
- Criterium code: 039.001

Inschrijver werkt volgens een onderhoudsplan van het in te zetten strooimaterieel, welke is opgesteld op basis van CROW 353 (Organisatie en bestrijding van wintergladheid

Verificatie

- onderhoudsplan van in te zetten strooimaterieel;
- rapport van de B-beurt (winteronderhoud) volgens CROW 353;
- of gelijkwaardig.

4.10 Mobiele werktuigen uitbesteding

4.10.1 Emissie-eisen mobiele dieselwerktuigen met variabel toerental

- Ambitieniveau: 1
- Criteriumtype: EIS
- Criteriumcode: 040.001

Deze eis uit de RBA is opgenomen in de Vraagspecificatie.

4.10.2 Het nieuwe draaien

- Ambitieniveau: 1
- Criteriumtype: EIS
- Criteriumcode: 040.04

Eis

Het aandeel van de machinisten en/of uitvoerders, voormannen en planners dat bij de uitvoering van de opdracht is betrokken en de erkende training Het Nieuwe Draaien heeft gevolgd is minimaal 25%.
Daarnaast hebben alle projectmedewerkers een project specifieke introductie ontvangen met aandacht voor Het Nieuwe Draaien aan de start van het project. Projectmedewerkers die pas na de start werkzaam worden bij het project, dienen alsnog de introductie te ontvangen.
De certificaten van 'Het Nieuwe Draaien' (met daarop de datum van het behalen van het certificaat) van de gedurende de contractperiode in te zetten medewerkers dienen beschikbaar te zijn bij de opdrachtnemer zodat deze door opdrachtgever middels een audit kunnen worden gecontroleerd. De opdrachtnemer geeft aan op welke wijze projectmedewerkers een project specifieke introductie ontvangen.

Verificatie

- Certificaten Het Nieuwe Draaien van erkende instelling/trainer.
- Informatie waaruit blijkt hoe een project specifieke introductie wordt gegeven.
- Of gelijkwaardig.

4.10.3 Onderhoud gebruikte mobiele werktuigen

- Ambitieniveau: 1
- Criteriumtype: EIS
- Criteriumcode: 040.007

Eis
Voor de in te zetten mobiele werktuigen dient te worden aangetoond dat er structureel en hoogwaardig onderhoud is gepleegd met aandacht voor de aspecten:

- Toepassen correcte machine-instellingen op basis van fabrieksspecificatie;
- Uitvoeren van periodieke materieelkeuring;
- Voorgeschreven uitvoering van het onderhoudsprogramma.

Verificatie

- Schriftelijke verklaring van gebruiker waaruit blijkt dat
    - de machine volgens een periodiek keuringssysteem wordt gekeurd (kopie keuringsformulier of keuringssticker voldoet ook) en
    - de machine regulier onderhouden wordt middels een onderhoudsprogramma (kopie onderhouds/servicecontract voldoet ook).
- Of gelijkwaardig.

4.10.4 Minder milieubelastende smeeroliën, hydraulische vloeistoffen en vetten

- Ambitieniveau: 1
- Criterium type: EIS
- Criterium code: 040.008

Smeerolie, hydraulische vloeistoffen en vetten dienen te voldoen aan de criteria 1 t/m 4 voor de toekenning van de EU-milieukeur voor smeermiddelen Besluit (EU) 2018/1702.
Als bij gebruik van smeermiddelen met accidenteel verlies het vereiste smeermiddel afwijkt van de voorgeschreven specificaties van de leverancier (van de voer- en/of werktuigen) dan dient de opdrachtnemer in overleg met de leverancier het toe te passen smeermiddel bepalen.
Besluit (EU) 2018/1702 maakt onderscheid in:

- smeermiddel met volledig verlies: een smeermiddel dat tijdens het gebruik volledig in het milieu vrijkomt;

- smeermiddel met gedeeltelijk verlies: een smeermiddel dat tijdens het gebruik gedeeltelijk in het milieu vrijkomt en waarvan het niet-vrijgekomen gedeelte voor herverwerking, recyclage of verwijdering kan worden teruggewonnen;
- smeermiddel met accidenteel verlies: een smeermiddel dat in een gesloten systeem wordt gebruikt, enkel accidenteel in het milieu kan vrijkomen en na gebruik voor herverwerking, recyclage of verwijdering kan worden teruggewonnen.

Verificatie

- Technische productspecificaties of andere documentatie waaruit blijkt dat aan dit criterium is voldaan.
- (Geldig) certificaat van een ISO type I milieukeurmerk, waarvan de eisen overeenkomen met de in dit criterium gestelde eisen, of een gelijkwaardig certificaat. Meer informatie over ISO type I milieukeurmerk is te vinden op de website van PIANOo. Producten met het Europese Ecolabel voldoen aan de gestelde eisen 1 t/m 4. Op de website van de Europese Commissie is een lijst beschikbaar van oliën en vetten die voldoen aan de eisen van het Europese Ecolabel.

4.10.5 Mobiele werktuigen en Bouwlogistiek - Uitbesteding / Voertuigen voldoen tenminste aan basiseisen voor emissies

- Ambitieniveau: 1
- Criterium type: Minimumeis
- Criterium code: 040.014
- Onderwerp: Uitlaatemissies voertuigen

Deze eis uit de RBA is opgenomen in de Vraagspecificatie.

4.10.6 Verplichte training 'Het Nieuwe Rijden' voor chauffeurs met B-rijbewijs

- Ambitieniveau: 1
- Criterium type: EIS
- Criterium code: 040.018

Alle chauffeurs met B-rijbewijs van voor 2008 die ten behoeve van de uitvoering van de opdracht zullen worden ingezet, hebben een training gevolgd van "Het Nieuwe Rijden" of een daarmee gelijkwaardige training die op zuinig rijgedrag gericht is. Chauffeurs die over een rijbewijs afgegeven na 1 januari 2008 beschikken, hebben al rijgedrag volgens "Het Nieuwe Rijden" aangeleerd en hoeven de training niet te volgen.
De certificaten van "Het Nieuwe Rijden" (met daarop de datum van het behalen van het certificaat) van de gedurende de contractperiode in te zetten chauffeurs dienen beschikbaar te zijn bij opdrachtnemer zodat deze door opdrachtgever middels een audit kunnen worden gecontroleerd. Indien chauffeurs aantoonbaar rijden in voertuigen die zijn uitgerust met een softwaresysteem voor monitoren en verbeteren van het rijgedrag, volstaat dit ook.

Verificatie:

- Certificaten van "Het Nieuwe Rijden" (met daarop de datum van het behalen van het certificaat) van de gedurende de contractperiode in te zetten chauffeurs.
- Informatie waaruit blijkt dat chauffeurs rijden in voertuigen die zijn uitgerust met een softwaresysteem voor monitoren en verbeteren van het rijgedrag.

4.11 Verkeersregelinstallaties

4.11.1 Diminrichting in regeltoestel

- Ambitieniveau: 1
- Criteriumtype: EIS
- Criteriumcode: 041.001

Eisen

1. Bij nieuwbouw dient een regeltoestel met diminrichting toegepast te worden, conform paragraaf 2, lid 4 van de Regeling Verkeerslichten van 1 juli 2019
2. Bij bestaande VRI-installaties dient een diminrichting te worden toegepast als dit technisch mogelijk is, zonder meerkosten, en als de roodlicht- en lampbewaking blijven functioneren.

4.11.2 Energiezuinige lichtbronnen

- Ambitieniveau: 1
- Criteriumtype: EIS
- Criteriumcode: 041.002

Eis

Energiezuinige lichtbronnen volgens Klasse II lichtbronnen.

Verificatie• Technische specificaties waaruit blijkt lichtbronnen klasse II worden toegepast;
• Of gelijkwaardig

4.11.3 Energiezuinige lampen voor scheepvaartseinen

- Ambitieniveau: 1
- Criteriumtype: EIS
- Criteriumcode: 041.004

Eis

Bij nieuwbouw of complete vervanging van scheepvaartseinen dienen Led2-lampen (of lampen met een vergelijkbare energiezuinigheid en levensduur), met 2 dimstanden en een HR dimtrafo te worden geïnstalleerd.

Verificatie

- KEMA-keur;
- Of gelijkwaardig.

4.11.4 Levenscycluskosten

- Ambitieniveau: 1
- Criteriumtype: EIS
- Criteriumcode: 041.012

Deze eis uit de RBA is opgenomen in de Vraagspecificatie.

4.11.5 Minimale levensduur en garantie

- Ambitieniveau: 1
- Criteriumtype: EIS
- Criteriumcode: 041.014

Eisen

Het eerste deel van de eisen is opgenomen in de Vraagspecificatie.

Aanvullende eisen:

1. De reparatie of de levering van relevante vervangingsonderdelen voor led-aspecten die abrupt defect raken, moet worden gedekt door een garantie van minimaal 5 jaar vanaf de datum van installatie.
   De opdrachtnemer moet een ondertekende kopie van de garantie verstrekken en moet de nodige contactgegevens (minimaal telefoonnummer en e-mailadres) voor de afhandeling van gerelateerde vragen of mogelijke claims bevatten. Aan de garantie worden de volgende eisen gesteld:
2. De garantie moet de kosten van de reparatie of vervanging van defecte onderdelen van ledmodules dekken binnen een redelijke termijn na melding van het defect (door de inkopende organisatie te specificeren in de uitnodiging tot inschrijving), hetzij rechtstreeks, hetzij via andere aangewezen derden.
3. De vervangingsonderdelen moeten dezelfde zijn als de originele onderdelen, maar als dat niet mogelijk is, mogen gelijkwaardige reserveonderdelen worden gebruikt die dezelfde functie vervullen op hetzelfde of een hoger prestatieniveau.
   De garantie dekt niet de volgende zaken:
   a) gebrekkige werking als gevolg van vandalisme, ongevallen of extreme weergebeurtenissen;
   b) led-units of armaturen die al geruime tijd onder abnormale omstandigheden werken (bijv. gebruikt met de verkeerde netspanning), voor zover dit door de aannemer kan worden aangetoond.

Verificatie

- Een test en verificatierapport opgesteld door een laboratorium dat door de International Laboratory Accreditation Cooperation is geaccrediteerd en dat voldoet aan IES LM-84 voor feitelijke gegevens en IES TM-28 voor geraamde gegevens;
- Of vergelijkbaar.

4.12 Groenvoorzieningen

4.12.1 Verwerven van bloembollen

- Ambitieniveau: 1

- Criteriumtype: EIS
- Criteriumcode: 043.002

Eisen
Minimaal 90 procent (berekend op basis van de aankoopsom) van het te gebruiken plantmateriaal (onder andere boomkwekerijproducten, bloembollen, vaste en eenjarige planten) voldoet ten minste aan de volgende eisen:

- Bij de teelt van het plantmateriaal zijn de volgende bepalingen ten aanzien van het gebruik van gewasbeschermingsmiddelen van toepassingopgenomen. De lijsten waarnaar wordt verwezen zijn te downloaden via deze link en zijn onderdeel van het certificatieschema On the way to PlanetProof:
    - Gewasbeschermingsmiddelen zijn niet toegestaan uit bijlage 2c, lijst I.
    - Er zijn aantoonbaar compenserende maatregelen genomen voor gewasbeschermingsmiddelen uit bijlage 2c, lijst II.
    - De middelen van lijst II van bijlage 2c en de overige wettelijk toegelaten gewasbeschermingsmiddelen die niet zijn genoemd in lijst I en lijst II van bijlage 2c., en ook niet in de lijst groene middelen/ laag risico-stoffen uit bijlage 2b, mogen onder de wettelijke voorwaarden worden gebruikt indien de maximale hoeveelheid actieve stof beneden de norm uit bijlage 1 blijft (actieve stofnorm).
    - De eisen 2.4 en 2.5 (maatregelen om de emissie van gewasbeschermingsmiddelen in het milieu te beperken) zijn aantoonbaar toegepast. In het geval het afsluiten van het contract en de levering in twee opeenvolgende kalenderjaren plaatsvindt, kan, indien aanwezig, de lijst toegestane middelen van één van deze jaren gebruikt worden.
- Bij de teelt van het plantmateriaal zijn voor de bemesting de wettelijke gebruiksnormen gehanteerd en is de organische stofbalans op bedrijfsniveau berekend. Hierbij moet inzichtelijk worden gemaakt dat het bedrijf een positieve organische stofbalans realiseert(jaarlijkse aanvoer van effectieve organische stof (EOS) is minimaal gelijk aan afbraak).
- Bij levering zit een lijst van het geleverde plantmateriaal met een opgave van de producten die voldoen aan de gestelde eisen en het daaruit afgeleide percentage van het totaal aan producten dat voldoet.

Verificatie

- Certificaat afgegeven door een voor het betreffende certificatieschema geaccrediteerde certificerende instelling, zoals:
    - On the way to PlanetProof;
    - Groenkeur boomkwekerijproducten;
    - MPS met aanvullend duurzaamheidscertificaat of –verklaring (voor het voldoen aan de lijst met toegestane gewasbeschermingsmiddelen uit het On the way to PlanetProof schema);
    - biologische keurmerken, zoals EU Bio keurmerk, EKO-keur, Demeter;
    - of gelijkwaardig.
- Registratie van de bij de teelt van de geleverde boomkwekerijproducten en bloembollen gebruikte gewasbeschermingsmiddelen en meststoffen, met van toepassing zijnde berekeningen waaruit blijkt dat binnen de gestelde normen is gebleven en bewijs van compenserende- en emissiebeperkende maatregelen. Deze registratie, berekeningen en compenserende- en emissiebeperkende maatregelen moeten zijn geaccordeerd door een onafhankelijke deskundige

derde (zoals een geaccrediteerde certificerende instelling). Het document kan per boomkwekerijkproduct of partij bloembollen zijn opgesteld, of de geaggregeerde gegevens van meerdere producten bevatten.

- Of gelijkwaardig.

4.12.2 Boomkwekerijproducten van een genetische kwaliteit (buitenstedelijk)

- Ambitieniveau: 1
- Criteriumtype: EIS
- Criteriumcode: 043.004

Deze eis uit de RBA is opgenomen in de Vraagspecificatie.

4.12.3 Meststoffen en bodemverbeteraars bij aanleg en onderhoud van openbaar groen (incl. sport- en speelvelden)

- Ambitieniveau: 1
- Criteriumtype: EIS
- Criteriumcode: 043.006

Eis
Het toepassen van meststoffen en/of bodemverbeteraars gebeurt conform een recente bodemanalyse (niet ouder dan drie jaar) en bijbehorend advies, uitgevoerd door een geaccrediteerd laboratorium en een ter zake kundig adviesbureau.

- De bodemanalyse omvat minimaal:
  - pH waarde en kalkbehoefte;
  - gehalte fosfaat, kali, magnesium, zwavel en stikstof;
  - organische stof en lutumgehalte.
- Het advies aangaande bemesting
  - geeft aan welke minimale hoeveelheid bemesting nodig is voor behoud van de kwaliteit van de beplanting gezien de staat van de bodem en de behoefte van de beplanting;
  - geeft, indien bemesting nodig is, aan welk type (of combinatie van typen) meststof(fen) moet worden gebruikt bij aanplant en eventueel in de onderhoudsfase met het oog op minimaal risico op uitspoeling;
  - biedt alleen ruimte voor incidentele tussentijdse extra stikstofbemesting, als de uitvoerder telkens met een N-mineraal monster aantoont dat dit nodig is voor het behoud van de kwaliteit van de beplanting.
- Het advies aangaande bodemverbetering
  - geeft aan of bodemverbeteraars nodig zijn voor het behoud of de verbetering van de kwaliteit van de bodem en het van nature aanwezige bodemleven;
  - geeft, indien bodemverbetering gewenst is, aan welk type(s) bodemverbeteraar gewenst is/zijn en hoe deze keuze aansluit op de bemestingsbehoefte van het plantmateriaal.

4.12.4 Ongewenste kruiden, ziekten en plagen (excl. sport- en speelvelden)

- Ambitieniveau: 1
- Criteriumtype: EIS

- Criteriumcode: 043.007

Eis
Bij de uitvoering van de werkzaamheden worden geen gewasbeschermingsmiddelen en biociden gebruikt

Verificatie
- Barometer Duurzaam terreinbeheer Zilver of Goud
- ;
- of gelijkwaardig.

4.12.5 Duurzaam ontwerp groenvoorziening

- Ambitieniveau: 1
- Criteriumtype: EIS
- Criteriumcode: 043.009

Deze eis uit de RBA is opgenomen in de Vraagspecificatie.

4.12.6 Eisen aan compost

- Ambitieniveau: 1
- Criteriumtype: EIS
- Criteriumcode: 043.017

Eisen:
De volgende eisen worden aan compost gesteld:
- Turf is niet toegestaan als organisch bestanddeel van een eindproduct;
- Het gehalte aan glas, metaal en plastic met een maaswijdte van > 2 mm (de som van alle bijdragen) in het eindproduct mag niet meer dan 0,1% bedragen, gemeten op basis van het droge gewicht.
- Het gehalte aan primaire ziekteverwekkers in het eindproduct mag niet hoger zijn dan de volgende waarden:
    - Salmonella spp: afwezig in 25 g vers gewicht;
    - E.coli: < 1000 kve/g vers gewicht (kve: kolonievormende eenheden).

Verificatie:
- Informatie over de gedetailleerde productsamenstelling, de herkomst van het organische materiaal en een verklaring over naleving van bovenstaande eisen verstrekken.
- Een Keurcompost certificaat, klasse A.
- Een EU-milieukeur certificaat voor groeimedia, bodemverbeteraars en strooisel overeenkomstig Besluit (EU) 2015/2099 van de Commissie1 of andere relevante milieukeur type I die aan de gespecificeerde criteria voldoet.
- Andere passende vormen van bewijs, zoals een technisch dossier van de fabrikant of een keuringsrapport van een onafhankelijke instantie.
- Of gelijkwaardig

4.12.7 Geen invasieve exoten

- Ambitieniveau: 1
- Criteriumtype: EIS
- Criteriumcode: 043.018

Eis:
Indien uitheemse soorten worden geplant, zijn deze niet (potentieel) invasief.
Het is niet toegestaan om plantmateriaal aan te planten van soorten die op de lijst van invasieve landplanten staan van de NVWA..

Verificatie
- Informatie verstrekken over (de naam van) het plantmateriaal dat wordt geleverd.
- Of gelijkwaardig.

Gebaseerd op EU GPP

4.13 Reiniging openbare ruimte

4.13.1 Verwijderen van graffiti met hogedrukwaterreiniger

- Ambitieniveau: 1
- Criteriumtype: EIS
- Criteriumcode: 044.001

Eis
Graffitiverwijdering van andere objecten dan gevels moet gebeuren met een hogedrukwaterreiniger (met eventueel het gebruik van reinigingsmiddelen) voorzien van een scheidingssysteem waardoor het vuile water opgevangen wordt en daarna verwerkt kan worden. Bijvoorbeeld met een waterrecyclesysteem dat het reinigingswater opvangt, filtert en hergebruikt.

Wanneer reinigingsmiddelen voor het verwijderen van graffiti worden gebruikt, is de eis ‘reiniging openbare ruimte / Milieukeur voor buitenschoonmaakmiddelen is verplicht’ van toepassing.

4.13.2 Milieu-impact onkruidbestrijding op verhardingen

- Ambitieniveau: 1
- Criteriumtype: EIS
- Criteriumcode: 044.006

Eis
Dit criterium is van toepassing daar waar volgens het Besluit gewasbeschermingsmiddelen en biociden, chemische onkruidbestrijding niet toelaatbaar is. Gedurende de contractperiode moet het aantal werkronden mechanische onkruidbestrijding beperkt blijven tot:
- voor de heteluchtmethode maximaal 6 werkronden per jaar;
- voor de overige mechanische methoden maximaal 4 werkronden per jaar
  Of De inschrijver dient aan te tonen dat er niet meer dan 350 kg aardgas (of vergelijkbaar broeikaseffect) per hectare per jaar wordt ingezet op verhardingen.

Verificatie

- Certificaat Barometer Duurzaam Terreinbeheer Niveau Zilver of Goud.
- Overige documentatie, waaruit blijkt dat:
    - Externe audits waarin steekproefsgewijs wordt gecontroleerd dat er geen bestrijdingsmiddelen zijn gebruikt;
    - Administratieve controle dat de chemievrije werkwijze in de onderhoudscontracten en opdrachten expliciet staat opgenomen;
    - Voor het aantonen van een maximale hoeveelheid werkronden per jaar: administratieve audit op basis van de registraties van mechanische onkruidbestrijding op verhardingen conform de gestelde criteria;
    - Niet meer dan 350 kg aardgas (of vergelijkbaar broeikaseffect) per hectare per jaar wordt ingezet op verhardingen: administratieve controle van het totale verbruik door onkruidbestrijdingsapparatuur in relatie tot machine-efficiëntie op basis van de hoeveelheid brandstof per hectare plaats zal vinden.
- Of gelijkwaardig.

4.13.3 Vermindering van PM10 straatstof

- Ambitieniveau: 1
- Criteriumtype: EIS
- Criteriumcode: 044.013

Eis:
De inschrijvers dienen te beschikken over schriftelijke procedures betreffende maatregelen ter vermindering van PM10-straatstof die moeten worden uitgevoerd door de volgende beste praktijken (of andere relevante maatregelen):

- stofbestrijdingspraktijken (stofbestrijdingsoplossingen, dispersietechnieken);
- straatreinigingspraktijken (mechanische en vacuümveegmachines, straatschrobbers, combinaties).

Verificatie

- Schriftelijke procedures en een schoonmaakdienstenplan voor het verminderen van PM10-straatstof, met inbegrip van de uitrusting en producten die worden gebruikt bij de uitvoering van de opdracht. Wanneer buitenschoonmaakmiddelen worden gebruikt moeten deze voldoen aan de eis ‘milieukeur voor buitenschoonmaakmiddelen’.
- of gelijkwaardig.

4.13.4 Milieukeur voor buitenschoonmaakmiddelen

- Ambitieniveau: 1
- Criteriumtype: EIS
- Criteriumcode: 044.014

Eisen

1. De te gebruiken buitenschoonmaakmiddelen voldoen aan de eisen zoals beschreven in Besluit (EU) 2017/1217 van de Commissie van 23 juni 2017 tot vaststelling van de criteria voor de toekenning van de EU-milieukeur aan schoonmaakproducten voor harde oppervlakken, of gelijkwaardig.
2. Schoonmaakproducten moeten worden geleverd met de aanbevolen doseringssystemen* (bv. pomp, maatcilinder), indien van toepassing. De informatie op het technisch gegevensblad van het doseringssysteem moet de dosis en de dispenser specificeren.

** Onder doseersystemen wordt verstaan: een doseerstation, doseerapparaat, doseerpatroon, of een alternatief dat tot hetzelfde resultaat leidt (het doseren van schoonmaakproducten). De leverancier van*

reinigingsmiddelen dient duidelijke doseerinstructies mee te leveren, zodat het reinigingsmiddel in de juiste hoeveelheden wordt toegepast.

Verificatie

EU-Ecolabel certificaat, of een gelijkwaardig certificaat;
Technisch gegevensblad met informatie over de wijze van doseren;
of gelijkwaardig.

Gebaseerd op EU GPP

4.14 Vaartuigen

4.14.1 Voorzieningen voor afvalwater

- Ambitieniveau: 1
- Criterium type: Minimumeis
- Criterium code: 045.001
- Onderwerp: Afvalwater

Het schip is voorzien van:

1. lekbakken voor lekwater en lekolie;
2. een gescheiden opvangsysteem en opslagsysteem voor lekwater en lekolie;
3. een grijswatertank met koppeling voor walafgifte indien er geen sprake is van een gesloten systeem of van behandeling aan boord;
4. een vuilwatertank met koppeling voor walafgifte;
5. indien het schip is voorzien van meerdere brandstofbunkers, zijn deze voorzien van een overvulbeveiliging, die de trimpomp buiten werking stelt bij overvullen.

Verificatie

- scheepsbouwkundig ontwerp of de tekeningen waaruit direct is af te lezen of de gevraagde voorzieningen zijn opgenomen;
- of gelijkwaardig.

4.14.2 Minder milieubelastende smeeroliën, hydraulische vloeistoffen en vetten

- Ambitieniveau: 1
- Criterium type: Minimumeis
- Criterium code: 045.002
- Onderwerp: Minder milieubelastende smeerolie, hydraulische vloeistoffen (en vetten)

Smeerolie, hydraulische vloeistoffen en vetten dienen te voldoen aan de criteria 1 t/m 4 voor de toekenning van de EU-milieukeur voor smeermiddelen Besluit (EU) 2018/1702.

Als bij gebruik van smeermiddelen met accidenteel verlies het vereiste smeermiddel afwijkt van de voorgeschreven specificaties van de leverancier (van de voer- en/of werktuigen) dan dient de opdrachtnemer in overleg met de leverancier het toe te passen smeermiddel bepalen.
Besluit (EU) 2018/1702 maakt onderscheid in:

- smeermiddel met volledig verlies: een smeermiddel dat tijdens het gebruik volledig in het milieu vrijkomt;
- smeermiddel met gedeeltelijk verlies: een smeermiddel dat tijdens het gebruik gedeeltelijk in het milieu vrijkomt en waarvan het niet-vrijgekomen gedeelte voor herverwerking, recyclage of verwijdering kan worden teruggewonnen;
- smeermiddel met accidenteel verlies: een smeermiddel dat in een gesloten systeem wordt gebruikt, enkel accidenteel in het milieu kan vrijkomen en na gebruik voor herverwerking, recyclage of verwijdering kan worden teruggewonnen.

Verificatie

- Technische productspecificaties of andere documentatie waaruit blijkt dat aan dit criterium is voldaan.
- (Geldig) certificaat van een ISO type I milieukeurmerk, waarvan de eisen overeenkomen met de in dit criterium gestelde eisen, of een gelijkwaardig certificaat. Meer informatie over ISO type I milieukeurmerk is te vinden op de website van PIANOo. Producten met het Europese Ecolabel voldoen aan de gestelde eisen 1 t/m 4. Op de website van de Europese Commissie is een lijst beschikbaar van oliën en vetten die voldoen aan de eisen van het Europese Ecolabel.
- Of gelijkwaardig.

4.14.3 Vaartuigen / Varend materieel voldoet aan basiseisen voor emissies

- Ambitieniveau: 1
- Criterium type: Eis
- Criterium code: 045.003

Deze eis uit de RBA is opgenomen in de Vraagspecificatie.

4.14.4 Maximaal energieverbruik vaartuig

- Ambitieniveau: 1
- Criterium type: Eis
- Criterium code: 045.005

Deze eis uit de RBA is opgenomen in de Vraagspecificatie.

4.14.5 Varend materieel gebruikt tenminste een basis aandeel duurzame energiedragers

- Ambitieniveau: 1
- Criterium type: Eis

- Criterium code: 045.016
- Deze eis uit de RBA is opgenomen in de Vraagspecificatie.

Ter informatie wordt hieronder een overzicht gegeven van de eisen in dit document en de codes waarmee deze eisen opgenomen zijn in de MVI-criteriatool.

Productgroep	Criterium	Code
Civiele constructies	Duurzaam ontwerp houten constructie	029.001
Civiele constructies	Duurzaam ontwerp staalconstructie	029.002
Civiele constructies	Duurzaam hout	029.007
Civiele constructies	Milieuvriendelijke smeermiddelen voor bewegingswerken	029.012
Civiele constructies	Betonmortel – constructief beton in het werk gestort	029.018
Civiele constructies	Keerwanden -prefab beton	029.019
Civiele constructies	Stelbeton	029.020
Civiele constructies	Stapelblokken prefab beton	029.021
Civiele constructies	Kanaalplaatvloeren	029.022
Civiele constructies	Verhardingslaag - gestort	029.023
Civiele constructies	Breedplaatvloeren - beton	029.024
Civiele constructies	Waterbouw asfalt	029.024
Conserveringswerken	Oplosmiddelarme conserveringssystemen	030.001
Conserveringswerken	Producten met lood- of chromaathoudende pigmenten	030.002
Conserveringswerken	Leveren beheer- en onderhoudsplan	030.004
Openbare verlichting	Toepassen ledverlichting	033.001
Openbare verlichting	Levensduur ledsysteem	033.002
Openbare verlichting	Dimbare OVL-installatie	033.003
Openbare verlichting	Lichthinder wordt beperkt	033.004
Riolering	Duurzaamheidseis voor nieuw te leveren betonnen rioleringsbuizen tot 1.000 mm	034.102
Riolering	Duurzaamheidseis voor nieuw te leveren betonnen inspectieputten	034.013
Riolering	Duurzaamheidseis voor betonnen kolken	034.014
Straatmeubilair	Straatmeubilair (m.u.v. Speeltoestellen): meer dan 5% kunststof	035.001
Straatmeubilair	Straatmeubilair (incl. Speeltoestellen): verven	035.003
Straatmeubilair	Duurzaam hout	035.005
Straatmeubilair	Speeltoestellen - kunststof	035.010
Straatmeubilair	Inkoop en reparatie van Speeltoestellen – kunststof: bij meer dan 25% kunststof bestaat dit voor meer dan 50% uit gerecycled kunststofonderdelen voorzien van markering	035.016
Wegen	Duurzaamheidseis voor een fietspad van gestort beton	036.029
Wegen	Duurzaamheidseis voor nieuw te leveren stelbeton	036.030
Wegen	Duurzaamheidseis voor nieuw te leveren betonstraatstenen	036.031
Wegen	Duurzaamheidseis voor betontegels	036.032
Wegen	Duurzaamheidseis voor nieuw te leveren grasbetontegels	036.033
Wegen	Duurzaamheidseis voor nieuw te leveren industrieplaten	036.034
Wegen	Duurzaamheidseis voor nieuw te leveren betonbanden	036.035
Wegen	Maximale milieukosten asfaltdeklaag	036.037
Wegen	Maximale milieukosten asfalt tussen- en onderlaag	036.038
Wegen	Beheer- en onderhoudsplan	036.005

Gemalen	Energierendement van systeem	037.001
Gemalen	Energierendement van systeemdelen	037.003
Gemalen	Smeeroliën en hydraulische vloeistoffen	037.004
Waterzuiveringsinstallaties en slibbehandeling	Ecotoxiciteit chemicaliën	038.001
Mobiele werktuigen uitbesteding	Emissie-eisen mobiele dieselwerktuigen met variabel toerental	040.001
Mobiele werktuigen uitbesteding	Training in het nieuwe draaien	040.004
Mobiele werktuigen uitbesteding	Onderhoud gebruikte mobiele werktuigen	040.007
Mobiele werktuigen uitbesteding	Minder milieubelastende smeerolie, hydraulische vloeistoffen	040.008
Mobiele werktuigen uitbesteding	Uitlaatemissies voertuigen	040.014
Mobiele werktuigen uitbesteding	Het nieuwe rijden	040.018
Verkeersregelinstallaties	Diminrichting in regeltoestel	041.001
Verkeersregelinstallaties	Energiezuinige lichtbronnen	041.002
Verkeersregelinstallaties	Energiezuinige lampen voor scheepvaartseinen	041.004
Verkeersregelinstallaties	Levenscycluskosten	041.012
Verkeersregelinstallaties	Minimale levensduur en garantie	041.014
Groenvoorzieningen	Verwerven van bloembollen	043.002
Groenvoorzieningen	Boomkwekerijproducten van een genetische kwaliteit (buitenstedelijk)	043.004
Groenvoorzieningen	Meststoffen en bodemverbeteraars bij aanleg en onderhoud van openbaar groen (incl. sport- en speelvelden)	043.006
Groenvoorzieningen	Ongewenste kruiden, ziekten en plagen (excl. sport- en speelvelden)	043.007
Groenvoorzieningen	Duurzaam ontwerp groenvoorziening	043.009
Groenvoorzieningen	Eisen aan compost	043.017
Groenvoorzieningen	Geen invasieve exoten	043.018
Reiniging openbare ruimte	Verwijderen van graffiti met hogedrukwaterreiniger	044.001
Reiniging openbare ruimte	Minder milieu-impact onkruidbestrijding op verhardingen	044.006
Reiniging openbare ruimte	Verminderen van PM10 straatstof	044.013
Reiniging openbare ruimte	Milieukeur voor buitenschoonmaakmiddelen	044.014
Reiniging openbare ruimte	Ondergrondse containerbak	044.015
Vaartuigen	Afvalwater	045.001
Vaartuigen	Minder milieubelastende smeerolie, hydraulische vloeistoffen	045.002
Vaartuigen	Uitlaatemissies	045.003
Vaartuigen	Energieverbruik ban het vaartuig	045.005
Vaartuigen	Duurzame energiedragers	045.016

Bijlage L Minimum eisen emissienormen materieel en energiedragers

Minimum eisen emissienormen materieel en energiedragers				
Materieel	Periode 1 2023-2024	Periode 2 2025-2027	Periode 3 2028-2029	Periode 4 2030 en verder
(Mobiele) werktuigen				
Minimaterieel (<19kW)	Geen minimum eis	Geen minimum eis	100% ZE	100% ZE
Zeer licht materieel (19-37 kW)	Stage IIIa	Stage IIIa	100% ZE	100% ZE
Licht materieel (37-56 kW)	Stage IIIb	Stage IIIb	100% ZE	100% ZE
Middelzwaar materieel (56-130 kW)	Stage IIIb	Stage IV met roetfilter[1]	Stage IV met roetfilter[1]	Stage IV met roetfilter[1] Vanaf 2035: 100% ZE
Zwaar materieel (130-560 kW)	Stage IIIb	Stage IV met roetfilter[1]	Stage IV met roetfilter[1]	Stage IV met roetfilter[1] Vanaf 2035: 100% ZE
Zeer zwaar materieel (>560 kW) en Specialistisch materieel (levensduur >15 jaar)	Geen eis	Geen eis	Katalysator en roetfilter[1]	Katalysator en roetfilter[1] Vanaf 2035: 100% ZE
Stationair materieel	Gelijk aan eisen niet-stationair	Gelijk aan eisen niet-stationair	Indien <130 kW: 100% ZE Indien >130 kW: gelijk aan eisen niet-stationair	Indien <130 kW: 100% ZE Indien >130 kW: gelijk aan eisen niet-stationair
Percentage ZE verrichte arbeid in het project (draaiuren * vermogen)	10-30%	30-70%	70-90%	90-100%
Percentage ZE materieel (mobiele) werktuigen	10%	30%	70%	90%

[1] Met 'katalysator' wordt bedoeld een effectieve SCR-katalysator. Met 'roetfilter' wordt bedoeld een werkend, gesloten roetfilter.
[2] Biobrandstoffen dienen aantoonbaar te voldoen aan de RED II middels een kopie van de Proof of Sustainability volgens ISCC (PoS).

De toegepaste begrippen komen overeen met de begrippen zoals gedefinieerd in de internationale emissiewetgeving.

Bijlage M Levering Areaalgegevens

In deze bijlage staat een aantal eisen met betrekking tot de levering van areaalgegevens ten behoeve van het beheer van het areaal door Rijkswaterstaat.

Tijdens de looptijd van de Overeenkomst kunnen de specificaties van de databestanden genoemd in deze bijlage wijzigen. De Opdrachtnemer dient te borgen, dat het door hem op te leveren bestand conform de op het moment van levering geldende versie is opgebouwd. De Opdrachtnemer kan er vanuit gaan, dat deze wijzigingen minimale extra kosten met zich meebrengen. Indien de wijzigingen meer kosten dan wat redelijkerwijze door de Opdrachtnemer kan worden ingeschat, dan dient hij dit onderbouwd aan de Opdrachtgever voor te leggen.

Voor de in deze bijlage genoemde software geldt, dat ten tijde van de oplevering de dan bij de Opdrachtgever vigerende versie dient te worden gehanteerd.

Data-eisen

1. Areaalgegevens

Data 00 Toegang tot beheerapplicaties en basisregistraties
De Opdrachtgever verleent de Opdrachtnemer toegang tot de nodige beheerapplicaties van het Beheer Management Systeem (BMS) van de Opdrachtgever en basisregistraties. Voor de toegang tot de beheerapplicaties en basisregistraties bestaan verschillende procedures. Een account mag alleen worden gebruikt door degene voor wie het is aangevraagd.
Tevens stelt de Opdrachtgever, indien nodig, één PC met benodigde software beschikbaar op een Rijkswaterstaatlocatie.

De aanvraag voor de toegang tot beheerapplicaties en basisregistraties gaat als volgt:

- Ultimo RWS, DISK, Meridian, 1GIS, LV BRO en LV BGT: de Opdrachtnemer dient de aanvraag in te dienen bij de Opdrachtgever. Voor DISK betreft dit zowel autoriseren als certificeren;
- Overige beheerapplicaties en basisregistraties: op verzoek van de Opdrachtnemer zal de Opdrachtgever hier de contactpersoon voor doorgeven.

Het BMS bestaat uit de volgende beheerapplicaties:

Beheerapplicatie	Van toepassing	Toegang
Ultimo RWS	Ja	Internet
1GIS	Ja	Internet
Basisregistratie Grootschalige Topografie (BGT)	Ja	Internet
DISK	Ja	Internet

Beheer Technische Documentatie (Meridian)	Ja	PC RWS locatie
NWB en WEGGEG	Nee	Internet
Garanties	Ja	Internet

Data 01 Droog en nat

De Opdrachtnemer dient de areaalgegevens van het door hem uitgevoerde Werk te leveren, zodat Rijkswaterstaat een goed beheer over het areaal kan doen. Hiervoor dient de Opdrachtnemer de volgende lijst als uitgangspunt te gebruiken: “Areaalinformatie RWS” te downloaden van www.rws.nl/datacontracteisen, tabblad Areaalgegevens.

Indien er areaalgegevens zijn, die niet op de lijst staan, maar die naar analogie van de rest van de lijst logischerwijs ook zouden moeten worden geleverd, dan dient de Opdrachtnemer hiervoor zo spoedig mogelijk na constatering een voorstel aan de Opdrachtgever te doen en deze na goedkeuring van het voorstel te leveren.
Indien door de Opdrachtnemer te bouwen objecten ontbreken op de lijst, dan dient hij zo spoedig mogelijk na constatering een voorstel te doen aan de Opdrachtgever over welke areaalgegevens van het object logischerwijs conform vergelijkbare objecten op de lijst door hem aan de Opdrachtgever moeten worden geleverd. Tevens dient de Opdrachtnemer deze areaalgegevens te leveren na goedkeuring van het voorstel door de Opdrachtgever.

De wijze waarop de gegevens moeten worden aangeleverd is afhankelijk van het systeem respectievelijk het format, dat in de bovengenoemde lijst per gegeven staat aangegeven in de kolom “Opslagsystemen / Format voor gegeven”. Indien er meerdere systemen en/of formats staan genoemd, dan dient voor al deze systemen en formats in het eigen formaat gegevens te worden aangeleverd.

- AutoCAD conform eis Data 02 “AutoCAD bestanden en tekeningen”;
- AutoCAD: conform RWS-CIV-voorschriften: conform eis Data 12 “Deformatiemetingen Kunstwerken”;
- Bronbestand: ieder pakket dient te worden geleverd op een voor het netwerk van Rijkswaterstaat geschikte gegevensdrager en dient een bestand te bevatten met een beschrijving van de inhoud van de levering;
- DISK c.q. Kunstwerkpaspoort: conform eisen Data 07 t/m Data 14 “Werkzaamheden met betrekking tot Kunstwerken en Verkeerskundige Draagconstructies”, waarbij Documenten inleesbaar zijn in MS Office. Tekeningen dienen conform eis Data 02 “AutoCAD bestanden en tekeningen” te worden aangeleverd.
- Document: opzet conform voorschriften Regionale Dienst. In geval een specifiek voorschrift in de bovengenoemde lijst wordt genoemd, geldt het genoemde voorschrift;
  bestandsformaat: inleesbaar inMS Office;
  indien alleen analoog beschikbaar: scannen en aanleveren in Adobe Reader;

- Foto of schets van doorrijprofiel: conform eis Data 17 “Doorrijprofielen”;
- 1GIS conform eis Data 03 “1GIS
- Garantie: conform eis Data 19 “Garantie”;
- Ultimo RWS: Conform eis Data 23 “Ultimo RWS”;
- Beheer Technische Documentatie (Meridian): conform eis Data 24 “Meridian”;
- Technisch Constructie Dossier (TCD): volgens regionale specificaties;
- Nationaal Wegenbestand (NWB) en Weggegevens Hoofdwegennet (WEGGEG): conform eis Data 20 “Nationaal Wegenbestand (NWB) en Weggegevens Hoofdwegennet (WEGGEG)”;
- Elektronische Navigatiekaart (ENC): Conform eis Data 21 “Elektronische Navigatiekaart”.

Bestanden dienen een naamgeving te hebben conform de aan het bestand gerelateerde documentatie. Indien dit niet is beschreven, dient de bestandsnaam de inhoud van het bestand weer te geven door middel van de typering van het document en een kenmerk (bijvoorbeeld het soort vergunning met vergunningnummer: “Vergunning WVO 102987.pdf”).

Data 01.a Consistentie in beheerapplicaties en basisregistraties

Rijkswaterstaat heeft een aantal beheerapplicaties en maakt gebruik van een aantal basisregistraties, met daarin gedeeltelijk dezelfde objecten en areaalgegevens. Iedere beheerapplicatie en basisregistratie heeft een eigen doel en inhoud (zie document ‘Toelichting OMS, BMS en Beheerapplicaties’ te downloaden van https://standaarden.rws.nl/link/standaard/6071), maar waarvan de inhoud wel aan elkaar is gerelateerd.

De Opdrachtnemer dient de gegevens in de beheerapplicaties van het Beheer Management Systeem en basisregistraties zodanig te actualiseren dat de decompositie, meta- en areaalgegevens in de beheerapplicaties en basisregistraties consistent zijn.

Het actualiseren van de GIS-beheerapplicaties, Ultimo RWS en zo nodig van DISK mag parallel lopen.

De Opdrachtnemer dient ten minste te voldoen aan de volgende eisen met betrekking tot het borgen van de consistentie van de areaalgegevens en de volgorde van het actualiseren van de beheerapplicaties en basisregistraties:

1. DISK en Ultimo RWS voor wat betreft kunstwerken:
   a. Nieuwe kunstwerken of onderdelen aanmaken voor in Ultimo RWS.
   b. Nieuwe kunstwerken of onderdelen aanmaken in DISK in overeenstemming met decompositie in Ultimo RWS.
2. GIS-bestanden:

a. De geactualiseerde gegevens van de definitieve terreinsituatie in de Basisregistratie Grootschalige Topografie (BGT) dienen te worden gebruikt om het 1GIS op te bouwen en aan te vullen.
b. Het DTB verder opbouwen en aanvullen met de niet-BGT gegevens van de definitieve terreinsituatie.
d. De GIS-laag “Kabels & Leidingen” dient conform de termijnen in paragraaf 4.2.3 “Leveren gegevens kabels en leidingen Rijkswaterstaat” van de Vraagspecificatie Proces te worden geactualiseerd en geleverd, op de situatie in 1GIS

3. Ultimo RWS voor wat betreft niet-kunstwerken:
   Het voorstel voor de decompositie van niet-kunstwerken areaal voor Ultimo RWS af te stemmen op de situatie in het Kerngis Droog en/of de BKN3.
4. Meridian en Ultimo RWS of EAM:
   De decompositie van nieuwe of gewijzigde onderdelen van het Werk dient in Ultimo RWS te zijn opgenomen en/of aangepast, voordat de gegevens van deze nieuwe of aangepaste onderdelen van het Werk in Meridian en Ultimo RWS kunnen worden opgenomen.

2. AutoCAD bestanden en tekeningen

Data 02

De Opdrachtnemer dient de as-built bestanden en tekeningen betreffende de bestaande situatie, voor zover niet reeds verstrekt, op te vragen bij de Opdrachtgever.

Bestaande tekeningen in RTW, die wijzigen door het Werk, dienen omgezet te worden naar NLCS.

Voor alle aangepaste of nieuw gerealiseerde (civiele) Werken dienen de as-built bestanden en tekeningen geometrisch en inhoudelijk een exacte weergave te zijn van het gerealiseerde Werk. Tevens dienen de vervallen en aangepaste as-built bestanden en tekeningen als gevolg van het gerealiseerde Werk binnen 4 weken na ingebruikneming – tenzij anders overeengekomen - aan de Opdrachtgever te worden geleverd.

De Opdrachtnemer dient de technische Documenten te leveren conform eis Data 24 “Beheer Technische Documentatie (Meridian)”.

De Opdrachtnemer dient de as-built bestanden en tekeningen te leveren conform de volgende specificaties:

- Bestandsformaat: inleesbaar inAutoCAD Map 3D 2022;
- Tekeningenformaat: opgebouwd conform NLCS (Nederlandse CAD standaard). Voor nadere informatie zie: http://www.digigo.nu/standaarden/nlcs (NLCS - digiGO;
- Document “Aanvullende eisen tekenwerk Rijkswaterstaat” te downloaden van www.rws.nl/datacontracteisen, tabblad CAD-bestanden en –tekeningen Rijkswaterstaat;
- Document “Tekenvoorschriften object- en lijninfrastructuur gebonden installaties” te downloaden van www.rws.nl/datacontracteisen,tabblad CAD-bestanden en –tekeningen Rijkswaterstaat.

Bestaande tekeningen, die niet conform NLCS zijn opgebouwd dienen, als daar kleine aanpassingen op plaatsvinden, niet te worden omgezet naar NLCS. Bij grotere aanpassingen dient in overleg met de Opdrachtgever te worden bepaald of deze omzetting dient plaats te vinden.

3. 1GIS-bestand

Data 03 1GIS

De Opdrachtnemer dient de gewijzigde terreinsituatie digitaal en geïntegreerd in het beschikbaar gestelde 1GIS-bestand te leveren conform de volgende specificaties:

- Productspecificaties 1GIS.

Deze productspecificaties zijn te downloaden van www.rws.nl/datacontracteisen, tabblad 1GIS.
Alle in het kader van het Werk nieuw aangebrachte en gewijzigde topografie dient te worden ingewonnen. Onder gewijzigde topografie worden ook vlakken en lijnen verstaan, die door vergroten, verkleinen of verleggen van aangrenzende vlakken kleiner of groter zijn geworden.

Data 04 Vervallen

Data 05 Vervallen

Data 06 Vaarwegmeubilair in 1GIS

Niet van toepassing.

4. Werkzaamheden met betrekking tot Kunstwerken en Verkeerskundige Draagconstructies

Data 07 Documenten behorende bij DISK, Inspectietekeningen, Instandhoudingsplan en Beheer- & Onderhoudsplan

Voor de Werkzaamheden rondom kunstwerken en documenten op te nemen in de beheerapplicatie DISK, conform de eisen in deze paragraaf, zijn de volgende documenten van toepassing:

- Handleiding DISK;
- ‘Instructie ten behoeve van vastlegging van overdrachtsgegevens voor Beheer en Onderhoud van Kunstwerken’, nr.182579, v1.3.
- Werkinstructie A17, Snelle naslag inspectietekeningen;
- Werkinstructie A18, Algemene beschrijving inspectietekeningen;
- Werkinstructie A19, Referentieset inspectietekeningen;
- Inspectiekader RWS;
- Productspecificatie Deformatiemeting Kunstwerken.

De Productspecificatie Deformatiemeting Kunstwerken is te downloaden via www.rws.nl/datacontracteisen, tabblad Deformatiemetingen kunstwerken.
De overige documenten en overige relevante informatie voor de Werkzaamheden zijn te vinden op: http://vpr.rws.nl/Algemeen/DISK-Helpdesk/default.aspx. Voor toegang tot deze Internetsite dient een mail

te worden gestuurd naar KCC@rws.nl waarin om toegang voor de vpr DISK-Helpdesk gevraagd wordt.

Data 08 *Autorisatie en certificering uitvoeringsinstantie*
Alle Werkzaamheden, die de Opdrachtnemer in het kader van het Werk in het beheerapplicatie DISK verricht, dienen te gebeuren door een daartoe door Rijkswaterstaat geautoriseerde en gecertificeerde gebruiker.
Voor autorisatie en certificering dient een mail te worden gestuurd naar KCC@rws.nl waarin om autorisatie en certificering voor DISK wordt gevraagd.

Het uitvoeren van de instandhoudingsinspectie en het opstellen van een rapport van de instandhoudingsinspectie en instandhoudingsplan dient te worden uitgevoerd door een voor DISK geautoriseerde en gecertificeerde inspecteur.

Data 09 *Aanpassingen decompositie kunstwerk in DISK*
Indien het noodzakelijk is om de in DISK aanwezige decompositie van het kunstwerk aan te passen, dan dient de Opdrachtnemer hierover eerst te overleggen met en toestemming te krijgen van de Opdrachtgever.

Data 10 *Beheerobjectcode*
Niet van toepassing.
Deze beheerobjectcode dient in DISK en 1GIS te worden verwerkt conform de betreffende specificaties.

Data 11 *Toetsen, actualiseren en leveren inspectietekeningen*
Niet van toepassing.

Data 12 *Deformatiemetingen Kunstwerken*
Niet van toepassing.

Data 13 *Instandhoudingsinspectie*
Niet van toepassing.

Data 14 *Instandhoudingplan van kunstwerken*
Niet van toepassing.*Data 15 Beheer- & Onderhoudsplan van kunstwerken*
Niet van toepassing.

Data 16 *Verkeerskundige draagconstructies (VDC)*
Niet van toepassing.

5. *Doorrijprofielen*

Data 17 Indien Werkzaamheden aan rijkswegen zijn verricht, dan dient de Opdrachtnemer voor de (vervroegde) ingebruikneming van het Werk, dan wel delen daarvan, aan de Opdrachtgever de doorrijprofielen (doorrijhoogten en doorrijbreedten) van de objecten die zich geheel of gedeeltelijk boven de rijksweg bevinden, te leveren conform de “Productspecificaties Doorrijprofielmeting kunstwerken en portalen” te downloaden van www.rws.nl/datacontracteisen, tabblad DoorrijprofielenFout! De hyperlinkverwijzing is ongeldig..

Tevens dient de Opdrachtnemer (tijdelijke) beperkingen van doorrijprofielen twee maanden vóór start van de voorgenomen beperking ter kennis te brengen van de Opdrachtgever, door middel van een duidelijke digitale foto (jpeg) van het object of schets indien het object nog moet worden geplaatst, waarop de doorrijhoogte, doorrijbreedte en locatie zijn weergegeven.

6. *Kunstwerkgegevens t.b.v. ontheffingverlening exceptioneel zwaar transport*

Data 18 Niet van toepassing.

7. *Garantie*

Data 19 De Opdrachtnemer dient de nieuwe of gewijzigde garanties op te nemen in een Excellijst. De Opdrachtnemer dient de garantiegegevens te leveren aan de Opdrachtgever voor de start van de garantieperiode zoals bedoeld in annex XV “Garanties”, conform de volgende specificaties:
1. de door de Opdrachtnemer in te vullen Excellijst;
2. toelichting op het invoeren van informatie over garanties;
3. processchema invoeren nieuwe garanties.

Deze specificaties zijn te downloaden van https://rws.nl/datacontracteisen, tabblad Garanties.

8. *Nationaal Wegenbestand (NWB) en Weggegevens Hoofdwegennet (WEGGEG)*

Data 20 Niet van toepassing.

9. *Elektronische Navigatiekaart (ENC)*

Data 21 Niet van toepassing.

10. *Beheer en onderhoud managementgegevens*

Data 22 *Decompositie van infrastructuur*
Met inachtneming van eis OP300 dient de Opdrachtnemer een voorstel voor de nieuwe of gewijzigde decompositie in de beheerapplicaties van het Beheer Management Systeem aan te leveren en daarbij gebruik te maken van de decompositie conform de NEN 2767 Conditiemeting en de aanvullende Rijkswaterstaat specificatie ‘Decompositiekader NEN 2767 RWS’. Dit laatste document is te downloaden van www.rws.nl/datacontracteisen, tabblad “Ultimo”.

De Opdrachtnemer dient er rekening mee te houden dat pas na verwerking door de Opdrachtgever van de nieuwe of gewijzigde decompositie, de bijbehorende gegevens door de Opdrachtnemer in de beheerapplicaties van het Beheer Management Systeem kunnen worden opgenomen. De Opdrachtgever heeft 2 weken nodig om de nieuwe of gewijzigde decompositiegegevens te verwerken.

De Opdrachtnemer mag in overleg met de Opdrachtgever voorstellen voor de nieuwe of gewijzigde decompositie vooruitlopend op het af- of opleverdossier in delen leveren.

De Opdrachtnemer dient er rekening mee te houden dat de NEN-2767 en de aanvullende Rijkswaterstaat specificatie veranderen, waardoor mogelijk de decompositie in de beheerapplicaties van het Beheer Management Systeem wijzigt.

Data 23 Ultimo RWS

De Opdrachtnemer dient in de beheerapplicatie Ultimo RWS de kwalitatieve gegevens te actualiseren conform de feitelijke toestand van het Werk en de kwantitatieve gegevens van het Werk, die door de Werkzaamheden wijzigen, te actualiseren.

Het actualiseren van de gegevens in het Ultimo RWS dient uiterlijk bij oplevering gereed te zijn, tenzij in de Vraagspecificatie een ander moment is aangegeven.

Het actualiseren van de gegevens dient te gebeuren conform de volgende specificatie, waarbij nadrukkelijk wordt aangegeven, dat alleen de decompositie zelf via export-import kan worden verwerkt in het Ultimo RWS:

- Productspecificatie Ultimo;
- Invulinstructie Ultimo.

Deze documenten zijn te downloaden van www.rws.nl/datacontracteisen, tabblad “Assetmanagementsysteem (Ultimo)”.

Data 24 Beheer Technische Documentatie (Meridian)

De Opdrachtnemer dient na de betreffende Werkzaamheden de bestaande technische documenten die in de beheerapplicatie Meridian aanwezig zijn, te actualiseren dan wel nieuwe technische documenten te maken en deze te leveren aan de Opdrachtgever ten behoeve van opname in Meridian. Tevens dient de Opdrachtnemer de meta-data van deze geactualiseerde en nieuwe technische documenten te leveren aan de Opdrachtgever. De Opdrachtnemer dient aan te geven welke bestaande technische documenten vervallen inclusief de vervaldatum en vervalreden.

De Opdrachtnemer dient ten behoeve van het actualiseren van bestaande technische documenten deze op te vragen bij de Opdrachtgever. De Opdrachtnemer dient ten behoeve van nieuwe technische documenten een documentnummer aan te vragen bij de Opdrachtgever.

Het opvragen, actualiseren en leveren dient te gebeuren conform de volgende specificatie:

- Eisen voor Datamodel Technische Documentatie.

Deze specificatie is te downloaden van www.rws.nl/datacontracteisen, tabblad “Beheer Technische Documentatie”.

11. IV-Netwerk

Data 25 *IV-Netwerk Documentatieset Eisen en Richtlijnen*

Indien Werkzaamheden aan het IV-netwerk zijn verricht, dan dient de Opdrachtnemer alle benodigde gegevens in het kader van het Werk ten behoeve van het 1GIS te leveren conform Data 03 van deze bijlage en conform de volgende specificaties:

- IV-Netwerk Documentatieset Eisen en Richtlijnen

Deze specificaties “IV-Netwerk Documentatieset Eisen en Richtlijnen” zijn te downloaden van www.rws.nl/datacontracteisen, tabblad IV-Netwerk Documentatieset Eisen en Richtlijnen.

Bijlage N Invulinstructie format LV BRO

Deze bijlage bevat een invulinstructie ten aanzien van het format van de landelijke voorziening basisregistratie ondergrond (LV BRO).

Deze invulinstructie bevat de zaken die altijd op een bepaalde wijze moeten worden ingevuld; de invulinstructie kan door de publicatie van nieuwe of gewijzigde BRO-catalogi wijzigen. De invulinstructie moet voorafgaand aan de opdrachtverlening door de Opdrachtgever worden aangevuld met zaken die specifiek samenhangen met de te verlenen opdracht.

Attribuut	Invulinstructie
Bronhouder	27364178 *(ALTIJD)* *Toelichting: het KvK nummer van Rijkswaterstaat ter identificatie als bestuursorgaan*
Object-ID	<Vul WBS element in> *Toelichting: het 'WBS-element niveau 2' uit SAP invullen ten behoeve van de Opdrachtnemer. Met behulp van dit nummer kan RWS ook op lange termijn de interne opdrachtgever en opdrachtnemer achterhalen; tevens is het mogelijk om alle onderliggende elementen te vinden. Een WBS-element is altijd als volgt opgebouwd: een letter, een punt, acht cijfers, een punt, vier cijfers. Dus bijvoorbeeld P.00000183.0002.* *Niet bekend met het nummer? Vraag het de betrokken adviseur bedrijfsvoering.*
Data-leverancier	Het KvK nummer van de hoofdopdrachtnemer. *(ALTIJD)* *Toelichting: dit is een invulinstructie voor de Opdrachtnemer*
Kwaliteits-regime	IMBRO *(ALTIJD)*
Kader aanlevering	<Vul het inwinkader in> *(PROJECTSPECIFIEK)* *Toelichting: Rijkswaterstaat kiest in welk kader de onderzoeken zijn uitgevoerd; keuze uit:* *a. Opdracht publieke taakuitvoering,* *b. Rechtsgrond Waterwet.*
Kader inwinning	Invullen door diegene die de opdracht verstrekt tot het onderzoek naar de ondergrond. Keuze uit 7 opties. *Toelichting: indien de uitvoerder van het onderzoek naar de ondergrond niet zelf verantwoordelijk is voor het bepalen welke onderzoeken naar de ondergrond nodig zijn in het licht van de werkzaamheden, kan het zo zijn dat de uitvoerder niet weet wat het doel is van het onderzoek dat hij uitvoert. Dit dient dan te worden voorgeschreven. Keuze uit onderzoek met als doel:* *1. eigenschappen van de ondergrond rondom waterkeringen te verkennen,* *2. eigenschappen van de ondergrond rondom bouwwerken en constructies te verkennen,* *3. eigenschappen van de ondergrond rondom wegen, spoorwegen, fiets- en voetpaden te verkennen,* *4. eigenschappen van de ondergrond in waterwegen te verkennen,*

	5. eigenschappen van de ondergrond te verkennen met een milieu hygiënische (natuurlijke of niet natuurlijke) achtergrond, *6. om veranderingen in de ondergrond t.g.v. werkzaamheden te verkennen. Betreffend onderzoek heeft veelal een lokaal karakter. Vaak is voorafgaand aan de werkzaamheden al in een ander kader informatie ingewonnen om de verandering te kunnen beoordelen,* 7. *Onderzoek met als doel een vergunning te onderbouwen.*
Eigenaar	Invullen door diegene die opdracht geeft tot het meten van grondwater met behulp van een grondwater-monitoringput die niet in eigendom is van Rijkswaterstaat. *Toelichting: het kan bijvoorbeeld gaan om het tijdelijk gebruiken van een put van een ander, maar ook op grond van een burger (laten) aanleggen van een put.* *De eigenaar moet gespecificeerd worden o.b.v. KVK-nummer. In het geval dat Rijkswaterstaat eigenaar is, moet KVK-nummer 27364178 worden ingevuld.*
Onder-houdende instantie	<Vul het KvK-nummer in> *(PROJECTSPECIFIEK)* Invullen door Rijkswaterstaat in geval dat grondwater-monitoringputten zullen worden aangelegd door de Opdrachtnemer maar het onderhoud door een ander wordt uitgevoerd, en die Opdrachtnemer geen kennis heeft van onderhoudende instantie(s) die hiervoor zijn gecontracteerd. *Toelichting: de onderhoudende instantie moet gespecificeerd worden o.b.v. KvK-nummer.*
Initiële functie	Invullen door diegene die opdracht geeft tot het aanleggen van een grondwatermonitoringput. Keuze uit 5 opties: *Toelichting: keuze uit:* *1. Brandput,* *2. Monitoring grondwaterstand,* *3. Monitoring grondwatersamenstelling,* *4. Monitoring grondwaterstand en grondwatersamenstelling,* *5. Grondwateronttrekking.*

Bijlage O Melding inzet Zelfstandige Hulppersoon

Het Uniform Europees Aanbestedingsdocument wordt als apart document als een interactief pdf-formulier ter beschikking gesteld via TenderNed.

Bijlage P Aanvullende eigen verklaring inzake Russische partijen

Naam en adres van de onderneming:
……

Inschrijvingsnummer Kamer van Koophandel (inschrijvingsnummer van het handelsregister of een overeenkomstig register van het land van vestiging van de onderneming):

KvK-nummer: ……

Vestigingsnummer: ……

Contactpersoon van de onderneming (naam, email, telefoon):
……

VRAGEN TEN AANZIEN VAN HET EUROPESE VERBOD OM OVERHEIDSOPDRACHTEN TE GUNNEN AAN RUSSISCHE PARTIJEN

1. Wordt de onderneming gedreven voor rekening van een Russisch onderdaan of een in Rusland gevestigde natuurlijk persoon, rechtspersoon, entiteit of lichaam?

Ja / nee (doorhalen wat niet van toepassing is)

2. Is de onderneming een rechtspersoon, entiteit of lichaam waarvan de eigendomsrechten voor meer dan 50% direct of indirect in handen zijn van een entiteit als bedoeld bij vraag 1?

Ja / nee (doorhalen wat niet van toepassing is)

3. Handelt de onderneming namens of op aanwijzing van een entiteit als bedoeld bij vraag 1 of 2?

Ja / nee (doorhalen wat niet van toepassing is)

4. Maakt de onderneming gebruik van een onderaannemer, leverancier of andere entiteit, waarbij de prestatie van deze betrokkene meer dan 10% van de waarde van de onderhavige opdracht vertegenwoordigt terwijl tevens voor deze betrokkene één van bovenstaande vragen 1 t/m 3 met “ja” beantwoord moet worden?

Ja / nee (doorhalen wat niet van toepassing is)

VERKLARING

Ondergetekende verklaart dat:

- de in deze vragenlijst opgenomen vragen volledig en naar waarheid zijn beantwoord;
- hij deze ingevulde vragenlijst onvoorwaardelijk en zonder enig voorbehoud heeft ondertekend; hij zich ervan bewust is dat het verstrekken van onjuiste of onvolledige informatie door de aanbestedende dienst kan worden aangemerkt als een valse verklaring en dat dit kan leiden tot een onvoorwaardelijke uitsluiting van het verrichten van Werkzaamheden in het kader van deze opdracht;
- er in de tekst van deze vragenlijst geen wijzigingen zijn aangebracht;
- deze vragenlijst is ondertekend door een daartoe, blijkens het handelsregister, dan wel een overeenkomstig register van het land van vestiging van de onderneming, vertegenwoordigingsbevoegde,

Ondertekening

Datum:

Plaats:

Handtekening:

Bijlage Q Producten en Diensten Catalogus Netwerken CIV

Rijkswaterstaat
Ministerie van Infrastructuur en Waterstaat

Bijlage Q Dienstencatalogus Netwerken CIV

Bijlage bij Vraagspecificatie Proces

D&C Vervanging Verlichting Schipholtunnel
Zaaknummer: 31212908

RWS Bedrijfsvertrouwelijk

Rijkswaterstaat
Ministerie van Infrastructuur en Waterstaat

Producten en Diensten Catalogus Netwerken CIV

Ten behoeve van RWS Infra

Uitgegeven door:

Service Portfolio Manager	Conclusion Operationele Service Integrator (OPSI)
Service Portfolio Manager	RWS CIV IRN INFRA NETWERKEN

Datum:	01-05-2025
Status:	Definitief
Classificatie:	Conclusion Vertrouwelijk, RWS Bedrijfsinformatie
Versie: 21.0	

Contents

Documentbeheer **3**
Documentversies 3

Inleiding **4**
Relatie met andere documenten 4
Opbouw 4
Dienstverlening RWS CIV IRN Infra Netwerken 4
Contact over deze Diensten Catalogus 7

PDC deel 1: Diensten RWS CIV IRN Infra Netwerken **8**

Diensten RWS CIV IRN Infra Netwerken **8**
Inleiding 8
Categorie Backbone (BB), Core, Centrale Voorzieningen (CV) 8
Categorie VPN 17
Categorie LAN aansluiting 25
Categorie Overig 28

PDC deel 2: Netwerkdiensten CIV Afnemer **33**

Netwerkdiensten CIV Afnemer **34**
Inleiding 34
Categorie VPN 34
Categorie VPN aansluiting 38
Categorie LAN aansluiting 53
Categorie Eindsystemen 64
Categorie Overig 73
Beheren IT-netwerkdiensten (Specials) 78
Verbindingen Lichteiland Goeree – Europlatform 78
CCM aansluiting 78

Totaal overzicht SLA Matrix **79**

Bijlage A Afkortingen en Begrippen **80**

Bijlage B Overzicht tabellen **84**

Bijlage C Overzicht figuren **85**

Documentbeheer

Documentversies

Eigenaar	Datum	Versie	Samenvatting van de wijziging	Status
KPN DO RWS		1 tm 19	Diversen, zie versie 20 voor details	
KPN DO RWS	31-03-2025	20	1. Loggingdienst: verwachte realisatie van de techniek, om zodoende herstelgaranties op de dienst te kunnen geven, is aangepast naar 2026. 2. Beheerverbindingen LEG-EPL: Servicelevel aangepast naar E8. 3. Categorie Special: Noodknopbediening Sijtwendetunnel uit dienstenportfolio verwijderd. 4. Toevoegen Hub Spoke als bestelbare optie op draadloze VPN aansluiting	Definitief
Conclusion OPSI	01-05-2025	21	1. Nieuw bronbestand met overzicht leveringen (eigenaar RWS ESI) verwerkt 2. Structuur document herzien als onderdeel van de Transitie naar nieuwe leverancier 3. Overgezet naar RWS huisstijl Splitsing in drie documenten: 1. Geconsolideerde technische service catalogus BOSI 2. PDC versie 21 tbv RWS infra 3. PDC versie 21 tbv externe afnemers (alleen deel 2)	Definitief

Inleiding

De Dienstencatalogus Netwerken-CIV beschrijft de IT-netwerkdiensten die beschikbaar zijn voor RWS en door RWS gemandateerde Afnemers, geïntegreerd door OPSI conform het BOSI-contract.

Doel van deze catalogus is het bieden van een overzicht van de diensten die RWS CIV IRN Infra Netwerken op netwerkgebied afneemt van de Service Providers en welke RWS CIV IRN Infra Netwerken biedt aan haar afnemers.

Relatie met andere documenten

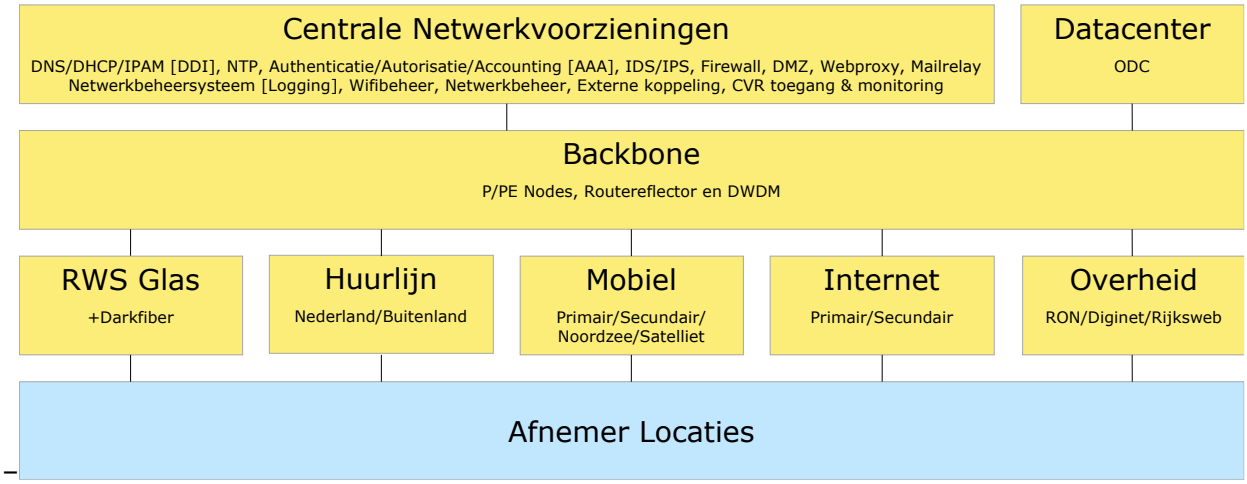
Document	Eigenaar	Versie	datum
Afnemer Netwerkdiensten Wizard	ESI	1.0	01-05-2025
Technische Service Tree	OPSI	1.0	01-05-2025

Opbouw
Deze catalogus bestaat uit de volgende onderdelen:

- Algemeen
  - Toelichting op de scope van de dienstverlening;
  - Ondersteuning via de Service Desk;
  - Service Providers – en beschrijving op hoofdlijnen van hun dienstverlening
- PDC deel 1: Netwerkdiensten RWS CIV IRN Infra Netwerken
  - Een beschrijving van de uitsluitend door/via RWS CIV IRN Infra Netwerken te bestellen diensten in de categorie Backbone, VPN, VPN Aansluiting, LAN Aansluiting, Eindsysteem en Special/Overig.
- PDC deel 2: Netwerkdiensten Klant
  - Een beschrijving van de door interne en externe afnemers te bestellen diensten in de categorie VPN, VPN Aansluiting, LAN Aansluiting, Eindsysteem en Overig.

Dienstverlening RWS CIV IRN Infra Netwerken
Algemeen
Rijkswaterstaat Centrale Informatievoorziening (CIV) zorgt voor de ontwikkeling en beschikbaarheid van informatie binnen Rijkswaterstaat. CIV zorgt voor industriële automatisering bij bruggen, tunnels, rijkswegen en andere objecten. Daarnaast verzorgt CIV de kantoorautomatisering. RWS CIV IRN Infra Netwerken draagt binnen RWS CIV zorg voor de netwerkinfrastructuur en bijbehorende dienstverlening.

Scope
RWS CIV IRN Infra Netwerken is verantwoordelijk voor het beheer, project- en contractmanagement van haar netwerkomgeving. De uitvoering hiervan is belegd bij de outsourcingspartner Conclusion Quanza.



Figuur 1 Scope IT-netwerkdiensten

De netwerkdienstverlening beslaat de volgende domeinen:

- RWS netwerk;
- LAN voor Kantoorautomatisering (KA);
- Object Access Netwerken:
    - Netwerken die worden gebruikt om objecten, binnen Rijkswaterstaat ook wel kunstwerken genoemd, maar ook systemen langs weg- en waterwegen, te ontsluiten;
- De WAN verbindingen naar Locaties (kantoren en rekencentra), wegkantsystemen, verkeerscentrales, objecten zoals bruggen, sluizen en tunnels en losse huurlijnen.
- Koppelingen met externe netwerken (internet, mobiel, de Haagse Ring, RON2.0 e.a.);
- Functieherstel glasvezelnetwerk:
    - Herstellen van verstoringen op RWS glasvezels;
    - Glasvezelbeheer (o.a. vezelbezetting en uitgifte van vezels).

Uitvoeren Operationele ITIL-diensten

De uitvoering van de verschillende ITIL-diensten is beschreven in het Ketenhandboek IT-netwerkdiensten. Hierin staan alle generieke afspraken binnen het ecosysteem van de IT-netwerkdiensten beschreven. Daarnaast bestuurt OPSI de verschillende service providers in de keten ondersteund door specifieke afspraken die zijn beschreven in Operational Level Agreements (OLA's). In dit hoofdstuk worden de belangrijkste afspraken, die relevant zijn voor de interne en externe afnemers van de dienstverlening, samengevat.

Service Control Center (SCC)

Ten eerste verwerkt de OPSI SCC, als centrale spil, alle vragen, orders en storingsmeldingen van de afnemers van de Rijkswaterstaat organisatie. Hierbij worden via een gecontroleerd proces de diverse toeleveranciers en derde partijen aangestuurd. Ten tweede verricht de SCC alle noodzakelijke registraties ten behoeve van terugkoppeling, rapportage, bijsturing en facturering.

Het SCC vormt een integraal onderdeel van de OPSI dienstverlening en omvat de

volgende functies:

- Helpdesk: Ondersteunen van de medewerkers/afnemers van Rijkswaterstaat bij vragen over afgenomen diensten;
- Orderdesk: Ingang waar geautoriseerde personen opdrachten en eenmalige diensten (Install, Move, Add en Change (IMAC's)) indienen;
- Melddesk: Voor het melden van storingen, incidenten en klachten.

Het SCC beantwoordt de vragen van Rijkswaterstaat. Als het SCC de vragen niet kan beantwoorden wordt contact gezocht met de achterliggende supportgroepen of derde contractpartijen om tot een antwoord te komen. Hierover zijn afspraken gemaakt met de achterliggende partijen.
Het SCC is 24x7 zowel telefonisch als per e-mail bereikbaar:

- Incidenten kunnen 24x7 telefonisch gemeld worden en worden conform geldende SLA afspraak afgerond;
- De afhandeling van orders zal plaatsvinden tijdens kantooruren;
- Informatievragen kunnen 24x7 per e-mail gesteld worden. Tijdens kantooruren kunnen deze vragen ook telefonisch gesteld worden. De afhandeling van informatievragen vindt plaats tijdens kantooruren.

Service Providers

CCMKO	Contact Center Missie Kritieke Ondersteuning
KA Service Desk	Service Desk KA-omgeving, on site support op grote kantoorlocaties
OPSI	Operationele integratie van de IT-netwerkdiensten
IB	Integraal Beheer van het RWS netwerk
O&A	Onderhouden en Aanpassen van IT-netwerkdiensten
SPIE	Field Services – diverse werkzaamheden op locatie ten behoeve van Beheer, Onderhoud en Aanpassen; voorraadbeheer netwerk hardware
Odido	Vaste data huurlijnen, Mobiele SIM-kaarten (backup)
Vodafone	Mobiele SIM-kaarten (primair)
ProximusNXT	Bestelling en levering Cisco Hardware

Bestellingen

Deze catalogus beschrijft de standaard bestelbare diensten van CIV IRN Infra Netwerken. Afnemers kunnen zonder tussenkomst van CIV IRN Infra Netwerken een standaard levering aanvragen. Een aantal standaard bestelbare items zijn geclassificeerd als "tactische leveringen", hiervoor dient CIV IRN Infra Netwerken akkoord te geven. Levervragen die (nog) niet met de standaard Product en Diensten Catalogus kunnen worden ingevuld worden On hold geplaatst tot een ontwikkeling van een standaard bestelbaar item door CIV IRN Infra Netwerken is afgerond. Indien levering vooruitlopend op ontwikkeling noodzakelijk is, kan met de PDC Uitzonderingen Procedure toestemming gevraagd worden om op basis van een PDC Exceptie de levering op te starten parallel aan een ontwikkeltraject.

Standaard leveringen
De standaard leverbare items uit deze catalogus zijn bestelbaar via de RWS TOPdesk SelfServicePortal via Startpagina > PDC IRN INFRA > Netwerk. Hierbij wordt onderscheid gemaakt tussen een tweetal type leveringen:

- Mutaties: Geautomatiseerd leveren van één of meerdere bestelbare items uit de PDC zonder coördinatie;
- Meervoudige (Gecoördineerde) PDC project leveringen: Leveren van één of meerdere bestelbare items uit de PDC onder besturing van een PDC Coördinator o.b.v. een prijsopgaaf

In geval van twijfel over de te bestellen standaard items kan middels de "Hulp bij mijn PDC bestelling"-tegel in TOPdesk een verzoek tot ondersteuning bij het samenstellen van de juiste bestelling worden ingediend.

Tactische leveringen
Er zijn ook een aantal tactische aanvragen gedefinieerd. Voor de levering hiervan dient contact opgenomen te worden met de Customer Relationship Manager van RWS CIV IRN Infra Netwerken. De Relatie Manager bepaalt of de aanvraag al dan niet in behandeling wordt genomen.

Verstoringen
Indien een verstoring van een IT-netwerkdienst optreedt, dient contact opgenomen te worden met de eerstelijns service desk. Vanuit een kantooromgeving is dat de KA Service desk, voor verstoringen 'in het veld' wordt contact opgenomen met het CCMKO. Indien zij constateren dat het een storing van de IT-netwerkdiensten betreft dan wordt het SCC van de OPSI aangestuurd.

Ten behoeve van het oplossen van verstoringen stuurt de OPSI, afhankelijk van het type verstoring, één of meerdere service providers aan. Als er assistentie op locatie nodig is zijn er twee opties:

- On site support door KA Service Desk, voor het initieel nadere informatie verzamelen over de verstoring;
- Field Services door SPIE voor alle andere benodigde activiteiten op locatie.

Contact over deze Diensten Catalogus
Voor vragen omtrent de standaard dienstverlening en dienstontwikkelingen kan contact opgenomen worden met de Customer Relationship Manager RWS CIV IRN Infra Netwerken, de Demand Manager RWS CIV IRN Infra Netwerken of hun Service Management collega's. De Service Delivery Manager OPSI is verantwoordelijk voor deze Diensten Catalgus.

PDC deel 1: Diensten RWS CIV IRN Infra Netwerken

Diensten RWS CIV IRN Infra Netwerken

Inleiding

De Netwerkdiensten RWS CIV IRN Infra Netwerken zijn uitsluitend te bestellen door medewerkers van CIV IRN Infra Netwerken. Bij vragen over deze diensten kan contact opgenomen worden met Service Management of de Customer Relationship/Demand Manager. De netwerkdiensten ten behoeve van afnemers zijn beschreven in deel 2 van deze catalogus: "Netwerkdiensten CIV Afnemer".

Categorie Backbone (BB), Core, Centrale Voorzieningen (CV)

De categorie **BB Core CV** omvat de centrale netwerkdiensten welke betrekking hebben op de backbone van het RWS netwerk, zoals voorzieningen om de veiligheid van het netwerk te garanderen. De backbone van het RWS CIV IRN Infra netwerk is de centrale netwerkinfrastructuur waarlangs het gegevensverkeer van de op de backbone aangesloten netwerken loopt.
De categorie Centrale Voorzieningen betreft de diensten en centrale componenten welke benodigd zijn om klantdiensten te kunnen leveren zoals DNS, IPS IDS, DWDM, toe Toegang en omgevingsmonitoring en Glasvezelbeheer.

Beheren Backbone diensten

RWS onderkent de volgende Backbone diensten:

1. Domain Name Services (DNS)
2. Intrusion Detection Services (IDS)
3. Intrusion Prevention Services (IPS)
4. DWDM
5. CVR Toegang en omgevingsmonitoring
6. Glasvezelbeheer

Quanza IB voert het beheer uit op een subset van deze Backbone diensten conform onderstaande SLA.

Dienstenmatrix Backbone								
Diensten	Beschikbaarheid				Storingshersteltijd in 95% van de gevallen			
	99.5%	99.9%	99.95%	99.999%	Service Window Kantoortijden		Service Window 24/7	
	Onbeschikbaarheid per jaar							
	ca 1d20u	ca 8u45m	ca 4u28m	ca 5m15s	8 uur	4 uur	8 uur	4 uur
DNS			v					v
IDS	v							v
IPS		v						v

Tabel 1 Beschikbaarheid Backbone diensten

Het backbone gedeelte van de dienst 'CVR toegang en monitoring' valt buiten scope van de dienstverlening; wel wordt voor deze dienst tweedelijnsondersteuning uitgevoerd.

Domain Name Services (DNS) CV
De centrale dienst DNS CV voorziet in het abonnement voor levering van "name services" aan alle eindsystemen die zijn aangesloten op het RWS netwerk op basis van het DNS protocol. Hierbij wordt onderscheid gemaakt tussen een centraal DNS CV abonnement en een aanvullend abonnement per appliance (toepassing).
De dienst voorziet in zowel hosting als resolving van domeinnamen. Daarnaast verzorgt DNS CV samen met Domain Host Configuration Protocol (DHCP) CV een gecentraliseerde IP Address Management (IPAM) functie om het beheer van DNS zones en DHCP scopes en opties efficiënt en effectief uit te kunnen voeren.
De dienst maakt gebruik van High Available DNS, een centraal management systeem en gecentraliseerde logging en levert de volgende functies:

- Centrale DNS dienst ten behoeve van interne- en externe resolving en hosting van DNS domeinen;
- Centraal beheren van gedecentraliseerde DNS resolvers in de RWS verkeerscentrales (POP locaties);
- DNS Forwarding, bedoeld om DNS query's te forwarden voor externe DNS namen op externe DNS servers, buiten het RWS domein;
- Zoveel mogelijk generieke DNS configuratie, waarbij het mogelijk is per zone te kiezen voor voorkeuren maar centraal beheer mogelijk is; Inherent High Available (één virtual DNS IP nummer per cluster);
- Mogelijkheid tot opzetten van een terminal connectie met een seriële poort en een console verbinding;
- Geschikt voor IPv6, geïmplementeerd op basis van Iv4;
- Logging van beheerhandelingen, DNS requests en failures wordt verstuurd naar centrale syslog servers.

Naast de centrale DNS dienstverlening is het middels de DDI (DNS DHCP IPAM) dienst mogelijk per VPN verschillende DNS en DHCP opties in te stellen en gedelegeerd beheer toe te passen in DNS zones en DHCP scopes. De dienst DDI is beschreven in de Categorie VPN.

IDS / IPS
IDS/IPS biedt een centraal beheerd en bestuurd Intrusion Detection System (IDS) voor verkeer tussen VPN's en voor verkeer van en naar de centrale voorzieningen, en Intrusion Prevention System(IPS) voor al het verkeer van en naar het internet. Doel van deze dienst is om gericht applicatie-, systeem- en netwerkbedreigingen te detecteren en risico's hierop te mitigeren.

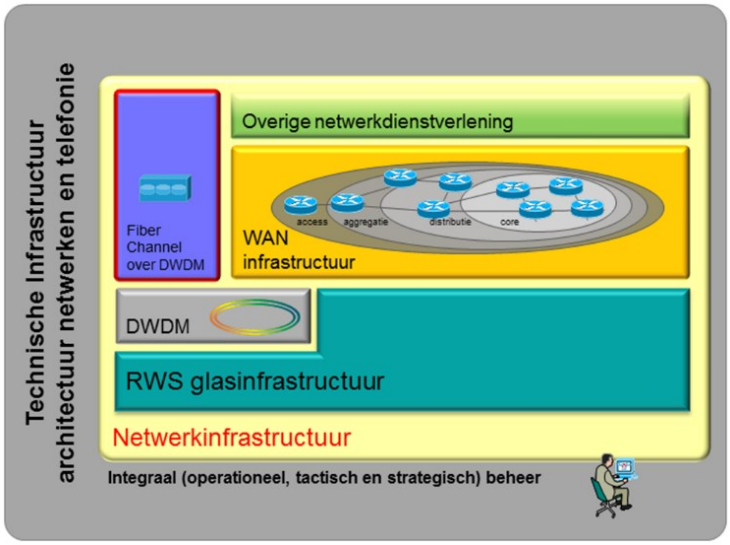
IDS/IPS monitort het RWS netwerk en de centrale netwerkdiensten om ongewone/verdachte verkeersstromen, patronen en gebeurtenissen te detecteren en rapporteert deze via een dashboard.

Daarnaast evalueert en rapporteert IDS/IPS verdachte verkeersstromen naar of vanuit eindstations bekend als 'malware', 'virale software', 'trojans', 'spyware', portscans en andere afwijkende datapatronen. IPS blokkeert verdacht verkeer en acteert daarmee als application layered firewall voor al het verkeer van en naar het internet. IPS wordt ook ingezet om intern verkeer vanuit het RWS netwerk richting andere netwerken te filteren en fungeert als centraal punt in het netwerk waar ongewenste verkeersstromen kunnen worden geblokkeerd. IDS/IPS wordt toegepast om te inspecteren en rapporteren op inter- VPN verkeer van alle RWS VPN's, in- en outbound verkeer met Externe koppeling, DMZ en de centrale voorzieningen en verkeer van en naar beheerinterfaces van beheerde apparatuur. Daarnaast wordt IDS/IPS toegepast om te inspecteren en te acteren op in- en outbound internet verkeer voor het RWS netwerk.
Daarnaast biedt IDS/IPS voor haar beheerders een platform om op gebruikersvriendelijke wijze het systeem te configureren, te laden met 'policies' en 'rules' als ook om gebeurtenissen te categoriseren, te rapporteren en in te richten door middel van 'dashboards' voor het verkrijgen van overzicht en inzicht.

IDS/IPS moet altijd bekend zijn met de te monitoren netwerken (set van IP adressen). Om onterechte meldingen (false positives) te beperken worden nieuwe door SP-IB uitgegeven netwerken automatisch toegevoegd aan de dienst bij aanvraag of wijziging van een VPN. Hiertoe beschikt het IDS-IPS over een profileringsfunctionaliteit waarin de verschillende netwerken opgenomen worden. Netwerken worden toegewezen middels een standaard policy maar het is ook mogelijk een specifieke policy in te richten voor specifieke netwerken.

De logging van de IDS sensoren en IPS worden verstuurd naar het centrale managementsysteem: De Firepower Management Center (FMC). Op basis van de ontvangen informatie kunnen uit het Defence Center verschillende rapportages worden opgevraagd.

FCoDWDM
De dienst Fibre Channel over Dense Wavelength Division Multiplexing (FCoDWDM) wordt geleverd over glasvezelverbindingen in de RWS infrastructuur. DWDM bestaat uit een point-to-point verbinding tussen bestaande datacenters en onder bepaalde voorwaarden naar nieuwe locaties.
Doormiddel van Fibre Channel over DWDM kan het glas efficiënter gebruikt worden. Het Fibre Channel protocol wordt gebruikt om verschillende locaties te verbinden ten behoeve van data storage synchronisatie.



Figuur 2 DWDM in het netwerk

De dienst DWDM wordt gerealiseerd door twee onafhankelijke verbindingen (unprotected pair) die over gescheiden optische paden en verschillende DWDM-nodes geleverd worden en die beschermd worden door de aangesloten apparatuur. Hiermee kan een hoge beschikbaarheid worden gerealiseerd.

De point-to-point verbinding tussen twee locaties moet voldoen aan de volgende voorwaarden:

- Standaard uitsluitend leverbaar tussen de locaties Datacenter AM2 en Datacenter AM3 (AM1.3 en AM4 zitten respectievelijk achter AM2 en AM4).
- Uitbreiding naar andere locaties mogelijk indien wordt voldaan aan de volgende voorwaarden:
    - Glas beschikbaar over 2 gescheiden routes;
    - Mogelijkheid tot plaatsen DWDM-apparatuur rekening houdend met de latency beperkingen (= afstand) van het Fibre Channelprotocol.
    - Meerdere verbindingen tussen 2 locaties is mogelijk, mits er voldoende ruimte is op de glasvezels.
    - Fibre Channel kan niet omgaan met een verandering van latency door het automatisch omschakelen naar een ander glastraject. Er worden geen *beveiligde* verbindingen aangeboden.
    - Om toch een hoge beschikbaarheid te kunnen bieden, worden Fibre Channel verbindingen altijd per paar geleverd. Een "paar" bestaat uit 2 onafhankelijke verbindingen, die over verschillende glastrajecten worden gerealiseerd.
    - De omschakeling van het primaire pad naar het secundaire pad wordt door de aangesloten Fibre Channel apparatuur (zoals bijvoorbeeld SAN-switches) geregeld.

Over DWDM kunnen de volgende koppelvlakken technisch gerealiseerd worden:

- 8Gbps Fibre Channel

De koppeling wordt standaard gemaakt met Multi-mode fiber (850nm) via een LC Connector.

CVR toegang en omgevingsmonitoring
RWS CIV IRN Infra Netwerken maakt voor de Centrale VIC-ruimtes (CVR-en) gebruik van een aantal applicaties ten behoeve van toegangsbeveiliging en omgevingsmonitoring. Middels deze netwerkdienst CVR toegang en omgevingsmonitoring wordt tweedelijns support bij incidentafhandeling van het CVR Toegang en Omgevingsmonitoringsysteem geborgd.

Scope van de dienstverlening
De eerstelijns ondersteuning en dagelijkse monitoring voor deze dienst worden verzorgd door RWS MKO. MKO kan gebruikersvragen en verstoringen via de OPSI aanmelden bij de Servicedesk van SPIE. Na het aanmaken van een melding kan RWS MKO optioneel tijdens kantoortijden telefonisch contact opnemen met SPIE om de melding te bevestigen of te bespreken. De eerste incidentanalyse en kwalificatie van een melding worden door RWS MKO uitgevoerd om OPSI/SPIE te voorzien van de juiste informatie: omdat de systeemcomponenten geen onderdeel uitmaken van de CMDB dient RWS MKO expliciet te vermelden op welk onderdeel de verstoring betrekking heeft. Daarna begeeft de engineer zich naar de locatie voor on-site herstel of eventueel kan de engineer remote in loggen voor de centrale systemen.
Tweedelijns support bij incidentafhandeling is op basis van een SLA binnen kantoortijden. Hierbij geldt een Next Business Day responsetijd en een hersteltijd van vijf werkdagen vanaf het moment van aanmelding van een incident door RWS CIV IRN Infra Netwerken.
De dienst omvat ondersteuning bij incidenten op zowel de centrale als decentrale systemen. Een verstoring leidt tot het gedeeltelijk of geheel uitvallen of incorrect werken van de centrale en decentrale systemen. Sensormeldingen vanuit het systeem bij normoverschrijding, zoals brand, water, temperatuur, luchtvochtigheid, automaatstand, toegangsverlening/weigering op locatie en deurstand, zijn buiten scope.

Toelichting dienst CVR toegang
De CVR toegang en omgevingsmonitoring bestaat uit een centraal en decentraal deel.

Centraal wordt gebruik gemaakt van de “iVisit” applicatie, waarin pasautorisaties worden geregistreerd, en de “iProtect” applicatie (als virtual appliance met iPuntu O.S.) die deze pasautorisaties distribueert naar de CVR’s. Daarnaast ontvangt “iProtect” alarmeringen van alle decentrale “Apollo’s”. De alarmeringen worden vertoond op het dashboard van “iProtect” en gelijktijdig per e-mail gemeld aan Rijkswaterstaat MKO. De ODC infrastructuur (IAAS) met daarbij o.a. het netwerk, firewalls en de hosting omgeving (inclusief Windows / MS SQL server) is buiten scope.

Decentraal wordt in de CVR-ruimte gebruik gemaakt van een “Apollo” welke voorziet in een aantal aansluitingen ten behoeve van Toegang en Omgevingsmonitoring:
- Temperatuur- / luchtvochtigheidssensoren in serie – maximaal 4 stuks (ruimte en apparatuur kasten);
- Kaartlezer buiten ruimte met beschermkap;

- Eén elektrisch slot (motor);
- Rookmelder op plafond;
- Waterdetectie in kelder;
- Naderingsschakelaar toegangsdeur;
- Storingscontact LSV-verdeler NO-BREAK en OSB;
- Storingscontact LSV-verdeler Netvoeding;
- Storingscontact Verdelers apparatuur kasten (MPK en RTK);
- Storingscontact Airconditioning.

De Apollo inclusief bekabeling en componenten (Temperatuur en LV sensoren, kaartlezer, elektrisch motorslot, rookmelder en waterdetector zijn in scope van de dienstverlening. De componenten naderingsschakelaar, verdelers met hulpcontacten, airconditioning, UPS met SNMP management kaart en de cilinder van het deurslot zijn buiten scope. De cilinder van het deurslot blijft de verantwoordelijkheid van de Rijkswaterstaat regio.

Voor deze dienstverlening gelden de volgende uitgangspunten:

- Er geschiedt geen reparatie van decentrale componenten op locatie. Het betreft "swap" dienstverlening waarbij het defecte component vervangen wordt. Zowel software/hardware resets als swaps maken deel uit van het incidentproces;
- Incidenten op de centrale omgeving worden opgelost om de gebruiker in staat te stellen op acceptabele wijze verder te werken. Het onderliggende probleem wordt via Problem Management structureel opgelost;
- Bij complete uitval van de centrale systemen kan herstel (restore) van de applicaties noodzakelijk zijn.
- Voor de centrale iVisit applicatie kan door Rijkswaterstaat zelf een snapshot teruggezet worden;
- Bij een complete crash van de iProtect applicatie kan geen garantie worden gegeven dat een snapshot werkend teruggezet kan worden;
- Remote toegang tot het Rijkswaterstaat ODC en de mogelijkheid tot inloggen op de centrale systemen is nodig voor deze dienstverlening. Daarbij moet er een remote omgeving beschikbaar zijn die mogelijkheid biedt om voldoende technische handelingen uit te voeren voor het onderzoeken en oplossen van storingen aan de decentrale en centrale systemen;
- De dienst is uitgerold voor een installed base van 56 CVR locaties. Andere locaties zijn buiten scope en dienen middels een Non PDC aanvraag te worden toegevoegd aan deze dienstverlening;
- De capaciteits- en beschikbaarheidsplanning is zodanig ingericht dat een aanbod van 5% van de installed base aan storingen binnen SLA kan worden aangenomen en afgehandeld. Dit betekent een gelijktijdige behandeling van het aantal openstaande calls gelijk aan 5% van het aantal CVR locaties, te weten 3 openstaande calls. Zodra een vierde call wordt aangemeld, zal deze als best inspanning worden opgepakt;
- RWS dient aan te geven wanneer extra werkzaamheden of verkeersmaatregelen noodzakelijk zijn en ook welke werkzaamheden en verkeersmaatregelen het betreft. Hiervoor gelden additionele kosten waarvoor tot maximaal €1.000,- van tevoren voor

akkoord gevraagd. Voor werkzaamheden waarvan de kosten deze grens overschrijden wordt een separate offerte uitgebracht waarop vooraf akkoord dient te worden gegeven door RWS;

- Indien er geen toegang mogelijk is tot de locatie met de uitgegeven tag, dan bestaat de mogelijkheid om gebruik te maken van de fysieke noodsleutel. Deze is in bezit bij Rijkswaterstaat en hiervoor dient de noodprocedure gebruikt te worden. Uitgangspunt is dat in dit geval toegang door Rijkswaterstaat geregeld wordt met een maximale wachttijd van 15 minuten. Een wachttijd langer dan 15 minuten wordt als meerwerk beschouwd en in overleg verrekend;
- (Preventief) onderhoud kan worden uitgevoerd binnen kantoortijden. De planning dient met SPIE afgestemd te worden en minimaal 10 werkdagen van tevoren gemeld te zijn als gepland werk;
- Een reeds met SPIE afgestemde planning wordt minimaal 10 werkdagen voorafgaand aan de werkzaamheden als gepland werk gemeld bij SPIE.
- Voor het oplossen van incidenten zijn soms vervangende materialen en componenten noodzakelijk. Van ieder decentraal component zal een service voorraad aangehouden worden. Alle meldingen veroorzaakt door herhaald of stelselmatig onkundig gebruik van apparatuur en/of programmatuur worden kenbaar gemaakt, zodat dit inzichtelijk wordt en hier structureel een oplossing voor komt;
- Jaarlijks preventief onderhoud en controle van zowel de decentrale Apollo met aangesloten sensoren en het elektrisch motorslot is vereist voor een correcte werking. Voor het oplossen van geconstateerde gebreken tijdens het preventief onderhoud wordt een offerte uitgebracht;
- Om de werking van het complete Apollo systeem te garanderen moet de centrale omgeving (iProtect en iVisit) ten minste één keer per jaar up-to-date gehouden worden (jaarlijkse Software Update);
- Bij het eerste preventief onderhoud worden alle serienummers van de desbetreffende componenten genoteerd en opgeslagen in de CMDB van SPIE. Bij uitwisseling van componenten op locaties voor het oplossen van incidenten zal er een update in deze CMDB plaatsvinden als gevolg van de swap.

Tabel 2 Overzicht CVR locaties in scope

CVR locaties in scope				
Noord Nederland (NN)				
CVR Joure CVR	CVR Hoogeveen	CVR Haren	CVR Werpsterhoek	CVR Zuidbroek
Midden Nederland (MN)				
CVR Deil	CVR Eemnes	CVR Everdingen	CVR Haarrijn	CVR Hoevelaken
CVR Lunetten	CVR Ouderijn	CVR Rijnsweerd		
West Nederland Noord (WNN)				
CVR Hoorn	CVR Watergraafsmeer	CVR Coenplein	CVR Badhoevedorp	CVR Kooimeer
CVR Nieuwe Meer	CVR Raasdorp	CVR De Hoek	CVR Den Oever	CVR Holendrecht

CVR locaties in scope				
CVR Almere	CVR Amstel			
West Nederland Zuid (WNZ)				
CVR Bodegraven	CVR Gorinchem	CVR Gouwe	CVR Kleinpolderplein	CVR Prins Clausplein 1
CVR Prins Clausplein 2	CVR Ridderkerk	CVR Terbregseplein		
Oost Nederland (ON)				
CVR Azelo	CVR Bankhoef	CVR Barneveld	CVR Beekbergen	CVR Deventer
CVR Hattemerbroek	CVR Lankhorst	CVR Lindeholt	CVR Maanderbroek	CVR Ouddijk
CVR Valburg	CVR Velperbroek	CVR Waterberg		
Zuid Nederland (ZN)				
CVR De Baars	CVR De Stok	CVR Ekkersweijer	CVR Galder	CVR Het Vonderen
CVR Hintham	CVR Hooipolder	CVR Kerensheide	CVR Kruisdonk	CVR Zaarderheiken

Glasvezelbeheer
Met de dienst Glasvezelbeheer voert Conclusion het beheer voor het glasvezelnetwerk van RWS. Dit betreft het aansturen van de werkzaamheden, het registreren van de liggingsinformatie (indien bekend) en het wijzigen van het fysieke glasvezelnetwerk. SPIE is daarnaast verantwoordelijk voor glasvezelregistratie. Rijkswaterstaat Areaalbeheer registreert de liggingsgegevens van kabels en leidingen (as-built informatie), dit valt buiten de scope van het Glasvezelbeheer.
De Installed base omvat zowel glasvezelkabel (GVK) als Hoge Dichtheid Polyetheen buis (HDPE).

De dienstverlening bestaat uit de volgende onderdelen:
- Administratie

Om operationele glasvezelkabel- en liggingsinformatie uit projecten, incidenten, reconstructies, nieuwbouw en onderhoud te administreren wordt het CMDB Glasbeheersysteem "COntrolled COnsistent Networks" (COCON) gebruikt. Hierin worden complexe glasvezel netwerkstructuren ingevoerd, gemuteerd en geraadpleegd.
- Leveren van Advies

Het leveren van advies is nader beschreven in de categorie Overig paragraaf 0.
- Incidentafhandeling

OPSI voert regie bij het oplossen van incidenten. Indien in het incidentmanagement van SP-IB onderzoek of actie nodig is ten aanzien van het glasvezelnetwerk analyseert de incidentcoördinator met behulp van COCON of en waar in het glasvezelnetwerk het incident wordt veroorzaakt. Deze informatie wordt gebruikt voor herstel van patches of om kabelherstel te laten verrichten. De vezelbeheerders van SPIE verwerken wijzigingen in de glasvezelbezetting als gevolg van de herstelwerkzaamheden in COCON.
- Uitvoeren geplande werkzaamheden aan de glasinfrastructuur

De impactanalyse bij Gepland Werk Glas is nader beschreven in de categorie Overig paragraaf 4.6.1.

- Uitvoeren kwaliteitscontrole

SPIE voert twee keer per jaar steekproefsgewijs kwaliteitscontroles uit. De locatie waar de controles worden uitgevoerd worden in onderling overleg bepaald.
De kwaliteitscontrole behelst:

- Controle op de kwaliteit van de glasvezelregistratie;
- Jaarlijkse controle op de juistheid van de geografische registratie van O&A (COCON) ten opzichte van de registratie in de Kabels & Leidingen administratie van RWS;
- Controle op de juistheid van de informatie op het label van verdelers en patches in technische objecten (CVR, VC, tunnel);
- Controle op de kwaliteit van de technische afwerking van glasvezels in technische objecten;
- Controle op de kwaliteit van de glasvezels doormiddel van Optical Time-Domain Reflector metingen.

Op grond van de uitkomsten van de controles stelt SPIE een rapport met bevindingen en bijbehorende maatregelen op. In overleg tussen RWS, OPSI en SPIE wordt vervolgens bepaald welke maatregelen gerealiseerd worden en wie verantwoordelijk is voor het dragen van bijbehorende kosten.

- Vezeluitgifte

SPIE geeft glasvezels uit aan projecten en houdt reserveringen en de resterende capaciteit bij. Uiteindelijk wordt het definitieve vezelgebruik in Cocon geregistreerd.

Bestelbare items en levertijd

Bestellingen worden door O&A Quanza verwerkt.
De categorie CV BB kent uitsluitend bestelbare items voor IDS/IPS weergegeven in de volgende tabel:

IDS IPS		
Eenmalige dienst	**Toelichting**	**evertijd in werkdagen**
IPS Centraal		
Aanvragen	Aanvragen IDS/IPS account *)	5
Opheffen	Opheffen IDS/IPS account *)	5
Wijzigen	Wijzigen IDS/IPS account *)	5
Activeren	Activeren intrusion rule **)	5
Deactiveren	Deactiveren intrusion rule **)	5

Tabel 3 Bestelbare items IDS/IPS

*) Bij het aanvragen van een account om toegang tot het systeem te krijgen dient aangegeven te worden welke rechten deze gebruiker moet krijgen. Accounts worden niet apart door configuratie management in de CMDB geregistreerd. Via een RFI kan een overzicht van de aanwezige accounts opgevraagd worden. Deze standaard opdrachten kunnen op basis van LNT-Express aangevraagd worden als tactische wijziging. Voor tactische aanvragen dient de afnemer contact op te nemen met de Relatie Manager van RWS CIV IRN

Infra Netwerken. De Relatie Manager bepaalt of de aanvraag al dan niet in behandeling wordt genomen.
**) Het betreft voor-gedefinieerde intrusion rules die geactiveerd of gedeactiveerd kunnen worden.

Categorie VPN
Virtual Private Networks (VPN's) zijn landelijk beschikbaar en kunnen middels de diensten VPN Aansluiting en LAN aansluiting tot op LAN access poort niveau op eindlocaties ontsluiting bieden tot systemen.
Optioneel kan het VPN via een Virtual Firewall verbonden worden met het internet middels Internet Access. Afhankelijk van het type VPN zijn bepaalde standaardvoorzieningen mogelijk, verplicht of beperkt. Een VPN biedt de mogelijkheid binnen een besloten en logisch gescheiden netwerk op veilige, betrouwbare wijze bedrijfsinformatie en applicaties te benaderen én informatie te delen tussen geografisch gescheiden netwerken als binnen één dedicated netwerk. Het VPN is randvoorwaardelijk om communicatie tussen eindsystemen op RWS en niet-RWS eindlocaties mogelijk te maken.
Onder de categorie Virtual Private Network (VPN) vallen de diensten **VPN**, **Virtual Firewall**, **DDI**, **DMZ** en **DMZ Client**, **Forward Webproxy** en **Mail Relay**.

Beheer VPN
RWS onderkent de volgende onderdelen van de categorie VPN:
1. VPN
2. Virtuele Firewall
3. DDI – DHCP & DNS
4. DDI – IPAM
5. DDI – Gedelegeerd beheer
6. DDI – NTP
7. DMZ en DMZ client
8. Forward Webproxy
9. Mail Relay

Quanza IB voert het beheer uit op deze VPN types conform onderstaande SLA.

MATRIX VPN											
Diensten	Beschikbaarheid							Storingshersteltijd in 95% van de gevallen			
	Enkel			Dubbel			VPN	Service Window Kantoortijden		Service Window"24/7"	
	99,5%	99,9%	99,95%	99,98%	99,99%	99,99%	99,999%				
	Onbeschikbaarheid per jaar										
	ca 1d20u	ca 8u45m	ca 4u28m	ca 4u28m	ca 1u45m	ca 0u52m	ca 5m15s	8 uur	4 uur	8 uur	4 uur
VPN							V				V
Virtual Firewall			V								V
DDI - DHCP & DNS*	V					V					V
DDI - IPAM		V									V
DMZ en DMZ Client					V						V
Forward Webproxy				V							V
Mail Relay				V							V

* De centrale beschikbaarheid van DDI componenten is 99,99%, deze zijn dubbel uitgevoerd en hiertoe geplaatst over 2 fysiek geografisch gescheiden locaties. De beschikbaarheid over de gehele keten is afhankelijk van de overige bouwstenen waar de afnemer gebruik van maakt.

Tabel 4 Dienstenmatrix VPN – diensten

VPN
Een Virtual Private Network (VPN) stelt RWS in staat (een) besloten en volledig gescheiden netwerk(en) te creëren. Dit maakt het mogelijk om op veilige, betrouwbare wijze informatie te delen tussen geografisch gescheiden netwerken alsof er één dedicated netwerk zou zijn. Een VPN is randvoorwaardelijk om communicatie tussen eindsystemen op RWS en niet-RWS eindlocaties mogelijk te maken. VPN's zijn landelijk beschikbaar en kunnen middels de diensten **VPN Aansluiting** en **LAN Aansluiting** tot op LAN access poort op eindlocaties ontsluiting bieden tot systemen.

Wanneer network services als DHCP, DNS, NTP, Internet Acces, Extranet Access of Remote Access tot het RWS netwerk nodig zijn voor het VPN, dan moeten deze verplicht via de PDC dienstverlening van CIV Netwerken worden afgenomen. Deze network services zijn nader toegelicht in paragraaf 0 van dit document.

Virtual firewall
Het RWS netwerk beschermt de integriteit en vertrouwelijkheid van de verschillende VPN's en DMZ's door middel van firewalls. Een firewall blokkeert alle communicatie, tenzij expliciet toegestaan. Daarnaast worden specifieke (potentieel schadelijke) communicatiepatronen binnen toegestane communicatie geblokkeerd.
Een Firewall Policy bepaalt per VPN, DMZ en het Internet welke communicatiestromen zijn toegestaan.

Een Firewall Policy bestaat uit een specificatie van toegestane datastromen waarbij niet meer toegang dient te worden verleend dan strikt noodzakelijk. Per VPN kan een virtual firewall geleverd worden.
Een datastroom wordt binnen de dienst Virtual Firewall gespecificeerd middels de volgende voorwaarden:

- Bron IP adres: IP adres waar datacommunicatie opgezet wordt (het beginpunt);
- Bron IP Protocol: TCP, UDP of ICMP;
- Bron Poort: IP poort nummer dat in combinatie met het Bron Protocol de applicatie op het Bron systeem identificeert;
- Doel IP adres: het IP adres waarnaar datacommunicatie opgezet wordt (de eindbestemming);
- Doel Protocol: TCP, UDP of ICMP;
- Doel Poort: het IP poort nummer dat in combinatie met het Doel Protocol de applicatie op het Doel systeem identificeert.

Om meerdere aaneengesloten IP adressen tegelijkertijd aan te duiden, kan in combinatie met het IP-adres ook het bron of doel IP-Subnetmasker aangegeven worden. Een IP-Subnetmasker specificeert het netwerksegment en de systemen in dit netwerksegment.

DDI
DDI (DNS DHCP IPAM) levert de aan IP-adressen gerelateerde services aan de Centrale Voorzieningen van het RWS netwerk. Daarnaast geeft het specifieke RWS medewerkers en

onderaannemers van RWS de mogelijkheid om relevante IP-gerelateerde configuraties te onderhouden.
De dienst DDI bevat de volgende onderdelen:

1. Gedelegeerd beheer voor DDI;
2. IP Address Management (IPAM);
3. Domain Name Services (DNS);
4. Dynamic Host Configuration Protocol (DHCP).

Ad1 Gedelegeerd beheer
De functie 'gedelegeerd beheer' geeft RWS medewerkers en RWS onderaannemers de mogelijkheid om de 'IP-ruimte' waarvoor zij verantwoordelijk zijn te beheren. Deze functie heeft de volgende kenmerken:

- Sterke gebruikers authenticatie met een hardware token (RSA) + gebruikersnaam/wachtwoord uit de RWS Active Directory (AD) of gebruik te maken van de SMS authenticatie binnen de dienst (een onderaannemer van RWS dient derhalve een AD account te hebben om gedelegeerd beheer te kunnen doen);
- Autorisatie via groepslidmaatschap in RWS AD. De permissies per groep (lezen, schrijven, en waar op) worden via een standaard aanvraag gerealiseerd;
- Zonder aangevraagde permissies heeft een medewerker geen mogelijkheden tot het gebruik van de 'gedelegeerd beheer' functionaliteit;
- Via 'gedelegeerd beheer' kan men de IPAM , DNS en/of DHCP gegevens muteren voor zover het eigenaarschap op de betreffende IP-ruimte reikt.
- Via 'gedelegeerd beheer' kan men daarnaast, afhankelijk van toegewezen permissies, inzicht krijgen in de inhoud van een DDI-profiel (welke DDI-info en welke permissies zijn toegewezen aan een rol).
- Logging van toegang en toegangspogingen;
- Voor gedelegeerd beheer is het van belang dat een gebruiker slechts lid is van 1 DDI-gerelateerde resourcegroep. De dienst werkt zo dat de permissies worden gekoppeld aan het eerste groepslidmaatschap dat in het kader van DDI wordt aangereikt vanuit de RWS AD omgeving.

Ad 2. IP Address Management (IPAM)
IPAM geeft geautoriseerde RWS medewerkers de mogelijkheid om IP-gerelateerde informatie vast te leggen om context te kunnen geven aan IP-gerelateerde gegevens zoals fysieke locatie, eigenaar, toepassing etc. Zo wordt IP-informatie beter bruikbaar als ondersteuning bij audits, het uitvoeren van kwaliteitscontrole, het toetsen van KPI's en het onderzoeken van verstoringen/incidenten (onder andere security).

IPAM heeft de volgende kenmerken:

- Een grafische gebruikersinterface;
- Informatievastlegging (eigenaar, toepassing, security classificatie etc.);
- Informatievastlegging per IP reeks of subnet;
- Zoekfunctie binnen velden IPAM database (IP adres, VPN naam, eigenaar, 'next Available IP' etc.);

- Vastlegging DNS naam die bij een IP-adres hoort en automatische synchronisatie met de DNS functie;
- Vastlegging DHCP gegevens van een IP-adres en automatische synchronisatie met de DHCP functie;
- Overerving van op hoger niveau vastgelegde informatie (zoals VPN naam waartoe de IP-ruimte behoort);
- Read only voor gegevens die niet gewijzigd mogen worden en schrijftoegang tot gegevens die gewijzigd mogen worden;
- Beschikbaar stellen IPAM informatie database via RWS Splunk feed (volledige export IPAM database 1x per 24 uur);
- Logging van alle mutaties, inclusief naam van de uitvoerende persoon en het tijdstip.

Ad 3. Domain Name Services (DNS)
De DNS-functie levert aan het RWS netwerk de centrale DNS functies voor het oplossen van interne RWS DNS zones en externe niet-RWS [1]DNS zones zoals Internet). Deze functie heeft de volgende kenmerken:

- Mutaties zijn mogelijk via aanvraag (per record of in bulk) of via gedelegeerd beheer;
- Zone transfers worden niet ondersteund;
- Voorziet in hosting en resolving van interne DNS domeinnamen;
- Resolving van externe DNS domeinnamen, hetzij generiek (recursief, bijvoorbeeld google.com), hetzij specifiek (Forwarding, bijvoorbeeld naar rijksweb.nl);
- Beschikbaar voor alle RWS MPLS VPN's, mits vanuit security regelgeving toegestaan en het geen gesloten VPN betreft;
- Zone informatie kan beschikbaar worden gesteld aan of worden afgeschermd voor bepaalde source IP subnetten door gebruik te maken van 'DNS views';
- DNSSEC[2]-validatie van DNS responses bij resolving op Internet (externe resolver). DNSSEC signing van RWS domeinen wordt niet ondersteund;
- Logging van DNS requests en failures;
- Dynamische zone updates als gevolg van IP adrestoekenning via DHCP (Dynamic DNS, ofwel DDNS) worden genegeerd.

Ad 4. Dynamic Host Configuration Protocol (DHCP)
DHCP levert het RWS netwerk de centrale DHCP functie voor het configureren van IP-instellingen op aangesloten apparatuur. Deze functie heeft de volgende kenmerken:

- De functionaliteit om op dynamische wijze de netwerkinstellingen van op het RWS netwerk aangesloten hosts te configureren (IP-nummers, name servers, gateway adressen, netmask, proxy adres e.d.);

[1] De externe DNS zones van RWS zelf (bv rws.nl) zijn buiten scope van deze dienst. Deze externe zones worden extern gehost, o.a. bij Prolocation. Verdere informatie bij IRN CIV netwerken.
[2] Is een crypto grafische beveiliging voor het DNS-protocol. Clients die deze uitbreiding ondersteunen, ontvangen van de DNS server adres-informatie met een digitale handtekening. Zo wordt de integriteit van de DNS omgeving en het transport van de DNS data beschermd.

- Aangezien de centrale DHCP gepositioneerd wordt buiten het broadcast domein dient op die delen waar DHCP van toepassing is, DHCP relay/helper op de VPN Aansluiting ingesteld te worden;
- Mutaties mogelijk via aanvraag (per scope met bijbehorende opties, of in bulk) of gedelegeerd beheer;
- Vendor specifieke DHCP options worden ondersteund;
- Het is mogelijk om een vast DHCP IP adres te koppelen aan hetzelfde systeem (MAC adres of Client-ID), standaard wordt een MAC adres gekoppeld aan een IP adres;
- DHCP configuratie is zoveel mogelijk generiek, maar kan per VPN-aansluiting van uitzonderingen worden voorzien na akkoord van CIV IRN Netwerken;
- Logging van DHCP requests en failures;
- Inzicht in de mate van uitnutting van een DHCP scope. Bij naderende (bv.80%) of volledige (100%) uitnutting wordt hierover genotificeerd. Sommige objecten moeten autonoom kunnen draaien en mogen derhalve geen gebruik maken van centrale DHCP.

Uitgangspunten DDI

De volgende uitgangspunten gelden voor DDI:

- Gebruiker krijgt alleen toegang tot IPAM indien deze in bezit is van een geldig RWS AD account;
- Netwerk connectiviteit dient te zijn ingeregeld om gebruik te kunnen maken van DNS;
- Voor DHCP worden geen scopes geboden met overlappende IP reeksen. Uitgangspunt is dat alle aansluitingen in het RWS netwerk unieke adressen hebben;
- RWS CIV-infra is verantwoordelijk voor de toetsing van aanvragen voor gedelegeerd beheer zodat alleen geautoriseerde personen toegang krijgen tot de data binnen DDI;
- Admin toegang wordt geregeld via centrale BAS service;
- DDI-configs zijn als het ware containers met DNS-, DHCP- en/of IPAM objecten. Men kan een wijziging aanvragen voor objecten in een container, of gedelegeerd beheer krijgen op de objecten in een container. Het beheer op de container zelf is voorbehouden aan SP-IB in diens verantwoordelijkheid voor het netwerk en de IT-netwerkdiensten;
- DDI profielen worden zo generiek mogelijk ingericht en onderhouden om te voorkomen dat een onoverzichtelijke set van profielen ontstaat. Dit is essentieel voor onder andere auditeerbaarheid van toegangsrechten. Tevens dient maximaal te worden geprofiteerd van overerving uit (default) settings;
- RWS stelt de profielnaam vast;
- De aanvrager (geprocedeerde) is verantwoordelijk voor de inzet c.q. gebruik;
- De gebruiker (bv gedelegeerd beheerder) is verantwoordelijk voor het veilig omgaan met de informatie en de toegangsmiddelen;
- De gedelegeerde beheerder is zelf verantwoordelijk voor verstoringen op de keten die voortvloeien vanuit aanpassingen die worden gedaan door de beheerder zelf;
- RWS is verantwoordelijk voor het aan SP-IB verstrekken van geldige digitale certificaten (PKI) voor de HTTPS ontsluiting van de ‘gedelegeerd beheer’ functie.

DMZ
De dienst DMZ (Demilitarised Zone) voorziet in een gecontroleerde communicatiezone tussen het interne en het externe netwerk om veiligheidsrisico's te verkleinen. Het externe netwerk, vaak het internet, is "untrusted". Een systeem in de DMZ is relatief vrij toegankelijk vanuit het publieke internet.
Het interne netwerk is echter een beschermd "trusted" deel van het netwerk, zoals een interne VPN, dat uitsluitend toegankelijk is voor geautoriseerde systemen en gebruikers.

Forward Webproxy
De dienst Forward Webproxy dient als uitgang voor al het websurfverkeer door gebruikers naar het internet en andere externe netwerken (en dus niet interne webapplicaties) en dient te worden afgenomen om websurfen op externe netwerken via http(s) protocollen mogelijk te maken.

Mail relay
De dienst Mail Relay dient als in- en uitgang voor al het e-mailverkeer van en naar het internet. Mail relay wordt ingezet als koppelvlak voor e-mailuitwisseling binnen RWS, met het internet en met organisaties aangesloten op het Rijksweb. Het koppelvlak scant inkomende en uitgaande e-mail op schadelijke of anderszins ongewenste inhoud middels verschillende beveiligingsvoorzieningen:

- Reputatie filtering: Het blokkeren van connecties van nodes op internet die bekend staan om ongewenst gedrag, zoals bekende bronnen van spam en malware;
- Relay bescherming: alleen relayen van uitgaande e-mail vanaf (RWS) hosts die geautoriseerd zijn om email via de relay te mogen uitsturen;
- Afzender controle: wanneer een afzendend domein een SPF DNS record heeft, zal de Mail Relay de daarin opgenomen policy honoreren;
- Bericht integriteitscontrole: via berichtondertekening uit naam van het domein (DKIM) beveiligde berichten worden gecontroleerd op authenticiteit en integriteit;
- Versleuteling van e-mailtransport;
- Adres controle: alleen e-mail voor bestaande RWS domeinen wordt verwerkt. Externe afzenders weren als zij vaak foutieve RWS emailadressen hanteren (bescherming RWS mailomgeving);
- Limiteren van berichtgrootte: maximaal 25MB. Aangesloten e-mailomgevingen kunnen minder groot staan ingesteld;
- Attachment controle: door RWS vastgestelde ongewenste bijlagen kunnen worden geblokkeerd;
- Malware controle: het blokkeren van e-mails met schadelijke inhoud;
- Spam controle:
  - Het in quarantaine plaatsen van mogelijke spamberichten;
  - het blokkeren van spamberichten.

Het onterecht blokkeren van een legitiem bericht (als spam) en het onterecht doorlaten van een spam bericht (als legitiem bericht) dient zo min mogelijk plaats te vinden. Hiervoor is het false positive rate gesteld op 1:1.000.000, wat betekent dat hooguit 1 op de miljoen op spam

gecontroleerde berichten onterecht als spam gekenmerkt mag worden en het false negative rate gesteld op 1:1.000, wat betekent dat hooguit 1 op de duizend op spam gecontroleerde berichten onterecht als legitiem bericht gekenmerkt mag worden.

Verder kent de Mail Relay de volgende functies:

- Quarantaine: berichten die mogelijk spam zijn worden in quarantaine geplaatst. De eindgebruiker kan een bericht desgewenst laten doorsturen naar de eigen mailbox;
- Interne notificaties: in een aantal situaties kunnen medewerkers van RWS een notificatie e-mail ontvangen:
  - Wanneer een schadelijk item is onderschept van of naar de betreffende medewerker;
  - Wanneer een bericht van of naar de betreffende medewerker niet gescand kon worden (bv wachtwoord beveiligde bijlage);
  - Wanneer er nieuwe spamberichten in de quarantaine zijn geplaatst voor de betreffende medewerker.
- Externe notificaties: als een externe zender een e-mail stuurt naar een niet bestaande RWS medewerker (foutief adres), krijgt de externe zender hiervan een notificatie;
- Disclaimer: er wordt door de Mail Relay geen disclaimer toegevoegd aan een e-mail.

De Mail Relay kent drie interfaces: SMTP voor e-mail transport; HTTP voor spam quarantaine en DNS voor afzender controle.

Bestelbare items en levertijd
Voor het VPN gelden de in onderstaande tabel weergegeven bestelbare items met bijbehorende standaard levertijden.

Tabel 5 Bestelbare items VPN diensten

VPN			
Eenmalige dienst	**Toelichting**	**Levertijd in werkdagen (SP-O&A)**	**SSR (door SP-IB)**
VPN			
Aanvragen	Leveren nieuw VPN	20	
Opheffen	Opheffen VPN	20	
Wijzigen	Wijzigen instelling bestaand VPN op afstand	10	
Aanvragen VPN QoS Profiel	Realiseren QoA profiel op VPN	20	
Virtual firewall			
Aanvragen	Leveren nieuwe Firewall	10	
Opheffen	Opheffen Firewall	10	
Wijzigen	Wijzigen/toevoegen/verwijderen Firewall rules (max. 20 rules per aanvraag*)	5	Ja
Wijzigen	Wijzigen/toevoegen/verwijderen Firewall rules met spoed	1	Ja
DDI-DHCP Scope			
Aanvragen	Aanvragen DHCP scope (IP range centrale distributie)	10	
Opheffen	Opheffen DHCP scope (IP range centrale distributie)	10	
Wijzigen	Wijzigen DHCP scope (IP range centrale distributie)	10	
Aanvragen toegang	Aanvragen toegang op bestaande DHCP scope RW/RO	10	
Opheffen toegang	Opheffen toegang op bestaande DHCP scope RW/RO	10	
DDI – DNS Domeinnaam			
Aanvragen	Leveren DNS domeinnaam/record (Host/Prt/A/CNAM/MX)	10	
Opheffen	Opheffen DNS domeinnaam/record (Host/Prt/A/CNAM/MX)	10	
Wijzigen	Wijzigen DNS domeinnaam/record (Host/Prt/A/CNAM/MX)	5	
DDI – Gedelegeerd beheer			
Aanvragen	Aanvragen DNS/DHCP/IPAM gedelegeerd beheer groep	10	
Opheffen	Opheffen DNS/DHCP/IPAM gedelegeerd beheer groep	10	
Wijzigen	Wijzigen DNS/DHCP/IPAM gedelegeerd beheer groep	10	
DDI – IPAM			
Aanvragen	Aanvragen/opvoeren van een (nieuw) netwerk, of nieuwe eigenaren van bestaand netwerk	10	
Opheffen	Opheffen van netwerk informatie van netwerken binnen een VPN	10	
Wijzigen	Opvoeren/update van host informatie binnen een netwerk	5	
DMZ en DMZ Client			

VPN			
Aanvragen	Aanvragen DMZ	30	
Opheffen	Opheffen DMZ	10	
Aanvragen Client	Aanvragen Client aansluiting	20	
Opheffen Client	Opheffen Client aansluiting	10	
Wijzigen Client	Wijzigen Client aansluiting	5	
Forward Webproxy			
Aanvragen	Aanvragen Forward Webproxy	In overleg	
Opheffen	Opheffen Forward Webproxy	In overleg	
Wijzigen	Wijzigen Forward Webproxy	In overleg	
Mail Relay			
Aanvragen	Aanvragen Mail Relay	In overleg	
Opheffen	Opheffen Mail Relay	In overleg	
Wijzigen	Wijzigen Mail Relay	In overleg	

* Wanneer er meer dan 20 rules gewijzigd moeten worden adviseren wij om gebruik te maken van een meervoudige PDC project aanvraag.

Levering gebeurt door Quanza – O&A met uitzondering van de Standaard Service Requests, die door Quanza – IB worden uitgevoerd. Voor alle werkzaamheden op locatie wordt SPIE aangestuurd.

Categorie LAN aansluiting

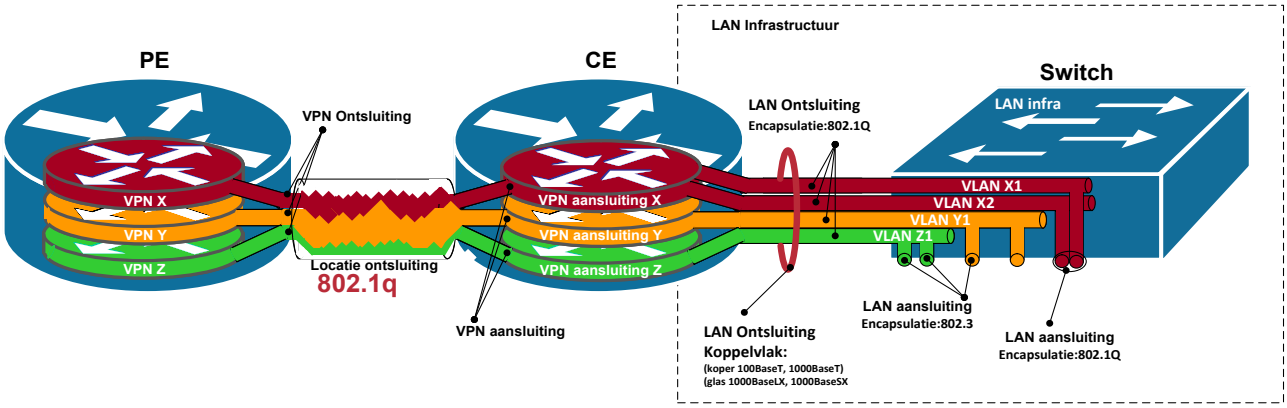
Een LAN aansluiting maakt het mogelijk om op RWS locaties connecties te maken over het netwerk. De categorie **Local Area Network (LAN) aansluiting die uitsluitend te bestellen is door CIV IRN Infra Netwerken** omvat de LAN aansluiting type ODC en de LAN aansluiting type SPAN. De overige LAN-aansluitingen zijn beschreven in deel 2 van de gTSC.

LAN Aansluiting type ODC

Het type LAN aansluiting ODC, weergegeven in Fout! Verwijzingsbron niet gevonden., is o ntwikkeld ten behoeve van de productieomgeving voor systemen met hoge eisen aan beschikbaarheid en bandbreedte zoals in het Overheid datacenter. Dit type LAN Aansluiting heeft de volgende kenmerken:

- Fysiek koppelvlak 100Base/1000Base/10GBase, inclusief bekabeling naar het patchpaneel op locatie;
- Gestandaardiseerd ethernet/IP gebaseerd datatransmissienetwerk voor Unicast & Multicast verkeer (inclusief IGMPv2/ IGMP snooping);

- Scheiding van applicatiedomeinen met behulp van VLAN's;
- Bij LAN ontsluiting is inter-VLAN routering toegestaan voor RWS CIV IRN Infra Netwerken, mits deze tot hetzelfde VPN behoren;
- Als onderdeel van een tactische change is het mogelijk om niet-routeerbare/geïsoleerde VLAN's aan te vragen. Tactische aanvragen zijn aanvragen waarvoor de afnemer contact op dient te nemen met de Relatie Manager van RWS CIV IRN Infra Netwerken. De Relatie Manager bepaalt of de aanvraag al dan niet in behandeling wordt genomen;
- De aansluiting is uitsluitend bedoeld voor eindsystemen. Aan de Edge wordt detectie van Spanning-tree toegepast om een loop-free topologie te waarborgen;
- Trunking (802.1Q) uitsluitend naar servers en Blade servers;
- VLAN's binnen een trunk naar een server of Blade server behoren aan uitsluitend één VPN. Hiervan kan afgeweken worden indien de scheiding tussen de VPN's gewaarborgd kan worden.[3] Koppelingen tussen de VPN's mogen uitsluitend via een firewall policy in de Centrale voorzieningen worden gerealiseerd;
- Bieden van LAN aansluiting redundant door interface bundeling (Etherchannel) via redundante switches t.b.v. servers en Blade servers;
- Alle Virtuele LANs worden gestretched over de ODC locaties AM2 en AM3 (via E-services Hub). Alle IP reeksen van de Virtuele LANs zijn via beide WAN uplinks benaderbaar (primair/back-up). Middels de dienstbouwsteen VPN-aansluiting wordt een primaire locatie aangegeven. De primaire locatie is de locatie waarnaartoe het verkeer gerouteerd zal worden als beide locaties beschikbaar zijn. De andere locatie wordt automatisch als back-up-locatie aangemerkt;
- Inter-VLAN verkeer tussen servers binnen een fysieke ODC locatie wordt zo dicht mogelijk bij de server, maar in elk geval binnen de fysieke locatie, afgehandeld.



Figuur 3 LAN infrastructuur ODC

Quanza IB voert het beheer uit op het type LAN aansluiting ODC conform onderstaande SLA.

[3] Dit kan bijvoorbeeld gerealiseerd worden door virtuele switches in de aangesloten hypervisor.

Dienstenmatrix LAN											
Type LAN Aansluiting	Bandbreedte	Beschikbaarheid						Storingshersteltijd in 95% van de gevallen			
		Enkel			Redundant			Service Window Kantoortijden		Service Window"24/7"	
		99,00%	99,50%	>99,7%	>99,8% **	99,95% ***	99,99% ***				
		Onbeschikbaarheid per jaar									
		ca 3d15u	ca 1d20u	ca 1d2u	ca 17u30m	ca 4u28m	ca 0u52m	8 uur	4 uur	8 uur	4 uur
ODC	<= 100 Mbps		V								V
	<= 1Gbps standaard		V								V
	<= 2Gbps (server/blade redundant)					V					V
	<= 4Gbps (server/blade redundant)					V					V
	<= 10Gbps (server/blade redundant)		V								V
	<= 20Gbps (server/blade redundant)					V					V
	<= 40Gbps (server/blade redundant)					V					V
**	indien sprake is van geografische redundantie glasvezelinfrastructuur										
***	over 2 switches										

LAN aansluiting type SPAN (uitsluitend te bestellen door RWS SOC)

Dit type LAN aansluiting maakt het mogelijk dat er een kopie van het lokale netwerkverkeer aan de RWS Cyber Security Logging en Monitoring (CSLM) keten kan worden geleverd. De SPAN poort wordt gerealiseerd op een laag-2 omgeving óf op basis van poort óf op basis van VLAN (max. 50 VLANs per poort). Management poorten en stack poorten komen niet in aanmerking voor de (R)SPAN-functionaliteit. Het gekopieerde verkeer kan worden verstuurd naar een of meerdere (max. 4 indien technisch mogelijk) poort(en) op dezelfde switch (SPAN) of naar een remote VLAN (RSPAN). Poort channels kunnen wel als source maar niet als destination worden ingezet, waarbij tevens de bandbreedte toereikend moet zijn. By default wordt gebruik gemaakt van ingress (inkomend) verkeer spannen. Egress (uitgaand) verkeer spannen kan alleen op speciaal verzoek, met toestemming van een RWS architect. De sensor die door het RWS SOC op de SPAN poort wordt aangesloten is geen onderdeel van de dienstverlening. (R)SPAN mag alleen worden uitgevoerd binnen één locatie. Wanneer het gebruik van (R)SPAN leidt tot een processor load van 70% of hoger op een switch zal deze poort na overleg met de aanvrager van de SPAN-poort (tijdelijk) worden uitgezet. (R)SPAN is niet geschikt voor forensische doeleinden.

Bestelbare items LAN aansluitingen

Voor de LAN aansluiting gelden de in onderstaande tabel weergegeven bestelbare items met bijbehorende standaard levertijden.

LAN Aansluiting			
Eenmalige dienst	**Toelichting**	**Levertijd in werkdagen**	**SSR door SP-IB)**
LAN aansluiting ODC (Uitsluitend bestelbaar via CIV IRN Infra Netwerken)			
Aanvragen	Leveren 1e LAN aansluiting op apparaat	60	
Opheffen	Opheffen laatste LAN aansluiting op apparatuur	60	
Activeren	Activeren extra LAN aansluiting en patching op locatie	5	
Deactiveren	Deactiveren extra LAN aansluiting en patching op locatie	5	
Wijzigen	Wijzigen instelling bestaande LAN aansluiting op afstand	5	
LAN aansluiting type SPAN (Uitsluitend te bestellen door RWS SOC)			

LAN Aansluiting			
Activeren	Activeren extra LAN aansluiting op afstand	5	
Deactiveren	Deactiveren extra LAN aansluiting op afstand	5	
Wijzigen	Wijzigen instelling bestaande LAN aansluiting op afstand	5	

Tabel 6 Bestelbare items categorie LAN aansluiting

Categorie Overig

Loggingdienst – in ontwikkeling
Logginginformatie over het netwerk is cruciaal bij het signalering en oplossen van incidenten. Daarnaast gebruikt het SOC van RWS de logdata voor controle op de beveliging van het netwerk. De beschikbaarheid en betrouwbaarheid van deze informatie wordt steeds belangrijker. Daarom zijn de afspraken over de Logging dienstverlening van de netwerkbeheerder aan het RWS Splunk team in deze dienst vastgelegd.

Het Splunkteam van RWS is de enige afnemer van deze dienst. Dit team ontvangt met deze dienst logdata van bron devices voor analyse en inzicht. De data wordt verstuurd in het door het RWS Splunkteam gewenste format waarmee zij hun eigen dashboards kunnen maken voor bijvoorbeeld het RWS SOC.
Het oplossen van incidenten op de Loggingsdienst gebeurt op basis van redelijke inspanning. Dat wil zeggen dat er geen garanties zijn afgesproken over herstel van de dienstverlening. Er loopt een traject om de loggingsomgeving robuuster in te richten, waarmee een beschikbaarheidsgarantie van 99,9% en hersteltijd van 4 uur geboden zal worden (verwachte realisatie 2026). Werkzaamheden aan de logservers worden 10 werkdagen vooraf gemeld door SP-IB aan het RWS Splunkteam. Dit kunnen patches zijn of reguliere werkzaamheden. Dit is exclusief security patches. Deze worden iom het RWS Splunk team zsm uitgevoerd. Wanneer er sprake is van een afwijkend logformaat, informeert SP-IB het RWS Splunkteam 10 werkdagen van tevoren, zodat het team de scripts kan aanpassen.

Aanvragen
Alleen het RWS Splunkteam kan wijzigingen op de dienstverlening aanvragen middels een aanvraag gecoördineerde levering in Topdesk. De netwerkbeheerder neemt contact op met het RWS Splunkteam voor verdere afstemming. De volgende standaard aanvragen zijn mogelijk:

- Verwijderen, aanpassen of toevoegen van een logbron aan bestaande logdata.
- 2x per jaar wordt de Splunk forwarder op de logservers van een upgrade voorzien die verstrekt wordt door het RWS Splunkteam. SP-IB installeert de nieuwe versie binnen 5 werkdagen na het akkoord van het CAB.

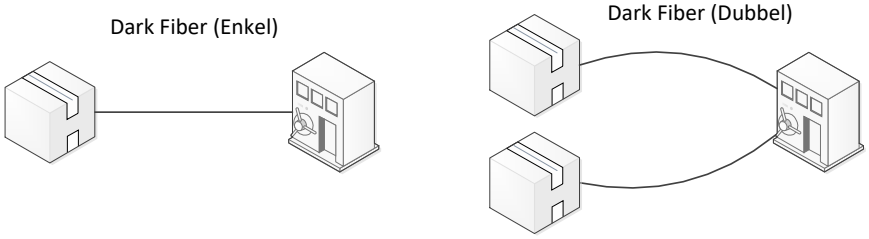
Dark Fiber Advies
Het doel van de dienst Dark Fiber is om RWS in uitzonderlijke gevallen in staat te stellen het Eigen Glas beschikbaar te stellen aan andere (overheids-)partijen in het geval van overcapaciteit. Daarnaast is het ook mogelijk om gebruik te maken van een Dark Fiber van andere (overheids-) partijen door RWS wanneer Eigen Glas niet beschikbaar is. Deze dienst kan alleen worden afgenomen na expliciete goedkeuring van de domeineigenaar van Infra Netwerken, en is uitsluitend te bestellen door medewerkers van CIV IRN Infra Netwerken. Om te bepalen of het op een bepaalde locatie mogelijk is gebruik te maken van de Dark Fiber dienst dient altijd eerst een Dark Fiber Advies te worden aangevraagd.

Dark Fiber RWS levering
Het doel van de dienst Dark Fiber is om RWS in uitzonderlijke gevallen in staat te stellen het Eigen Glas beschikbaar te stellen aan andere (overheids-)partijen in het geval van overcapaciteit. Daarnaast is het ook mogelijk om gebruik te maken van een Dark Fiber van andere (overheids-) partijen door RWS wanneer Eigen Glas niet beschikbaar is. Deze dienst kan alleen worden afgenomen na expliciete goedkeuring van de domeineigenaar van Infra Netwerken en is uitsluitend te bestellen door medewerkers van CIV IRN Infra Netwerken. Dark Fibers zijn onbelichte glasvezelverbindingen tussen 2 locaties, bestaande uit een vezelpaar. De capaciteit van Dark Fiber is afhankelijk van het aanwezige type glasvezel, de te overbruggen afstand en de apparatuur die door de afnemer wordt ingezet. Dark Fibers worden in heel Nederland geleverd. Hierbij wordt alleen gebruik gemaakt van bestaande infrastructuur. Binnen een Dark Fiber levering is geen sprake van aanleg van nieuwe glasvezels. De Dark Fiber dienst is unmanaged, er vindt geen proactieve bewaking plaats.

Opties
De Dark Fiber dienstverlening onderscheidt een aantal opties met betrekking tot de uitvoering van de Dark Fiber, demarcatie/eindpunten en aansluitvarianten.

1. Enkel / Dubbel uitgevoerde Dark Fiber

Een Dark Fiber-verbinding, weergegeven in Figuur 4, bestaat uit twee vezels en kan worden uitgevoerd met een enkele of dubbele verbinding.



Figuur 4 Dark Fiber uitvoering

Dark Fiber (Enkel) = Een vezelpaar tussen twee eindpunten.

Dark Fiber (Dubbel) = Twee geografisch gescheiden vezelparen tussen twee eindpunten, administratief en procedureel onlosmakelijk met elkaar verbonden. Op het moment dat er een storing is op de ene glasvezelverbinding, dan kan de gebruiker door zelf om te schakelen het dataverkeer door laten gaan over de andere glasvezelverbinding. Uiteraard kunnen ook beide verbindingen actief gebruikt worden.

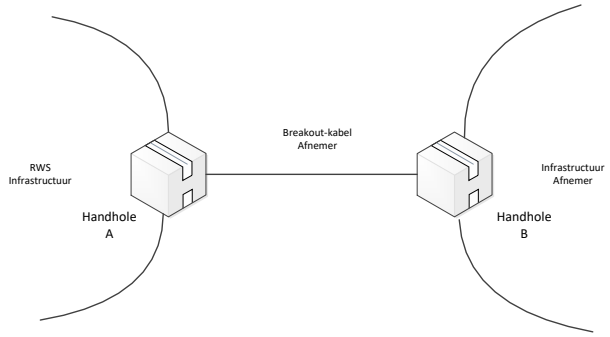
2. Demarcatie / Eindpunten

Het demarcatiepunt van de Dark Fiber verbinding kent twee uitvoeringsvormen. Eindpunten kunnen ondergronds (laskoppeling in een glasvezelkabelput) of bovengronds (patchpaneel in RWS-ruimte) zijn.
De koppelvlakken van de Dark Fibers zijn ofwel ondergronds (glasvezellassen), dan wel bovengronds (patchpaneel).

3. Aansluitvarianten

Er bestaan twee aansluitvarianten (Figuur 5):

1. Handhole (ondergronds)



Figuur 5 Aansluitvariant Handhole

Het koppelvlak voor de Dark Fiber-verbinding bevindt zich in Handhole A.

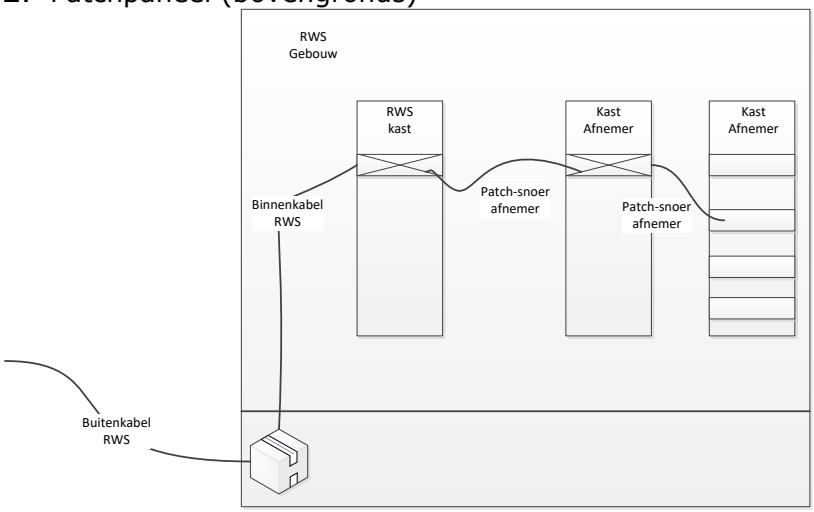
Verantwoordelijkheden RWS-afnemer:

- de aanleg van haar glasvezelinfrastructuur inclusief de Handhole voor koppeling met de RWS-glasvezelinfrastructuur;
- de aanleg van de break-out-kabel tussen beide Handholes;
- het invoeren van de break-out-kabel in Handhole B;
- het koppelen van de glasvezels van de break-out-kabel aan de glasvezelinfrastructuur in Handhole B.

Verantwoordelijkheden RWS:

- het projecteren van de glasvezels in de RWS-infrastructuur (uitgevoerd door SP-O&A);
- het invoeren van de break-out-kabel in Handhole A (uitgevoerd onder regie SP-O&A);
- het koppelen van de glasvezels (voorzien van connectoren type E2000/APC) van de break-out-kabel aan de glasvezelinfrastructuur in Handhole A (uitgevoerd onder regie SP-O&A).

2. Patchpaneel (bovengronds)



Figuur 6 Aansluitvariant Patchpaneel

Binnen een gebouw van RWS wordt de Dark Fiber-verbinding opgeleverd op een patchpaneel, welke is gemonteerd in een 19”-kast. Het patchpaneel is de domeinscheiding tussen RWS en de RWS-afnemer.

Binnen de Dark Fiber-dienstverlening valt het:

- Aanbrengen patchpaneel in 19”-kast (indien noodzakelijk);
- Projectering glasvezel-posities op patchpaneel;
- Aanbrengen label op posities op patchpaneel.

Specifieke leveringsvoorwaarden

Dark Fiber mag uitsluitend worden gebruikt voor het transport van optische transmissiesignalen.
De systemen die daarvoor door de afnemer worden ingezet, moeten voldoen aan de laserveiligheidseisen in IEC 60825-2 met betrekking tot laser class 1 (maximaal vermogen van 10 mW bij 1550 nm of 16 mW bij 1310 nm).

Als het vanwege afstandsoverbrugging noodzakelijk is om meer vermogen toe te passen, dan mogen ook systemen van laser class 1 M of 3 B worden toegepast. Dit mag alleen als deze zijn uitgerust met een (geactiveerde) voorziening die de laser uitschakelt bij een onderbreking in het lichtcircuit. Deze technieken zijn bekend als Automatic Laser Shutdown (ALS), Automatic Power Reduction (APR) en Intelligent Power Reduction (IPR).

Omdat deze technieken niet altijd vastgelegd zijn in internationale normen dienen de specificaties aan SP-O&A ter beoordeling te worden aangeboden. SP-O&A behoudt zich het recht voor om in geval van twijfel deze systemen te testen op bovengenoemde normen en indien nodig consequenties te verbinden aan de uitkomst van die testen.

Transmissiesystemen die in laser class 4 vallen, mogen nooit worden ingezet op Dark Fiber. Dit in verband met de veiligheid van SP-O&A - en andere medewerkers. Er zijn geen eisen gesteld aan de maximale lengte van Dark Fibers.

PDC deel 2: Netwerkdiensten CIV Afnemer

VPN (functionaliteiten)
VPN
Virtual Firewall
DDI
DMZ
Forward Webproxy
Mail Relay
VPN Aansluiting
VPN aansluiting
Draadloze VPN aansluiting
Externe koppeling
LAN Aansluiting
LAN aansluiting type Gebouw
LAN aansluiting type Rekencentrum (VC/VP)
LAN aansluiting type CVR/VOR
LAN aansluiting type Weg- / Waterkant
LAN aansluiting type Onderstation
LAN aansluiting type Offshore
LAN aansluiting type KA, incl. callcenter
WIFI
Eindsysteem
Digitale Video aansluiting
Remote Access groepsprofiel
AAA RAS gebruiker
AAA NAC Profiel
PPP aansluiting
TBMS BUS
Draadloze aansluiting
Overig
Glas Adviezen, Netwerk Adviezen

Tabel 7 IT-netwerkdiensten CIV Klant

Netwerkdiensten CIV Afnemer

Inleiding
Dit deel van de catalogus biedt een overzicht van de diensten welke door afnemers van CIV IRN Infra Netwerken kunnen worden besteld in de categorie VPN, VPN Aansluiting, LAN Aansluiting en Eindsysteem. De uitsluitend door dan wel via CIV IRN Infra Netwerken te bestellen diensten zijn beschreven in deel 1 "Netwerkdiensten CIV IRN Infra Netwerken". Voor vragen hierover kan contact worden opgenomen met de Customer Relationship Manager van CIV IRN Infra Netwerken.

Categorie VPN
Onder de categorie Virtual Private Network (VPN) vallen het VPN en de additionele functionaliteiten op het VPN zoals DDI, DMZ en DMZ Client, Mail Relay en de Virtual Firewall. Om gebruik te kunnen maken van verscheidene functionaliteiten uit de categorieën Eind-systemen, LAN aansluiting en VPN aansluiting wordt gebruik gemaakt van een VPN. De aan-vrager dient aan te geven op welk VPN hij aangesloten wenst te worden.

Virtual Private Networks (VPN's) zijn landelijk beschikbaar en kunnen middels de diensten VPN aansluiting en LAN aansluiting tot op LAN access poort niveau op eindlocaties ontsluiting bieden tot systemen. Optioneel kan het VPN via een Virtual Firewall verbonden worden met andere VPN's en met het internet. Afhankelijk van het type VPN zijn bepaalde standaardvoorzieningen mogelijk, verplicht of beperkt. Het VPN is in twee varianten te bestellen; het any-to-any VPN en het Hub-Spoke VPN. De infra adviseur ondersteunt de besteller bij het maken van de keuze voor een van de types.

VPN any-to any
In dit type VPN is er binnen het VPN transparante communicatie mogelijk tussen alle locaties die aangesloten zijn op het betreffende VPN.

VPN Hub-Spoke
In een Hub-Spoke VPN is rechtstreekse communicatie tussen locaties (zgn. Spokes) uitgesloten. Een VPN aansluiting Spoke kan enkel met de Hub of met externe VPN's communiceren via een Firewall. Dit type VPN is met name bedoeld voor netwerkomgevingen waar verhoogde veiligheid voorop staat. Multicast wordt in een Hub-Spoke VPN niet ondersteund.

De Hub-Spoke functionaliteit is te bestellen door een combinatie van de volgende diensten:
- VPN type Hub-Spoke
- VPN aansluiting type Hub (locatie Primair/Secundair verplicht aangeven wanneer het een CV of ODC locatie betreft)
- VPN aansluiting type Spoke
- VPN FW Policy&Rules

Per VPN type Hub-Spoke worden één of meerdere Spoke aansluitingen en één Hub-functie ondersteund. De Hub-functie is redundant te leveren over twee geografisch gescheiden locaties (primair/secundair). De Hub functie is alleen leverbaar op de locaties Centrale Voorzieningen, ODC en Verkeerscentrales.

Wanneer eenmaal voor een type VPN is gekozen, any-to-any of Hub-Spoke, dan is er geen migratie naar een ander type mogelijk. Er kan alleen naar een ander type worden overgestapt dmv bestellen van de activiteiten ''opheffen'' van het bestaande type VPN en ''aanvragen'' van het gewenste type VPN.

Een VPN biedt de mogelijkheid binnen een besloten en logisch gescheiden netwerk op veilige, betrouwbare wijze bedrijfsinformatie en applicaties te benaderen én informatie te delen tussen geografisch gescheiden netwerken als binnen één dedicated netwerk. Het VPN is rand-voorwaardelijk om communicatie tussen eindsystemen op twee RWS locaties en tussen RWS en niet-RWS eindlocaties mogelijk te maken. Afhankelijk van het doel van het VPN dienen de in onderstaande tabel weergegeven functionaliteiten verplicht of optioneel afgenomen te worden om gebruik te maken van de diensten beschreven in de categorieën Eindsystemen, LAN aansluiting en VPN aansluiting.

VPN functionaliteiten		
Functionaliteit	**Standaard / Verplicht/Optioneel**	**Specificatie**
Managed IP-VPN	Standaard	Any to any, of Hub Spoke, IP connectiviteit tussen op de RWS backbone ontsloten locaties. Routering binnen een virtueel netwerk in de RWS backbone met een door de beheerder SP-IB toegewezen IPv4-adresruimte
Externe koppeling	Optioneel	In- en/of uitgaand verkeer naar aangesloten externe netwerken (Categorie VPN Aansluiting)
Internet Access met gefilterd Internet	Standaard	Veilige en gecontroleerde toegang tot het Internet voor in- en/of uitgaand internet verkeer voor interactie met partijen buiten de RWS organisatie.
Virtual Firewall	Verplicht	Beschermt de integriteit en vertrouwelijkheid van het VPN middels een firewall. De Virtual Firewall bepaalt per VPN welke communicatiestromen zijn toegestaan en blokkeert alle niet expliciet toegestane communicatie(patronen). Ieder VPN heeft een eigen Virtual Firewall.
IDS/IPS	Standaard	IDS controleert het verkeer tussen VPN's en van en naar het Internet op schadelijke aspecten en IPS blokkeert volgens ingestelde policies.
Mail Relay	Optioneel	Benodigd om e-mail te ontvangen van en versturen naar externe netwerken via smtp protocol. Mail Relay heeft daarbij verschillende beveiligingsvoorzieningen zoals controle op de reputatie van een systeem op Internet,

		versleuteling van email transport en inhoudelijke controle van berichten.
DNS (DDI)	Verplicht bij Internet Access	De functie DNS levert 'name services' aan de, binnen het VPN, aangesloten systemen op basis van het DNS protocol en voorziet in DNS name resolving van Internet systemen.
DHCP (DDI)	Standaard	De functie DHCP levert een centrale voorziening om clients (en hosts) binnen het VPN op dynamische wijze van netwerkinstellingen te voorzien middels DHCP (Dynamic Host Configuration Protocol)
IPAM (DDI)	Standaard	Address Management geeft geautoriseerde RWS medewerkers de mogelijkheid om de IP-gerelateerde informatie vast te leggen en hier context aan te geven. Zo wordt IP-informatie beter bruikbaar als ondersteuning bij audits, kwaliteitscontrole en incidenten.
Gedelegeerd beheer (DDI)	Standaard	Geeft RWS medewerkers en RWS onderaannemers de mogelijkheid om de 'IP-ruimte' waarvoor zij verantwoordelijk zijn te beheren.
Remote Access	Optioneel bij Internet Access	Remote Access door personen (Internet) naar RWS systemen ten behoeve van remote beheer.
QoS	Optioneel	Congestiebeheersing door end to end Quality Of Service (QoS) binnen een VPN. QoS is niet overal en altijd leverbaar.
NTP	Standaard	De functie NTP levert een centrale klok waarmee eindsystemen binnen het VPN hun tijd kunnen synchroniseren via het NTPv4 protocol.

Tabel 8 VPN functionaliteiten

Beheer VPN

RWS onderkent de volgende onderdelen van de categorie VPN:

1. VPN
2. Virtuele Firewall
3. DDI – DHCP & DNS
4. DDI – IPAM
5. DDI – Gedelegeerd beheer
6. DDI – NTP
7. DMZ en DMZ client
8. Forward Webproxy
9. Mail Relay

Quanza IB voert het beheer uit op deze VPN types conform onderstaande SLA.

MATRIX VPN											
Diensten	Beschikbaarheid							Storingshersteltijd in 95% van de gevallen			
	Enkel			Dubbel			VPN	Service Window Kantoortijden		Service Window"24/7"	
	99,5%	99,9%	99,95%	99,98%	99,99%	99,99%	99,999%				
	Onbeschikbaarheid per jaar										
	ca 1d20u	ca 8u45m	ca 4u28m	ca 4u28m	ca 1u45m	ca 0u52m	ca 5m15s	8 uur	4 uur	8 uur	4 uur
VPN							V				V
Virtual Firewall			V								V
DDI - DHCP & DNS*	V					V					V
DDI - IPAM		V									V
DMZ en DMZ Client					V						V
Forward Webproxy				V							V
Mail Relay				V							V

* De centrale beschikbaarheid van DDI componenten is 99,99%, deze zijn dubbel uitgevoerd en hiertoe geplaatst over 2 fysiek geografisch gescheiden locaties. De beschikbaarheid over de gehele keten is afhankelijk van de overige bouwstenen waar de afnemer gebruik van maakt.

Tabel 9 Dienstenmatrix VPN – diensten

Bestelbare items en levertijd

Voor het VPN gelden de in onderstaande tabel weergegeven bestelbare items met bijbehorende standaard in werkdagen weergegeven levertijden. De levertijden voor verschillende bestelbare items lopen parallel, niet sequentieel. De dienst VPN is niet apart door afnemers te bestellen.

VPN			
nmalige dienst	**Toelichting**	**evertijd in werkdagen oor SP-O&A)**	**SSR oor SP-IB)**
VPN			
Aanvragen	Leveren nieuw VPN	20	
Opheffen	Opheffen VPN	20	
Wijzigen	Wijzigen instelling bestaand VPN op afstand	10	
Aanvragen VPN QoS Profiel	Realiseren QoA profiel op VPN	20	
Virtual firewall			
Aanvragen	Leveren nieuwe Firewall	10	
Opheffen	Opheffen Firewall	10	
Wijzigen	Wijzigen/toevoegen/verwijderen Firewall rules	5	Ja
Wijzigen	Wijzigen/toevoegen/verwijderen Firewall rules met spoed	1	Ja
DDI – DHCP Scope			
Aanvragen	Aanvragen DHCP scope (IP range centrale distributie)	10	
Opheffen	Opheffen DHCP scope (IP range centrale distributie)	10	
Wijzigen	Wijzigen DHCP scope (IP range centrale distributie)	10	
Aanvragen toegang	Aanvragen toegang op bestaande DHCP scope RW/RO	10	
Opheffen toegang	Opheffen toegang op bestaande DHCP scope RW/RO	10	
DDI – DNS Domeinnaam			
Aanvragen	Leveren DNS domeinnaam/record (Host/Prt/A/CNAM/MX)	10	
Opheffen	Opheffen DNS domeinnaam/record (Host/Prt/A/CNAM/MX)	10	

VPN			
Wijzigen	Wijzigen DNS domeinnaam/record (Host/Prt/A/CNAM/MX)	5	
DDI – Gedelegeerd beheer			
Aanvragen	Aanvragen DNS/DHCP/IPAM gedelegeerd beheer groep	10	
Opheffen	Opheffen DNS/DHCP/IPAM gedelegeerd beheer groep	10	
Wijzigen	Wijzigen DNS/DHCP/IPAM gedelegeerd beheer groep	10	
DDI – IPAM			
Aanvragen	Aanvragen/opvoeren van een (nieuw) netwerk, of nieuwe eigenaren van bestaand netwerk	10	
Opheffen	Opheffen van netwerk informatie van netwerken binnen een VPN	10	
Wijzigen	Opvoeren/update van host informatie binnen een netwerk	5	
DMZ en DMZ Client			
Aanvragen	Aanvragen DMZ	30	
Opheffen	Opheffen DMZ	10	
Aanvragen Client	Aanvragen Client aansluiting	20	
Opheffen Client	Opheffen Client aansluiting	10	
Wijzigen Client	Wijzigen Client aansluiting	5	
Forward Webproxy			
Aanvragen	Aanvragen Forward Webproxy	In overleg	
Opheffen	Opheffen Forward Webproxy	In overleg	
Wijzigen	Wijzigen Forward Webproxy	In overleg	
Mail Relay			
Aanvragen	Aanvragen Mail Relay	In overleg	
Opheffen	Opheffen Mail Relay	In overleg	
Wijzigen	Wijzigen Mail Relay	In overleg	

Tabel 10 Bestelbare items VPN diensten

Levering gebeurt door Quanza – O&A met uitzondering van de Standaard Service Requests, die door Quanza – IB worden uitgevoerd. Voor alle werkzaamheden op locatie wordt SPIE aangestuurd.

Categorie VPN aansluiting
De categorie Virtual Private Network (VPN) aansluiting beschrijft verschillende type aansluitingen: de **VPN aansluiting** (bedraad middels RWS glasverbindingen of huurlijnen), de **Draadloze VPN aansluiting** en de **VPN Aansluiting ten behoeve van derde partijen** (externe koppeling).

Beheren IT-netwerkdiensten (VPN-aansluitingen)
Quanza IB voert het beheer uit op deze VPN diensten conform onderstaande SLA.

Dienstenmatrix VPN Aansluiting										
Type VPN Aansluiting	Bandbreedte	Beschikbaarheid					Storingshersteltijd in 95% van de gevallen			
		Enkel	Dubbel**	Redundant	Ipsec	Ipsec MCPE	Service Window Kantoortijden			Service Window"24/7"
		99,50%	99,80%	99,99%	99,99%	98%				
		Onbeschikbaarheid per jaar								
		ca 1d20u	ca 17u30m	ca 0u52m	ca 0u52m	ca 7d7u	8 uur	4 uur	8 uur	4 uur
Bedraad ****	< 10Mb (128/256/384 /512/640/768 /896 Kbps) (1/1.25/1.5/1. 75/2/3/4/5/6/ 7/8/9 Mbps)	V	V	V						
	10 Mb tot 1 Gb (10/20/30/40/ 50/60/70/80/ 90/100/200/ 300/400/500/ 600/700/800/ 900 Mbps)	V	V	V				V		V
	!Gb tot en met 10Gb 91/2/3/4/5/6/ 7/8/9 Gbps)	V	V	V						
Draadloos	2G of 4G ***	V	V*							V
Externe koppeling	Geen garantie	V	V	V	V	V				
RKN		V		V			V			V

*	Beschikbaar als Ruggedized (Router geschikt voor ongeconditioneerde ruimte)
**	Variant wordt beperkt ingezet. Indien het niet mogelijk is dubbel te ontsluiten, dan is het mogelijk de enkele variant dubbel uit te voeren middels een mobiele backup. Voor de mobiele backup is beschikbaarheid niet gegarandeerd.
***	Afhankelijk van ingezette hardware, geen bandbreedte garantie.
****	Dit betreft een bruto bandbreedte van huurlijnen. De netto bandbreedte bestaat uit de bruto bandbreedte minus een eventuele tunneloverhead van max 8Kbps

Tabel 11 Dienstenmatrix categorie VPN - aansluiting

Bestelbare items en levertijd

Voor de VPN aansluiting gelden de in onderstaande tabel weergegeven bestelbare items en bijbehorende levertijden.

VPN Aansluiting			
Eenmalige dienst	**Toelichting**	**Levertijd in werkdagen (door SP-O&A)**	**SSR (door SP-IB)**
Bedraad			
Aanvragen	Leveren 1e VPN aansluiting (levering en installatie verbinding + apparatuur)	90	
Opheffen	Opheffen laatste VPN aansluiting (opheffen verbinding + verwijderen apparatuur)	10	
Activeren	Activeren nieuwe VPN aansluiting (op afstand) op bestaand apparaat waar al tenminste één andere VPN aansluiting is aangesloten.	5	
Deactiveren	Deactiveren VPN aansluiting (op afstand) waarna er nog minstens één VPN aansluiting op het apparaat overblijft.	5	
Toeslag Hub-Spoke	Toeslag voor het activeren of deactiveren van de Hub-Spoke functionaliteit op een VPN aansluiting	x	

VPN Aansluiting			
Wijzigen	Wijzigen optie instelling(en) bestaande VPN aansluiting (op afstand)	5	
Aanvragen back-up Mobiel	Leveren back-up Mobiel	20	
Opheffen back-up Mobiel	Opheffen back-up Mobiel	10	
VPN Aansluiting Connect en Inter Connect			
Activeren – LO Enkelvoudig (99,5%)	Activeren extra VPN aansluiting op afstand	In overleg	
Activeren – LO Redundant (99,99%)	Activeren extra VPN aansluiting op afstand	In overleg	
Deactiveren	Deactiveren extra VPN aansluiting op afstand	In overleg	
Wijzigen	Wijzigen instellingen bestaande VPN aansluiting op afstand	In overleg	
Draadloos			
Aanvragen	Leveren 1e VPN aansluiting op apparaat (met en zonder installatie(*))	90	
Opheffen	Opheffen draadloze VPN aansluiting (met en zonder installatie(*))	90	
Wijzigen	Wijzigen configuratie	5	
Activeren	Activeren extra VPN aansluiting op afstand	5	
Deactiveren	Deactiveren extra VPN aansluiting op afstand	5	
Wijzigen	Wijzigen instelling bestaande VPN aansluiting op afstand	10	
Aanvragen Dekkingsmeting Mobiel	Leveren dekkingsmeting mobiele ontvangst inclusief rapport	5	
Externe Koppeling			
Aanvragen IPsec	Leveren IPsec verbinding	10	
Opheffen	Opheffen IPsec verbinding	10	
Wijzigen	Wijzigen IPsec verbinding	5	Ja
Aanvragen MCPE	Leveren Managed CPE met apparaat Aanvragen beheerde router Verplicht bij externe koppeling op basis van vaste verbinding, optioneel bij IPsec	90	
Opheffen MCPE	Opheffen verbinding met en het opruimen van beheerde router	20	
Wijzigen MCPE	Het aanbrengen van wijzigingen in de routering in de MCPE(s)	10	
Aanvragen vaste verbinding(**)	Aanvragen ON2013 verbinding (i.c.m. MCPE)	90	
Opheffen vaste verbinding (**)	Opheffen ON2013 verbinding (i.c.m. MCPE)	10	

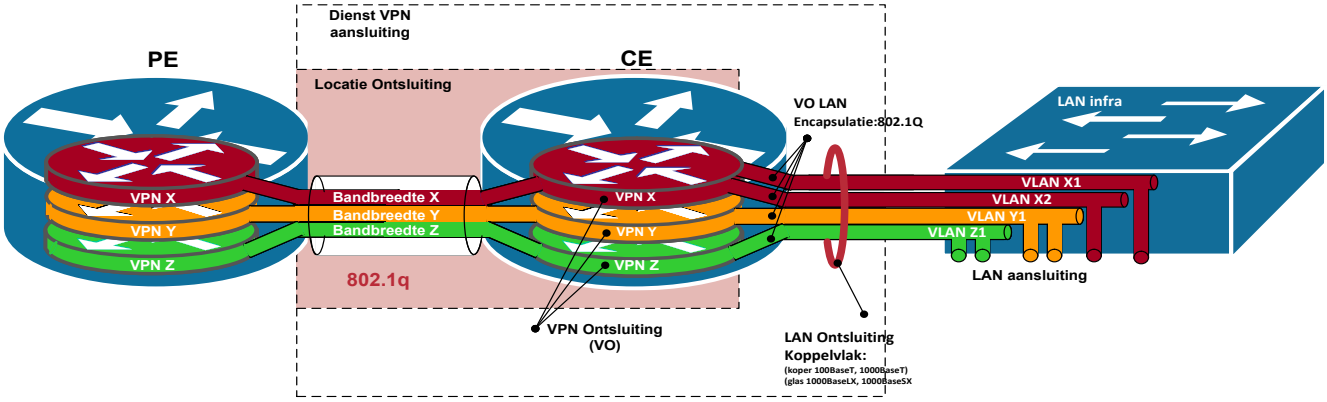
VPN Aansluiting			
RKN aansluiting			
Aanvragen	Van toepassing wanneer hardware geleverd moet worden of op een nieuw VPN moet worden aangesloten	90	
Activeren	Activeren extra VPN aansluiting op afstand	5	
Wijzigen	Wijzigen instelling bestaande VPN aansluiting op afstand	5	
Deactiveren	Deactiveren VPN aansluiting op afstand	5	
Opheffen	Van toepassing wanneer hardware gede-installeerd moet worden of wanneer door opzegging van de laatste aansluiting tevens een VPN moet worden gedeactiveerd	10	

Tabel 12 Bestelbare items categorie VPN aansluiting

Levering gebeurt door Quanza – O&A met uitzondering van de Standaard Service Requests, die door Quanza – IB worden uitgevoerd. Voor alle werkzaamheden op locatie wordt SPIE aangestuurd.

VPN aansluiting Bedraad

De VPN aansluiting omvat de fysieke en logische koppeling van een VPN met de LAN infrastructuur op een RWS -of RWS klantlocatie zoals schematisch is weergegeven in Figuur 7.



Figuur 7 Schematische weergave van de VPN aansluiting

De VPN aansluiting dient als ontsluiting tussen de RWS backbone en de LAN infrastructuur waarop eindsystemen zijn aangesloten. Op dezelfde hardware en transmissie kunnen meerdere VPN aansluitingen geleverd worden. Deze VPN aansluitingen zijn een logisch component op de fysieke hardware.

De VPN aansluiting is de aansluiting middels fysieke transmissie (RWS glas, huurlijnen of Dark Fiber Derden*) en biedt de volgende functies en opties ten behoeve van de LAN infrastructuur op een RWS of RWS klant locatie:

- Toegang tot een bestaand VPN;
- 100MB(UTP), 1GE (UTP of Glas) of 10GE (Glas) fysiek koppelvlak naar LAN infrastructuur;
- DHCP relay functionaliteit ten behoeve van DHCP;

- Wake on LAN;
- Eén of meerdere VLAN's, met per VLAN een IPv4 gateway adres en eventueel routering.

* Inzet van een Dark Fiber van andere (overheids-) partijen door RWS is in uitzonderlijke gevallen mogelijk wanneer Eigen Glas niet beschikbaar is. Hiervoor is expliciete goedkeuring van de domeineigenaar van Infra Netwerken nodig en is uitsluitend te bestellen door medewerkers van CIV IRN Infra Netwerken.

Functies en opties VPN aansluiting

De verschillende functies en opties voor de VPN aansluiting zijn hieronder beschreven.

A. VPN aansluiting type hub of type spoke

Wanneer er een nieuw VPN besteld wordt, kan men de keuze maken voor een any-to-any of een Hub-Spoke-VPN. Wanneer gekozen is voor een VPN type Hub-Spoke zal er per locatie aangegeven moeten worden bij de VPN aansluitingen of dit een Hub of een Spoke locatie betreft. Bovendien zal voor dit type VPN aansluiting per locatie tevens de activiteit toevoegen Firewall rule moeten worden besteld.

- VPN Aansluiting Type Spoke; Spokes zijn decentrale knooppunten die verbonden zijn met maximaal één Hub. Spokes kunnen niet onderling communiceren, alleen via de hub.
- VPN Aansluiting Type Hub; de Hub is het belangrijkste knooppunt in het Hub-Spoke netwerk. Het dient als centrale punt voor het beheer, de controle en de distributie van gegevens. En heeft meer bandbreedte dan de Spokes. De Hub-locaties worden beperkt tot de Centrale Voorzieningen, Verkeerscentrales en ODC locaties.

De VPN Aansluitingen type Hub en Spoke zijn met een gelijke beschikbaarheid te bestellen als een standaard VPN Aansluiting (enkel 99,5%, dubbel 99,8%, redundant 99,99%).

B. Bandbreedte

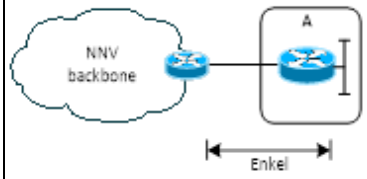
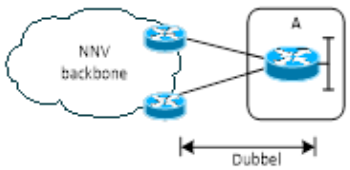
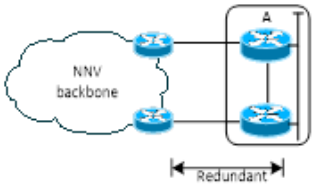
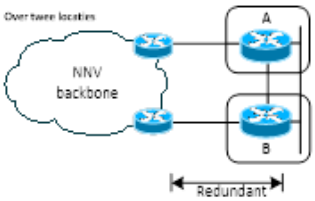
Op een Router/CE worden naast de Klant-VPN's maximaal 3 Beheer-VPN's geconfigureerd:
- Ten behoeve van de Router [CE:MGT]
- Ten behoeve van KA LAN Switch(es) [LAN:MGT]
- Ten behoeve van Overige LAN Switch(es) [EXT:MGT]

De bandbreedte voor een Beheer-VPN is afhankelijk van de bandbreedte van de VPN Ontsluiting:
- 128Kb voor 2Mb en 10Mb
- 1Mb voor 100Mb
- 10Mb voor 500Mb, 1Gb en 10Gb

De bandbreedte optie komt daadwerkelijk overeen met de geconfigureerde bandbreedte (in geval dat shaping mogelijk is).
Er wordt niet overboekt. Dat betekent dat de optelsom van de Klant-VPN's en Beheer-VPN's bandbreedtes samen kleiner of gelijk aan de bandbreedte van de VPN ontsluiting moet zijn (geldig voor zowel RWS Glas als ontsluiting middels huurlijn).

C. Beschikbaarheid

De VPN Aansluiting heeft vier beschikbaarheidsopties waarvan er drie zijn weergegeven in Figuur 8. De beschikbaarheid op locatie wordt bepaald door de VPN Aansluiting met de hoogste beschikbaarheidseis. Een beschikbaarheid van 99,999% kan uitsluitend worden aangevraagd via RWS CIV IRN Infra Netwerken als maatwerk.

Beschikbaarheid VPN Aansluiting		
Enkel	**Dubbel**	**Redundant**
99,5% 	99,8% 	99,99%  99,99% 
middels één tracé ontsloten naar één backbone router.	middels geografisch gescheiden tracés ontsloten naar twee geografisch gescheiden backbone routers.	

Figuur 8 Beschikbaarheid VPN Aansluiting

D. DHCP relay

Middels Dynamic Host Configuration Protocol (DHCP) kunnen eindsystemen binnen een LAN segment (VLAN) dynamisch van IP adressen worden voorzien. Met de DHCP relay functie kunnen per LAN segment de hiertoe toegewezen DHCP servers worden ingesteld. Er wordt een maximum van 3 DHCP servers per LAN segment ondersteund.

E. WoL

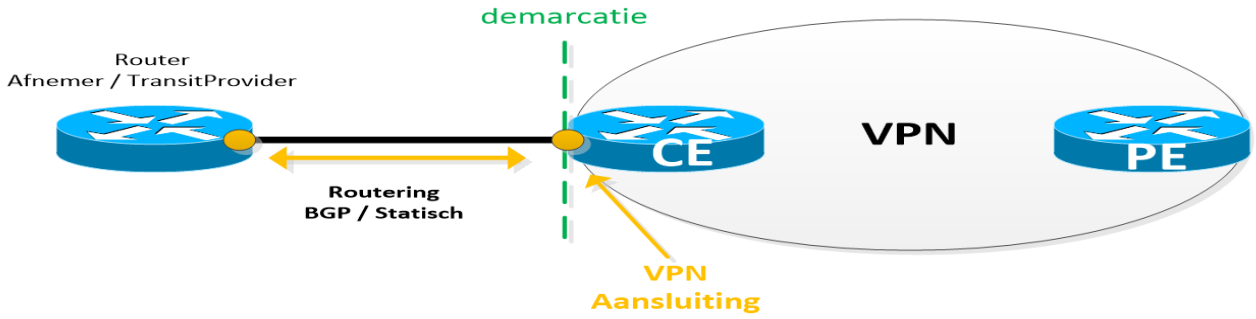
Wake on LAN (WoL) biedt de mogelijkheid netwerk devices op afstand te starten, bijvoorbeeld voor onderhouds- werkzaamheden.

F. Routering

Door middel van een LAN ontsluiting wordt een fysieke koppeling met de LAN infrastructuur tot stand gebracht. Deze wordt geleverd als een laag 3 interface. Elk LAN domein wordt op een gescheiden CE domein gekoppeld met een unieke LAN Ontsluiting.
In de dienstverlening worden vier routeringsopties onderscheiden: standaard, statisch, dynamisch type “Connect” en dynamisch type “InterConnect”. Deze worden hieronder nader toegelicht.

1. Standaard routering

Standaard wordt routering ingericht doormiddel van een VLAN-interface op de LAN aansluiting (VPN Ontsluiting LAN) zoals weergegeven in Figuur 9. Er kunnen meerdere VPN Ontsluiting (VO) LANs per VPN Aansluiting worden ingericht. De VPN Aansluiting is beperkt tot een enkel LAN domein.

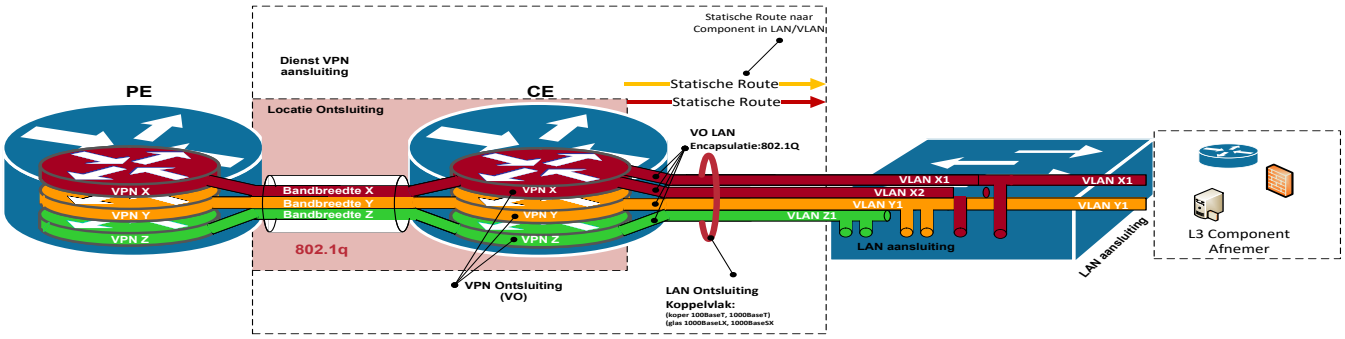


Figuur 9 Standaard routering VPN Aansluiting

Afwijkend kan routering naar een Laag 3 component op het Local Area Network (LAN) van de VPN-Aansluiting ingericht worden. Deze routering kan naar keuze statisch of dynamisch geleverd worden.

2. Statische routering

Indien gewenst is het ook mogelijk routering naar een component achter de VPN Aansluiting toe te passen doormiddel van statische routering zoals weergegeven in onderstaand figuur. Deze optie maakt het mogelijk om een component op het LAN aan te sluiten om zo een extern netwerk te kunnen benaderen. Het is niet toegestaan om tussen RWS netwerken te routeren.

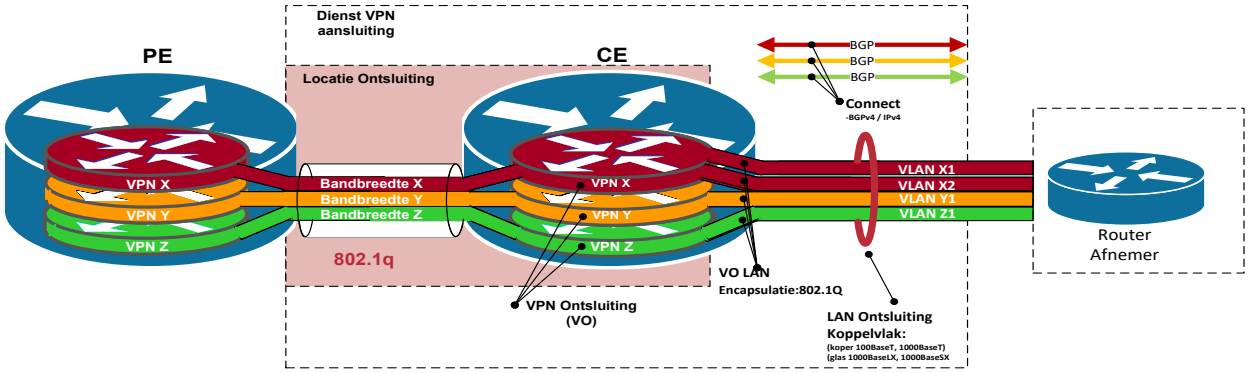


Figuur 10 Statische routering VPN Aansluiting

Voor meer informatie omtrent deze optie kan contact opgenomen worden met Service Management.

3. Dynamisch: VPN Aansluiting Connect

De VPN Aansluiting Connect, zoals weergegeven in onderstaand figuur, maakt het middels dynamische routering mogelijk netwerk-informatie uit te wisselen tussen het VPN en de afnemer. Deze optie is beschikbaar voor afnemers die geen transit-functionaliteit vervullen.



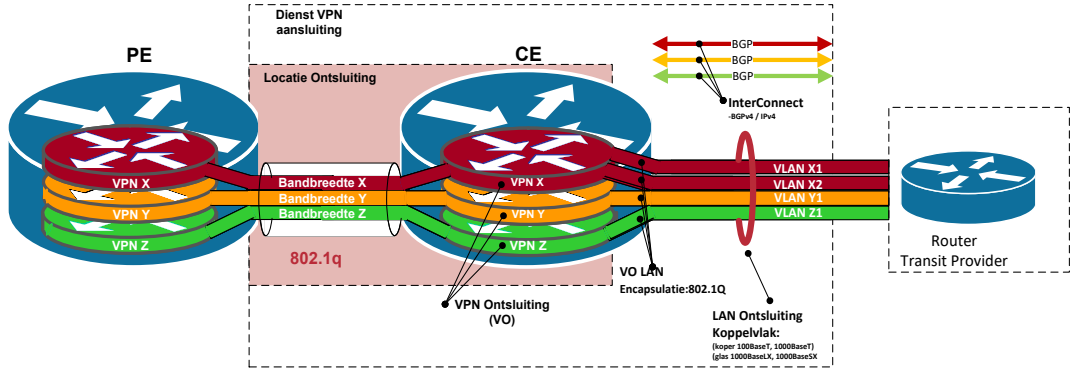
Figuur 11 Dynamische routering - VPN Aansluiting Connect

Voor een VPN-Aansluiting Connect op basis van dynamische routering zijn onderstaande uitgangspunten van toepassing:

- Klantapparatuur wordt direct op de LAN Ontsluiting aangesloten;
- Er wordt gebruik gemaakt van BGPv4. Hiermee is deze optie beperkt tot IPv4;
- Per VPN Aansluiting wordt één BGP-sessie toegestaan;
- Bij een redundante Locatie Ontsluiting is een redundante BGP koppeling mogelijk, waarbij één van de koppelingen als primair wordt behandeld en de tweede als secundair (back-up). De afgenomen bandbreedte geldt voor de gehele redundante koppeling;
- Toepassing van de BGP Attributen AS-Path prepending en MED wordt ondersteund;
- Standaard adverteert de VPN Aansluiting de gehele routeringstabel van het VPN. Optioneel is het mogelijk om een default-route toe te voegen of enkel een default route te adverteren naar de transit-provider;
- De afnemer van de VPN Aansluiting dient gebruik te maken van een Publieke AS. Indien de afnemer hier niet over beschikt wijst de Service Provider van RWS CIV IRN Infra Netwerken een Private AS toe;
- De afnemer mag niet als 'transit' fungeren voor andere partijen;
- Standaard worden max. 100 IPv4 routes van de afnemer geaccepteerd. In overleg kan dit worden aangepast;
- De afnemer van de VPN Aansluiting geeft de IP-netwerken op die worden geadverteerd naar de VPN Aansluiting. De Afnemer kan een ruimer IP-subnet opgeven en daarbinnen kleinere IP-netwerken adverteren (Bijvoorbeeld 172.16.0.0/16 opgeven waarbinnen enkel 172.16.1.0/24 en 172.16.2.0/24 worden geadverteerd door de Afnemer naar RWS);
- De IP-netwerken van de afnemer moeten conformeren aan het IP-plan van het VPN;
- Multicast wordt niet ondersteund.

4. Dynamisch: VPN aansluiting InterConnect

De VPN aansluiting InterConnect, zoals weergegeven in onderstaand figuur, is een optie op de VPN aansluiting om middels dynamische routering netwerk-informatie uit te wisselen met het VPN en wordt gebruikt om het RWS netwerk te koppelen met andere transit/provider netwerken.



Figuur 12 Dynamische routering - VPN Aansluiting InterConnect

De VPN-Aansluiting InterConnect koppelt een VPN op het domein van RWS met een VPN op het domein van de transit-provider. Route uitwisseling vindt plaats middels BGPv4.

De volgende uitgangspunten zijn van toepassing:

- Apparatuur van de transit-provider wordt direct op de LAN Ontsluiting aangesloten;
- Er wordt gebruikgemaakt van BGPv4. Hiermee is deze optie beperkt tot IPv4;
- Per VPN aansluiting wordt één BGP-sessie toegestaan.
- Bij een redundante Locatie Ontsluiting is een redundante BGP koppeling mogelijk, waarbij één van de koppelingen als primair wordt behandeld en de tweede als secundair (back-up). De afgenomen bandbreedte geldt voor de gehele redundante koppeling;
- Toepassing van de BGP Attributen AS-Path prepending en MED wordt ondersteund;
- Standaard adverteert de VPN Aansluiting de gehele routeringstabel van het VPN. Optioneel is het mogelijk om een default-route toe te voegen of enkel een default route te adverteren naar de transit-provider;
- De VPN-aansluiting fungeert als transitkoppeling. Het BGP AS-plan wordt in overleg afgestemd;
- Publieke BGP AS-nummers worden standaard geaccepteerd. Gebruik van Private AS-nummers
- worden vooraf afgestemd;
- Standaard worden maximaal 1000 IPv4-routes per VPN geaccepteerd vanuit de transit-provider. In overleg kan deze waarde verhoogd worden;
- De IP-netwerken die door de transit-partij worden geadverteerd maar RWS dienen aan het IP-plan van het VPN te voldoen;
- Multicast wordt niet ondersteund.

VPN aansluiting type RKN (Rijkswaterstaat Koppel netwerk)

Rijksoverheden en Overheden maken gebruik van verschillende Wide Area Netwerken met als doel een communicatie-infrastructuur te realiseren. Optimale samenwerking tussen alle

(Rijks)overheids-partijen is cruciaal, waarbij overdracht en gebruik van informatie tussen partijen een belangrijk uitgangspunt is.

Het Rijkswaterstaat Koppel Netwerk (RKN) is aangesloten op het centrale Koppelnet Publieke Sector (KPS) en biedt en ontsluiting naar koppelnetwerken van andere (Rijks)overheidspartijen op basis van het Diginetwerk Afsprakenstelsel. Tevens biedt RKN ontsluiting naar het koppelnet van DMO RON2.0 (WAN-I, DCI, Rijksweb en DWR).

Partners van RWS kunnen met de bouwsteen Rijkswaterstaat Koppel Netwerk (RKN) als "aangesloten overheidsorganisatie" aangesloten worden op het Rijkswaterstaat Koppel Netwerk (RKN) en transit aanvragen naar (een) andere aangesloten overheidsorganisatie(s).

De bouwsteen Rijkswaterstaat Koppel Netwerk (RKN) is een integratie-dienst, waarbij de bouwsteen 'VPN' en de bouwsteen 'VPN aansluiting' worden samengevoegd. Alle service management communicatie (eenmalige diensten, incidenten, rapportages, capaciteitsmanagement etc.) vindt plaats o.b.v. de RKN-bouwsteen.

Nieuwe transit providers kunnen via de Service Manager worden toegevoegd op basis van RFI (conform het SPM-proces) en nieuwe transit VPN's kunnen worden aangevraagd op basis van de PDC dienst RKN.

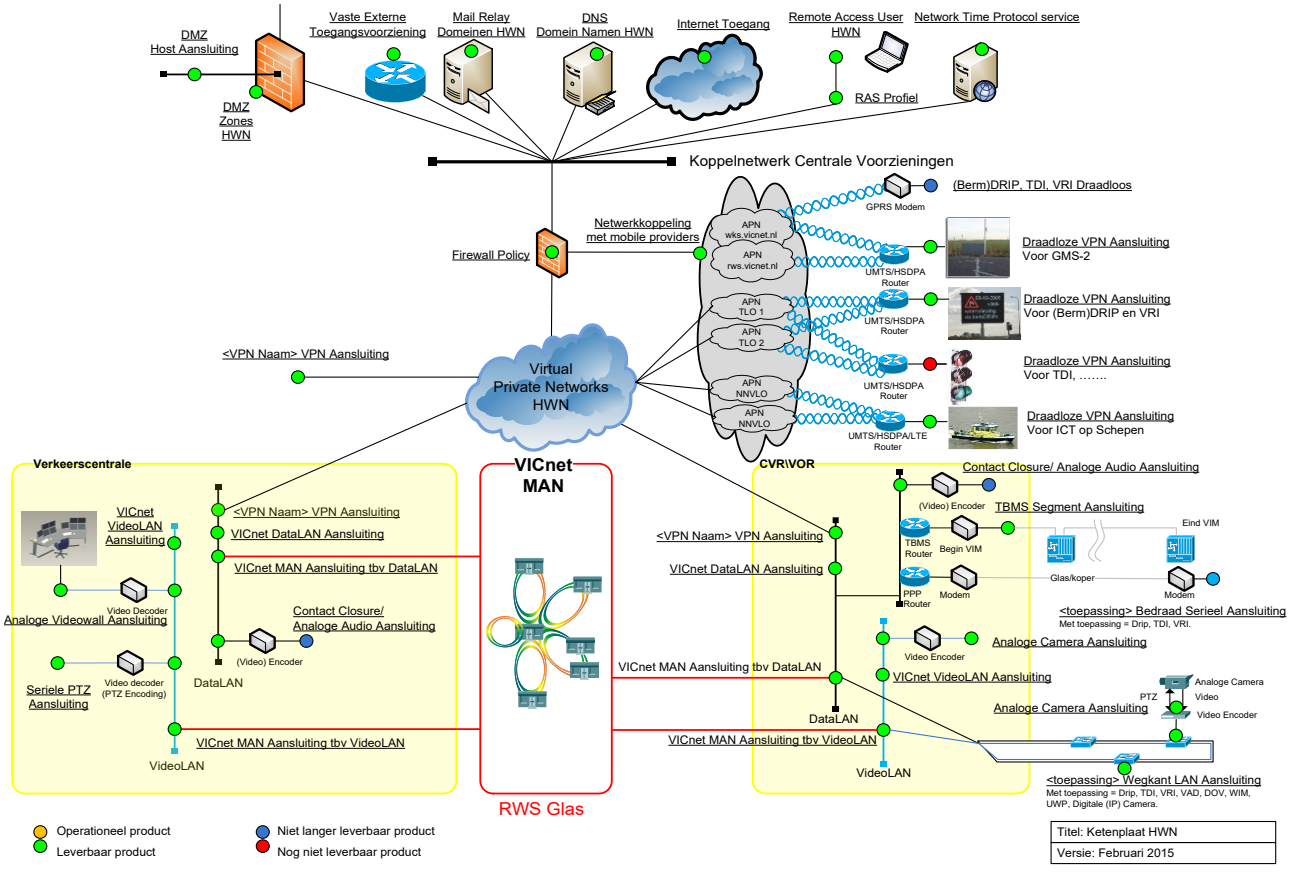
Voor de afnemers van diensten over het RKN-netwerk wordt een VPN aansluiting. Enkelvoudig gerealiseerd op één RWS ODC-locatie of een VPN Aansluiting Redundant over de RWS ODC-locaties AM2/AM3. Per afnemer wordt per RWS ODC-locatie één fysieke interface beschikbaar gesteld welke meerdere logische VPN-aansluitingen kan leveren.

De oplossing voorziet in statische of dynamische routering aan de kant van de afnemers. De verantwoordelijkheid van SP-O&A eindigt op de patchpanelen waarop de apparatuur van RWS is afgewerkt.

Maandelijkse rapportage op incident, problem, availability, capacity en changes per deelnemer per koppeling aan de SLM van RWS. Naast een klantrapportage wordt ook een totaalrapportage op de interface aan de providerkant voor capacity management geleverd.

VPN aansluiting type Draadloos

De draadloze VPN aansluiting is de mobiele en logische koppeling van een VPN met de LAN infrastructuur op een RWS -of RWS klantlocatie zoals schematisch is weergegeven in Figuur 13 en is inzetbaar om zowel locaties als apparaten aan te sluiten. De aansluiting bestaat uit een draadloze router voorzien van mobiele SIM-kaart(en).



Figuur 13 Schematische weergave draadloze VPN Aansluiting

De Draadloze VPN aansluiting biedt dezelfde functionaliteiten als de VPN aansluiting zoals beschreven in bovenstaande paragraaf met afwijkende beschikbaarheid. De Draadloze VPN aansluiting is niet geschikt voor missiekritieke systemen. Door het gebruik van publieke draadloze infrastructuur kan niet aan BIV-normen worden voldaan. Bovendien is gebruik van Multicast niet toegestaan.

Aanvullend gelden de volgende functionaliteiten:

- Transmissie 2G/4G (op schepen wordt geen gebruik gemaakt van 2G transmissie);
- Single SIM voor standaard beschikbaarheid (legacy, niet bestelbaar) of Dualprovider/ Dual SIM voor hogere beschikbaarheid;

- In ongeconditioneerde omgevingen wordt een Ruggedized router geleverd. Langs de weg kant is dit verplicht.

De dienst kent de volgende eigenschappen:

- Simkaarten worden altijd meegeleverd met de beheerde router, andere Simkaarten mogen niet gebruikt worden;
- Afhankelijk van de dekkingsgraad van mobiel zijn er verschillende antenne opties beschikbaar;
- Afnemer kan ervoor kiezen de installatie door de RWS aannemer te laten uitvoeren;
- Voor inbouw in weg- of waterkanttoepassingen gelden veelal specifieke montagevoorschriften die beschikbaar zijn op de VPR.

SIM-kaarten

Bij een draadloze VPN aansluiting wordt de connectiviteit verzorgd met behulp van twee SIM-kaarten. In verband met de business continuity eisen is er een primaire en een secundaire SIM-kaart nodig bij twee verschillende mobiele providers. Onder het contract ON2013 zijn dit Vodafone (primair) en KPN (secundair). In het nieuwe contract CDR2023 zijn dit ODIDO (primair) en Vodafone (secundair).

(*) "Met installatie" betekent, dat de installatie door SPIE gebeurt; "zonder installatie" betekent, dat de SPIE de hardware voorbereidt tot en met staging, maar dat de installatie zelf door een lokale aannemer gebeurt.

VPN aansluiting type externe koppeling

De dienst Externe Koppeling maakt het mogelijk om een niet-RWS-netwerk op een vaste locatie veilig permanent te koppelen met het RWS-netwerk. Hiermee is permanente beveiligde transparante netwerkcommunicatie mogelijk.
Toepassingen hiervoor zijn bijvoorbeeld machine-to-machine communicatie zoals beheersystemen van derde partijen die directe en transparante koppeling tot de door hen beheerde systemen op het RWS-netwerk nodig hebben.
Afhankelijk van de gebruikte transporttechnologie en al dan niet toegepaste redundantie kunnen er SLA's gegeven worden op de beschikbaarheid van en bandbreedte voor deze communicatie.

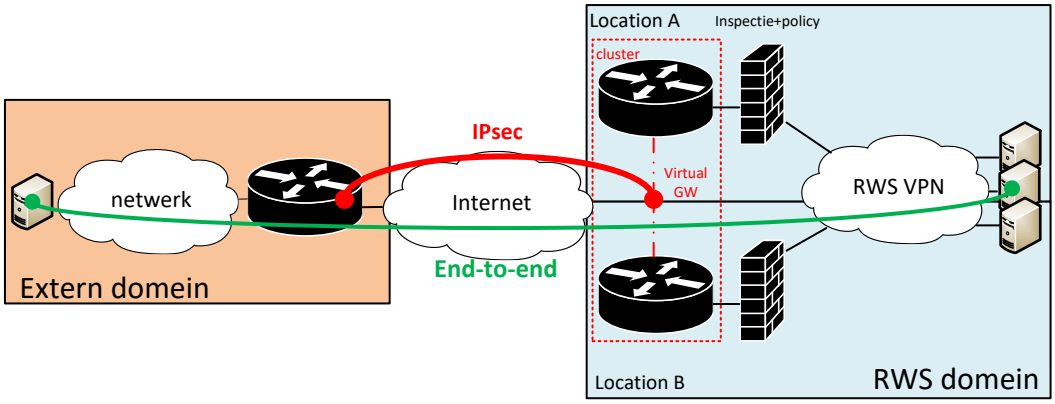
De Externe Koppeling maakt het mogelijk om via een (un)trusted netwerk (bv internet) veilig een niet RWS locatie te ontsluiten naar het RWS netwerk. De vertrouwelijkheid en integriteit van de data wordt gewaarborgd door gebruik te maken van een overlay techniek op basis van IPsec waarin de data versleuteld verstuurd wordt tussen RWS en de aangesloten partij. Er kan ook gekozen worden om een externe koppeling te realiseren via een vaste VPN aansluiting die wordt gekoppeld aan het RWS netwerk.

De externe partij kan er voor kiezen eigen apparatuur in te zetten die logisch wordt aangesloten op het RWS netwerk. Deze partij zal zich wel moeten conformeren aan de interfaces (Zie hfst 3) gesteld vanuit SP-O&A, hierbij moet gedacht worden aan de communicatie protocollen en encryptie standaarden om de data veilig te kunnen

transporteren. Deze interfaces kunnen van tijd tot tijd worden aangepast als er bv nieuwe standaarden zijn voor de gebruikte encryptiemethoden. Van de aangesloten partij mag worden verwacht dat deze mee gaat met deze nieuwe voorwaarden.

Op dit moment worden er drie opties geboden voor het leveren van een externe verbinding:

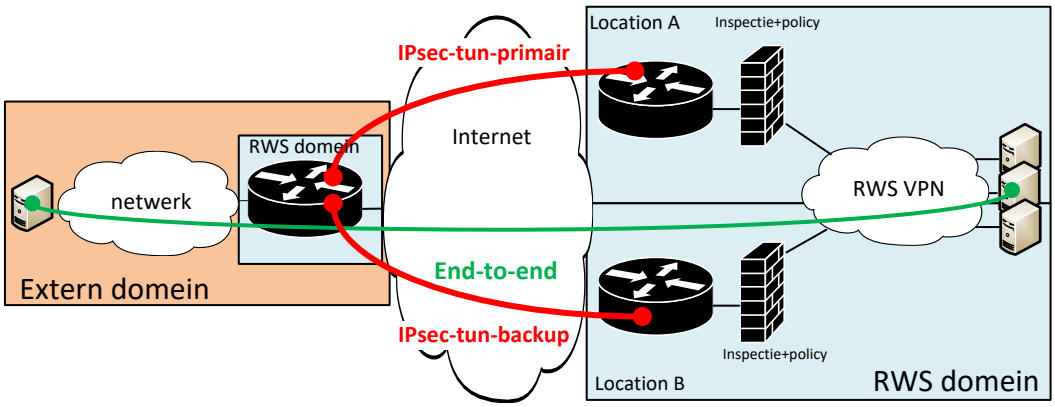
IPSEC zonder managed CPE
IPSEC zonder managed CPE is weergegeven in onderstaand figuur en redundant opgebouwd aan de RWS zijde waarbij de apparatuur over twee geografisch gescheiden locaties een cluster vormt. Op deze omgeving worden alleen nog de marktconforme veilige encryptie standaarden gebruikt. Er wordt gebruik gemaakt van een virtual IP adres voor de VPN gateway. Hierdoor is de perceptie van de afnemer dat er slechts één component staat.



Figuur 14 IPSEC

IPSEC met managed CPE (MCPE)
Bij deze optie, weergegeven in onderstaand figuur, wordt het internet gebruikt als transportmedium tussen het RWS netwerk en de externe partij. De externe partij dient zorg te dragen voor een werkende internet verbinding en een computerruimte waarin de apparatuur geïnstalleerd kan worden. Op locatie van de externe partij wordt een beheerd netwerk device geplaatst vanuit SP-O&A. SP O&A draagt zorg voor het opzetten van de veilige logische verbinding waarin het dataverkeer versleuteld wordt. Deze wordt aan de RWS-zijde redundant ontsloten over twee geografisch gescheiden locaties. SP-IB monitort actief de CPE die bij de externe partij staat.

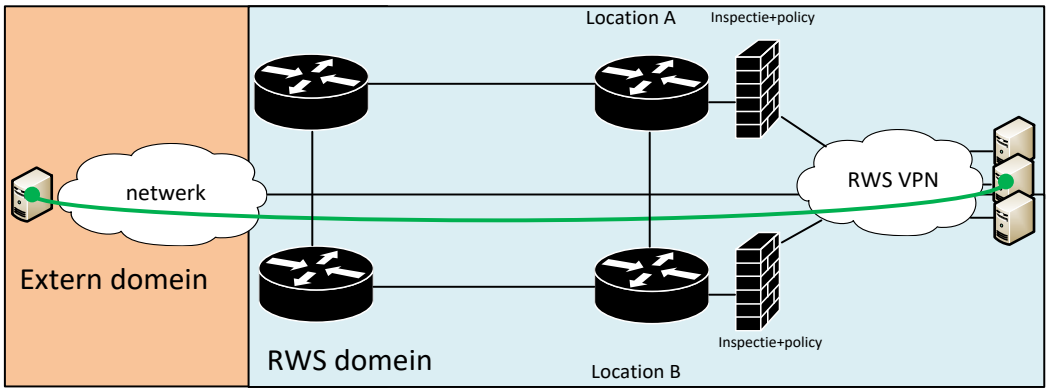
Voordelen	Nadelen
• Flexibel • Veilig • Relatief snel te leveren • Alleen een transparante internet verbinding nodig. • ConclusionQuanza zorgt voor een werkende end-to-end verbinding.	• End-to-end geen SLA af te geven • Geen bandbreedte garantie • Standaard alleen leverbaar binnen NL



Figuur 15 IPsec + MCPE

Vaste verbinding
Bij deze optie, weergegeven in onderstaand figuur, wordt een vaste verbinding ingezet vanuit de bouwsteen 'VPN aansluiting'. De VPN aansluiting zal op een veilige manier worden aangesloten op het RWS netwerk. De verbinding t/m de locatie van de afnemer valt onder de verantwoordelijkheid van ConclusionQuanza.

Voordelen	Nadelen
• Veilig • End-to-end SLA (zie SLA VPN aansluiting) • Diverse beschikbaarheid opties (zie VPN aansluiting) • Bandbreedte garantie	• Langere levertijd • Standaard alleen leverbaar binnen NL • Extra VPN + VPN Firewall nodig



Figuur 16 Voorbeeld redundante vaste verbinding

De dienst kent de volgende eigenschappen en uitgangspunten:

- Voor vaste externe toegangsvoorzieningen die geen SLA's vereisen wat betreft beschikbaarheid en bandbreedte, kan er gekozen worden om te koppelen via het internet en IPsec. De randvoorwaarde hiervoor is dat de niet-RWS-locatie beschikt over een eigen internetvoorziening met voldoende beschikbare netwerk capaciteit voor de beoogde communicatie.
- Apparatuur die op locatie bij een derde partij wordt geplaatst, dient te worden geplaatst in een ruimte die voldoet aan de eisen, beschreven in de NNV aansluitvoorwaarden.
- Voor beveiliging worden componenten gebruikt die aantoonbaar voldoen aan geaccepteerde beveiligingscriteria zoals NBV[4] goedkeuring of certificering volgens ISO/IEC 15408 (common criteria)[5] .
- De systeem eigenaar/ product manager van de beschikbaar gestelde applicaties, systemen, netwerken en informatie dient expliciet toestemming te geven voor deze netwerk toegang.
- De dienst is alleen voor CIV-onderdelen of externe partners die een contract afgesloten hebben met CIV. Voor het gebruik van de externe koppeling dienen externe partners te voldoen aan de "RWS-voorwaarden Externe koppelingen".
- De klant conformeert zich bij afname van deze dienst expliciet aan het beveiligingsbeleid van Rijkswaterstaat.
- Iedere vaste externe toegangsvoorziening met een derde partij dient een benoemde functioneel beheerder te hebben.
- Vaste externe toegangsvoorzieningen worden bij voorkeur via het internet gerealiseerd via de standaard-beveiligingsfaciliteiten van NNV met gebruik maken van IPsec VPN-technologie.
- De vaste externe toegangsvoorziening voldoet aan de baseline beveiliging BIR2017.
- De vaste externe toegangsvoorziening ondersteunt alleen IPv4 unicast.
- Er kan alleen gebruik worden gemaakt van publieke adressen voor de communicatie tussen de externe partij en RWS.
- Routering tussen de externe partij en ConclusionQuanza is op basis van statische routes.

Bij het aanvragen of wijzigen van een vaste externe toegangsvoorziening voor een derde partij dient het "RWS Netwerktoegang voor Derden" proces gevolgd te worden. Dit proces kan opgestart worden door het invullen en bij de Corporate Servicedesk indienen van het "Aanvraagformulier Netwerktoegang voor Derden."

Externe koppelingen in de vorm van vaste verbindingen
(**) Externe koppelingen in de vorm van vaste verbindingen worden afgenomen via het ON2013 contract; medio 2025 wordt dit vervangen door het CDR2023 contract. Leverancier is voor beide contracten ODIDO.

[4] NBV: Nationaal Bureau voor Verbindingsbeveiliging, onderdeel van het ministerie van BZK.
[5] Voor een common criteria beoordeling moet een bewuste keuze worden gedaan voor een EAL-niveau en een protection profile dat voldoende is voor de toepassing.

Het gaat om de volgende dienstverlening door ODIDO:

IP & Ethernet VPN	20Mb/s, Beheerprofiel Laag	BD01
	20Mb/s, Beheerprofiel Standaard	BD02
	20Mb/s, Beheerprofiel Hoog	BD03
	100Mb/s, Beheerprofiel Standaard	BD11
	100Mb/s, Beheerprofiel Hoog	BD12
	1Gb/s, Beheerprofiel Standaard	BD21
	1Gb/s, Beheerprofiel Hoog	BD22
	1Gb/s, Beheerprofiel Non-stop	BD23
On-Net maken, Odido	On-net maken (glasvezel), opstartkosten	AG01
	On-net maken (glasvezel), graafkosten per meter	AG02
	On-net maken (glasvezel), kosten boren per meter	AG03
	On-net maken (radioverbinding)	AG04
On-Net maken, Inkoop 3e partij	Opslag op eenmalig kosten bij inkoop 3de partij	TP01
	Opslag op maandelijkse kosten bij inkoop 3de partij	TP02
PSTN Verbindingen	PSTN (koper), Beheerprofiel Laag	PS01
	PSTN (glas), Beheerprofiel Laag	PS02
	PSTN (glas), Beheerprofiel Hoog	PS03

Tabel 13 Vaste verbindingen ODIDO

Categorie LAN aansluiting

Een LAN aansluiting maakt het mogelijk om op RWS locaties connecties te maken over het netwerk. De categorie **Local Area Network (LAN) aansluiting** omvat de verschillende type LAN aansluitingen voor Kantoor Automatisering-LAN (KA-LAN en LAN aansluiting type KA), WIFI, Centrale VicNet Ruimte (CVR) en VicNet Object Ruimte (VOR), Wegkant/Waterkant systemen, Gebouwen, Rekencentrum (VC/VP) en type Offshore voor aansluitingen op zee.

Functionele omschrijving

De dienst LAN aansluiting biedt toegang tot een virtueel netwerk via een fysieke LAN poort. De LAN aansluiting is opgebouwd uit de volgende componenten:

LAN ontsluiting dit is de logische koppeling naar een specifiek VPN
VLAN dit is een virtueel LAN (VLAN) in de fysieke infrastructuur (bijvoorbeeld de switches)
LAN aansluiting de fysieke poort die toegang biedt naar het virtuele LAN
Network Access Control (NAC) Netwerktoegangsbeveiliging op LAN niveau. Eindgebruikers en eindsystemen krijgen pas netwerktoegang na succesvolle authenticatie.

Ethernet infra dit is de fysieke infrastructuur (bekabeling en switches)

Ethernet Infra

Het component Ethernet infra is zo opgebouwd dat de dienst LAN aansluiting bijna overal leverbaar is. Hiervoor moet wel bekabeling aanwezig zijn, of aan te leggen zijn, tegen acceptabele kosten. Deze dienst biedt een fysieke ethernet aansluiting voor een eindsysteem. Deze wordt op een door een VPN ontsloten locatie gerealiseerd middels een VPN aansluiting.

Network Access Control (NAC)

Wanneer een eindgebruiker of eindsysteem verbinding maakt met het netwerk wordt met behulp van NAC (Network Access Control) bepaald of deze geautoriseerd is om toegang tot het netwerk te hebben. Door middel van NAC wordt ook bepaald tot welke gebruikersgroep de eindgebruiker behoort. De gebruikersgroepen worden vastgelegd in zogenaamde NAC-profielen (Informatie hierover is te vinden in paragraaf 0). NAC wordt verplicht ingeschakeld op LAN dienstverlening op kantoorlocaties. Hiervan kan alleen worden afgeweken bij devices die geen 801.2x ondersteunen. Een security exceptie is hiervoor randvoorwaardelijk. Deze zal door de afnemer zelf moeten worden aangevraagd binnen RWS.
NAC is generiek ontwikkeld, ook voor alle overige type LAN aansluitingen behalve op ODC LAN of op LAN aansluitingen die geïntegreerd zijn in een Backbone Edge(CE-router). Om NAC te gebruiken is een NAC profiel noodzakelijk. De Infra Adviseur Netwerken begeleidt het aanvragen van een profiel.

Beheren LAN-aansluitingen

RWS onderkent de volgende LAN-aansluitingen:

1. Gebouw
2. LAN-aansluiting type KA
3. Rekencentrum
4. CVR/VOR
5. Callcenter
6. Wegkant/Waterkant
7. Offshore
8. Wifi
9. Open Wifi

Quanza IB voert het beheer uit op deze LAN-diensten conform onderstaande SLA.

Dienstenmatrix LAN											
Type LAN Aansluiting	Bandbreedte	Beschikbaarheid						Storingshersteltijd in 95% van de gevallen			
		Enkel			Redundant			Service Window Kantoortijden		Service Window"24/7"	
		99,00%	99,50%	>99,7%	>99,8% **	99,95% ***	99,99% ***				
		Onbeschikbaarheid per jaar									
		ca 3d15u	ca 1d20u	ca 1d2u	ca 17u30m	ca 4u28m	ca 0u52m	8 uur	4 uur	8 uur	4 uur
Gebouw			V			V			V		V
Rekencentrum (VC/VP)			V			V			V		V
CVR/VDR	Auto (voorkeursinstelling)		V				V				V
	10 Mbps		V				V				V
	100 Mbps		V				V				V
	1000 Mbps		V				V				V
Callcenter	<= 100 Mbps of		V			V					V
	<= 1 GBps of		V			V					V
	<= 2 * 1 Gbps (Server)		V			V					V
Wegkant/Waterkant*	<= 1Gbps			V	V						V
KA LAN	<= 100 Mbps of		V			V		V	V		V
	<= 1 GBps of		V			V		V	V		V
	<= 2 * 1 Gbps (Server/blade)		V			V		V	V		V
Wifi****			V					V			

*	max 2 storingen per jaar
**	indien sprake is van geografische redundantie glasvezelinfrastructuur
***	over 2 switches
****	radiodekking
*****	type Offshore is Redelijke Inspanning (ivm specfieke locatie)

Tabel 14 Beschikbaarheids eisen LAN aansluiting

Bestelbare items levertijd

Voor de LAN aansluiting gelden de in onderstaande tabel weergegeven bestelbare items met bijbehorende standaard levertijden.

LAN Aansluiting			
Eenmalige dienst	**Toelichting**	**Levertijd in werkdagen (door SP-O&A)**	**SSR (door SP-IB)**
RWS Netwerk LAN *(Gebouw, Rekencentrum (VC/VP), CVR/VOR, KA)*			
Aanvragen	Leveren 1e LAN aansluiting op apparaat	60	
Opheffen	Opheffen laatste LAN aansluiting op apparaat	10	
Activeren	Activeren extra LAN aansluiting op afstand	5	
Deactiveren	Deactiveren extra LAN aansluiting op afstand	5	
Wijzigen	Wijzigen instelling bestaande LAN aansluiting op afstand (alleen voor LAN aansluiting KA)	5	
Wegkant/Waterkant, Onderstation, Offshore			
Aanvragen	Leveren 1e LAN aansluiting op apparaat	60	
Aanvragen	Leveren 1e LAN aansluiting op apparaat zonder installatie(*)	60	
Opheffen	Opheffen laatste LAN aansluiting op apparaat	10	
Opheffen	Opheffen laatste LAN aansluiting op apparaat zonder installatie(*)	10	
Activeren	Activeren extra LAN aansluiting op afstand	5	
Deactiveren	Deactiveren extra LAN aansluiting op afstand	5	
WIFI			
Aanvragen	Leveren access point	50	
Opheffen	Opheffen access point	20	
Wijzigen	Wijzigen instelling access point op afstand	5	

LAN Aansluiting			
Aanvragen site survey (per etage)	Leveren site survey op locatie	15	
Open WIFI			
Activeren Open WIFI	Open WIFI functionaliteit op locatie / verdieping / ruimte (excl. site survey) met of zonder apart SSID	20	
Deactiveren Open WIFI	Open WIFI functionaliteit op locatie / verdieping / ruimte (excl. site survey) met of zonder apart SSID	20	
Wijzigen Open WIFI	Registratie MAC adres vaste apparatuur per 10 devices	1	
Aanvragen site survey (per etage)	Leveren site survey Open WIFI op locatie	15	

Tabel 15 Bestelbare items categorie LAN aansluiting

Levering gebeurt door Quanza – O&A met uitzondering van de Standaard Service Requests, die door Quanza – IB worden uitgevoerd. Voor alle werkzaamheden op locatie wordt SPIE aangestuurd.

(*) Met installatie betekent, dat de installatie door SPIE gebeurt; zonder installatie betekent, dat de hardware wordt afgeleverd door SPIE, maar dat de installatie zelf door een lokale aannemer gebeurt.

RWS Netwerk LAN

Onder RWS Netwerk LAN worden alle LAN aansluitingen verstaan met uitzondering van Kantoor Automatisering LAN, WIFI en OpenWIFI. Deze specifieke diensten met bijbehorende kenmerken zijn separaat beschreven.

Op basis van de gewenste beschikbaarheid, bandbreedte, robuustheid en functionaliteit zijn er meerdere RWS Netwerk LAN opties mogelijk.

LAN aansluiting type Gebouw: *voor systemen met middelhoge snelheden en data throughput*

Dit type LAN aansluiting wordt toegepast voor systemen (onder andere datacollectie-pc's) met middelhoge snelheden en data throughput in RWS gebouwen zoals Industriële Automatisering (IA's) en Object LAN's. De uitvoering is op basis van een RJ45 koppelvlak. Redundante aansluiting van eindsystemen en loadbalancing zijn niet mogelijk.

LAN aansluiting type Rekencentrum (VC/VP): *voor systemen met hoge eisen aan beschikbaarheid en bandbreedte ten behoeve van Verkeerscentrales en Verkeersposten*

Dit type LAN aansluiting wordt ingezet voor systemen met hoge eisen aan beschikbaarheid en bandbreedte, toegepast in Verkeerscentrales en Verkeersposten. Uitvoering is op basis van een koper (RJ45) of glas-koppelvlak. Schaalbaarheid is in dit type LAN aansluiting mogelijk.

LAN aansluiting type CVR / VOR*: o.b.v. schaalbaarheid, robuustheid en hoge beschikbaarheid*

Dit type LAN aansluiting is bedoeld om in CVR/VOR ruimten langs Rijks(water)wegen een connectie te maken met verkeersmanagementsystemen in Verkeerscentrales (VC) en het RWS Overheid Data Center (ODC). De dienst biedt de noodzakelijke LAN functionaliteit ten behoeve van het aansluiten van inwin- en besturingssystemen zoals meetsystemen, camera's, radarsystemen, noodsystemen en signaleringsystemen. Belangrijke kenmerken zijn schaalbaarheid, robuustheid en hoge beschikbaarheid. Redundante aansluiting van eindsystemen en loadbalancing zijn niet mogelijk.

De volgende voorwaarden gelden voor het type LAN aansluiting CVR/VOR:

- Een geconditioneerde omgeving;
- De LAN aansluiting is uitsluitend bedoeld voor eindsystemen. Het aansluiten van netwerk apparatuur zoals routers, switches en access points op een LAN aansluiting is niet toegestaan;
- Deze dienst biedt uitsluitend ondersteuning voor TCP/IP en Ethernet. Andere protocollen zoals IPX/SPX of veldbus protocollen zoals Profinet, Modbus en SafetyNET worden niet ondersteund.
- Voor het aansluiten van digitale eind devices kan dit type LAN-aansluiting geleverd worden met optische SFP's (single of dual fiber). Aangesloten eind devices dienen in de directe omgeving van de switch te staan. Het demarcatiepunt van de dienstverlening op deze LAN aansluiting is de LAN-poort. Bekabeling vanaf de LAN-poort naar het eind device, en eventuele media convertor, zijn geen onderdeel van de dienst. Deze LAN poorten zijn expliciet alleen voor eind devices bedoeld zijn en niet om routers of switches aan te sluiten.

De duplex instelling van een LAN aansluiting wordt standaard ingesteld op de voorkeursinstelling (Auto) waarbij een onderhandelprotocol zorgt dat beide aangesloten apparaten dezelfde duplex instelling hebben. Hierbij wordt onderscheid gemaakt tussen Half Duplex (eenrichtingsverkeer, om en om zenden en ontvangen) en Full Duplex (tweerichtingsverkeer, tegelijk van beide kanten zenden en ontvangen mogelijk). Indien de Auto instelling voor beide aangesloten apparaten niet naar behoren werkt kan de aansluiting in sommige gevallen op Half of Full Duplex worden ingesteld.

LAN aansluiting type Wegkant/Waterkant *ten behoeve van ongeconditioneerde ruimtes*

Deze LAN aansluiting is bedoeld om ethernet/IP gebaseerde weg- en waterkant toepassingen te koppelen op een VPN. Deze dienst wordt onder andere toegepast bij DRIPs, DOV, TDI, VRI, VAD, Weigh In Motion weegbruggen (WIM), IP-camera's, Digitale Camera aansluitingen en het UWP. Het biedt een hoge beschikbaarheid en betrouwbaarheid waarbij het mogelijk is om onderdelen eenvoudig te vervangen met behoud van functionaliteit.

Afwijkend ten opzichte van andere ethernet/IP gebaseerde LAN producten worden omwille van de relatief grote afstanden de ethernetswitches in cascade (ring-topologie) geschakeld. Standaard is de beschikbaarheid redundant (>99,8%) door een geografisch gescheiden Glasvezelring (loopt via een geheel andere [vaar]weg dan wel aan de andere zijde van de [vaar]weg retour). Indien er geen geografisch gescheiden Glasvezelring mogelijk is, maar wel een fysieke Glasvezelring, kan op verzoek van de Afnemer en met toestemming van CIV Infra deze Dienst geleverd worden met een beschikbaarheid enkelvoudig (>99,7%; loopt via dezelfde [vaar]weg of via dezelfde Glasvezelkabel retour).
Deze dienst is geschikt gemaakt voor het leveren in ongeconditioneerde ruimtes doormiddel van passieve koeling en biedt ten behoeve van de service provider SP-IB remote beheerfunctionaliteit van de apparatuur voor netwerkmanagement.
In het kader van beveiliging worden niet gebruikte poorten dichtgezet, applicatiedomeinen in aparte VLAN's ondergebracht ten behoeve van de scheiding van netwerk services, switches in afgesloten kasten geplaatst, MAC Address filtering toegepast op wegkantswitches, vindt beheeradmin toegang plaats via de centrale AAA Service, is beheer van VLAN/VPN gescheiden van data VLAN's en wordt gebruik gemaakt van Detect en Disable unidirectional links.

Voor dit type LAN aansluiting geldt een aantal aanvullende voorwaarden:
- Plaatsing en montage op DIN rail, 19" rack of 'board' vereist;
- Er worden maximaal 27 switches cascade geschakeld;
- Met een 1000Base-LX interface kan een afstand worden bereikt van 10km en met de ZX variant ca 70km (conform specificaties) per switch;
- Voor het aansluiten van digitale eind devices kan dit type LAN-aansluiting geleverd worden met optische SFP's (single of dual fiber). Aangesloten eind devices dienen in de directe omgeving van de switch te staan. Het demarcatiepunt van de dienstverlening op deze LAN aansluiting is de LAN-poort. Bekabeling vanaf de LAN-poort naar het eind device, en eventuele media convertor, zijn geen onderdeel van de dienst. Deze LAN poorten zijn expliciet alleen voor eind devices bedoeld zijn en niet om routers of switches aan te sluiten.
- Deze LAN aansluiting wordt standaard geleverd met een dubbele (net)voeding. Indien noodzakelijk kan deze geleverd worden met een enkelvoudige voeding en/of een voeding met lage inschakelstroom (≤ 16 A). Bij gebruik van een enkelvoudige voeding wordt de beschikbaarheid naar 99,5% teruggebracht.

LAN aansluiting type Onderstation *ten behoeve van ongeconditioneerde ruimtes*

Deze LAN aansluiting is toepasbaar met en zonder WKS, en is geschikt om bijvoorbeeld camera's, DRIP's, TDI's, WIM's etc. op afstand van een WKS of CVR/VOR aan te kunnen sluiten. De LAN aansluiting type Onderstation wordt geleverd middels een switch met maximaal 4 aansluitmogelijkheden, met een enkelvoudige voeding en wordt enkelvoudig aangesloten via RWS glas. Hierdoor kent deze dienst een lagere beschikbaarheid garantie; maximaal 95%.

LAN aansluiting type Offshore

De dienst LAN aansluiting type Offshore biedt LAN aansluitingen op offshore objecten op de Noordzee, zoals Windmolenparken (WMP's), windturbinegeneratoren (WTG's) en olie-&gasplatforms. Deze dienst kent geen service levels, omdat er op zee geen garantie mogelijk is voor het tijdig beschikbaar hebben van apparatuur en monteurs. Vervangende hardware voor de LAN Aansluiting type Offshore is in geval van defecten binnen 24 uur beschikbaar op een aangewezen locatie aan de wal. De exploitanten van de offshore objecten hebben eigen gespecialiseerde installatie- en onderhoudspartijen. Deze partijen vervoeren de (vervangende) hardware vanaf de aangewezen locatie aan de wal naar de offshore objecten en zorgen voor installatie en onderhoud. De dienstverlening maakt gebruik van bestaande connectiviteit van wal tot platform (bijvoorbeeld glas) van derde partijen. De aanvrager van de dienst zorgt dat deze connectiviteit voor de LAN aansluiting type Offshore beschikbaar is en gebruikt kan worden.

KA LAN (niet meer bestelbaar)

De KA LAN omgeving is bedoeld om ethernet/IP gebaseerde apparaten zoals desktops en servers te koppelen aan RWS VPN's via een Managed LAN. Deze dienst wordt geboden in geconditioneerde ruimtes in RWS kantoorgebouwen en kan alleen worden afgenomen per switch met 24 of 48 KA LAN poorten. Deze dienst wordt vervangen door de LAN aansluiting type KA, waarbij inzet van NAC verplicht is, tenzij er een security exceptie verkregen is. Voor nieuwe bestellingen dient de dienst LAN aansluiting type KA te worden aangevraagd.

KA LAN is opgebouwd uit de volgende componenten:

LAN aansluiting	Lokale LAN poort, gekoppeld in een VLAN, op de Ethernet infrastructuur
Local Area Network	Laag 2 Ethernet VLAN op de Ethernet infrastructuur
Ethernet infra	Ethernet infrastructuur in gebouwen

Op basis van de grootte van de locatie en bijbehorende KA omgeving wordt onderscheid gemaakt tussen 3 type KA LAN waarvan de kenmerken zijn weergegeven in Tabel 16 Opties type KA LAN. Alle locaties zijn geschikt voor één of meerdere VPN aansluitingen.

Opties type KA LAN aansluiting												
Type locatie	Desktop poorten	Server poorten	LAN			MER/SER			Routering	WAN Router		Bladeservers
			10Base-T	100Base-T	1000Base-T	Geen	Één	Meerdere		Enkelvoudig	Dubbelvoudig	
Klein	<=24		✓	✓		✓	✓			✓		
Middelgroot	✓	✓	✓	✓	✓*		✓	✓		✓	✓	
Groot	✓	✓	✓	✓	✓		✓	✓	✓		✓	✓

Tabel 16 Opties type KA LAN

*Enkele server poorten
**Beperkt aantal 1000Base-T poorten

De KA-LAN omgeving kent de volgende functies:

- Het is mogelijk meerdere VLAN's te creëren op een fysieke poort (trunking). De VLAN's dienen toe te behoren aan één VPN;

- Om de netwerkcapaciteit uit te breiden, is het mogelijk om tussen twee switches port-channeling toe te passen. Hiermee wordt de capaciteit van beide switches gecombineerd;
- Er wordt een spanning-tree protocol toegepast om problemen in het netwerk te detecteren en te voorkomen;
- Het is mogelijk om niet-routeerbare /geïsoleerde VLAN's aan te vragen. Deze VLAN's worden wel administratief gekoppeld aan een VPN Aansluiting;

LAN aansluiting Type KA en LAN aansluiting type Call center

De LAN Aansluiting type KA is bedoeld om ethernet/IP gebaseerde apparaten zoals desktops en servers te koppelen aan RWS VPN's via een Managed LAN. Deze dienst wordt geboden in geconditioneerde ruimtes in RWS kantoorgebouwen. De LAN aansluiting type KA wordt standaard verplicht geleverd mét NAC.
Ten behoeve van Call Center omgevingen is het mogelijk Power over Ethernet (PoE) toe te passen. Hiermee kan een aangesloten apparaat zoals een call center server, bedien PC, telefoon of Wall board via de aansluiting op de switch van stroom worden voorzien.

Wifi

De dienst WIFI biedt veilige draadloze netwerktoegang op RWS locaties die zijn aangesloten op het RWS netwerk. De WiFi dienstverlening ondersteunt de WiFi standaarden WiFi-2 t/m WiFi-6, waarbij overigens alleen WiFi-6 nog nieuw te bestellen is.

Er worden vier gebruikersgroepen onderkend:

- RWS medewerkers met door RWS beheerde mobiele devices voorzien van een RWS certificaat
  kunnen middels de SSID's 'RWS-intern' of 'RijkskantoorRoam' toegang krijgen tot de WiFi dienstverlening van RWS.
  Hiermee kunnen de RWS beheerde mobiele werkplekken draadloos worden verbonden en daarbij logisch dezelfde toegang verkrijgen als via een vaste bedrade kantoor aansluiting (KA).
- Deelnemers van Rijkskantoorroam:
  Deelnemers van Rijkskantoorroam kunnen middels het SSID 'RijkskantoorRoam' toegang krijgen tot de WiFi dienstverlening van RWS die is gekoppeld aan de Rijkskantoor dienstverlening.
- Deelnemers van Govroam, zie https://govroam.nl/ voor actuele deelnemers:
  - Door middel van de overheid brede 'Government roaming Nederland' oplossing wordt gefilterde internettoegang geboden voor alle medewerkers van de overheidsorganisaties die aangesloten zijn op de landelijke Govroam dienstverlening.
  - BYOD RWS medewerkers: Het SSID 'govroam' is voor RWS medewerkers beschikbaar voor BYOD devices.
- Gastgebruikers die akkoord gaan met de algemene voorwaarden van RWS en daarmee zonder identificatie toegang krijgen tot het publieke internet op de door RWS CIV aangewezen locaties

Elke groep kent een specifieke, functioneel andere Service Set Identifier (SSID) zoals weergegeven in Tabel 17 Overzicht gebruikersgroepen WIFI en Open WIFI**.** Het SSID zorgt

voor functiescheiding tussen de verschillende logische draadloze netwerken. SSIDs kunnen worden ingesteld per locatie of specifieke ruimte binnen een locatie. Zo kunnen er op een locatie in verschillende ruimten verschillende SSIDs actief zijn. Het aanvragen van een nieuwe functie binnen een SSID of een geheel nieuw SSID kan uitsluitend via CIV RWS IRN INFRA.

Voor de WiFi dienstverlening zijn een tweetal standaard sets van SSID's opgesteld. Één set is bedoeld voor een RWS-locatie en de tweede set is bedoeld voor een RWS-locatie die is aangemerkt als Rijksverzamelkantoor. Gasttoegang is voor beide locaties een optie.

RWS-locatie:
- SSID 'RWS-intern'
- SSID 'govroam'
- SSID tbv OpenWiFi (per locatie aan te vragen)

RWS-locatie aangemerkt als Rijksverzamelkantoor:
- SSID 'RijkskantoorRoam'
- SSID 'govroam'
- SSID 'RijkskantoorGast'

Omschrijving	Functie	Identiteit bekend	SSID	VPN	Security Zone
RWS beheerd device voorzien van RWS-certificaat	Toegang tot interne RWS applicaties, toegang tot internet via bouwsteen Webproxy.	Ja	RWS-intern	RWS:RWS	Semi-trusted
Stichting Govroam	Toegang internet voor gastgebruikers en RWS medewerkers die gebruik maken van een BYOD	Ja	govroam	RWS:Govroam	Untrusted
Rijkskantoor-roam voor RWS-panden die tevens rijks-kantoorpand zijn	- Voor RWS-medewerkers met een door RWS beheerd mobiel device voorzien van een RWS-certificaat. - Voor IDV-G gebruikers van Rijkskantoorroam.	Ja	Rijkskantoor Roam	- RWS:RWS (RWS-medewerkers) - WAN-i (IDV-G)	Semi-trusted
Gastgebruikers zonder account / Open WiFi	Toegang publiek internet	Nee	Rijkskantoor Gast		Untrusted

Omschrijving	Functie	Identiteit bekend	SSID	VPN	Security Zone
(overige locaties)					

Tabel 17 Overzicht gebruikersgroepen WIFI en Open WIFI

De dienst WIFI voorziet in het ophangen van Access Points (AP's) op locaties waarmee gebruikers een draadloze verbinding kunnen opzetten.

Voor het inrichten van een nieuwe locatie en/of een nieuw gedeelte van een bestaande locatie wordt verplicht een inmeting uitgevoerd (dekking en capaciteit) om te bepalen op welke locaties AP's er geplaatst dienen te worden. De AP's worden op strategische plaatsen gemonteerd en zodanig ingesteld zodat binnen het afgesproken dekkkingsgebied roaming tussen deze AP's mogelijk is. Door de strategische plaatsing van de AP's zal de WiFi-dienstverlening het uitvallen van een enkel AP op kunnen vangen, de naburige AP's zorgen in deze situatie voor herstel van dekking (zie ook uitgangspunten hieronder).
De inmeting is een momentopname, interne verhuizingen kunnen de dekking beïnvloeden. De plaatsing van AP's wordt altijd afgestemd met de gebouwbeheerder.

Uitgangspunten

Voor WIFI gelden de volgende uitgangspunten:

- WIFI is niet bedoeld voor missiekritieke applicaties!
- De WIFI AP's worden middels Power over Ethernet (PoE) voorzien van voeding. PoE wordt door de LAN-aansluiting geleverd.
- WIFI wordt uitsluitend geboden op RWS locaties voorzien van minimaal een vaste VPN aansluiting, aangevuld met een "LAN- of KA-LAN aansluiting";
- Voor het inrichten van WIFI op nieuwe locaties is de afname van een nieuwe VPN aansluiting ten behoeve van het WIFI verkeer vereist;
- De 99,5% beschikbaarheid heeft betrekking op de aanwezige radiodekking op een locatie of in een ruimte. De implementatie van AP's zorgt er voor dat bij uitval van een enkel AP de radiodekking gegarandeerd blijft. Uitval van een enkel AP zal niet tot connectiviteitsverlies leiden, wel zal de beschikbare bandbreedte tijdelijk afnemen.
- De WiFi dienst is geschikt voor Voice, Real-Time en Data toepassingen. Alle toepassingen worden met gelijke prioriteit behandeld;
- Wijzigingen in de omgeving, bijvoorbeeld het plaatsen van wanden of een toename in medewerkers kunnen van invloed zijn op de prestaties van het draadloze netwerk;
- Minimale connectiesnelheid van een client is 12Mbps, lagere snelheden worden niet ondersteund;
- Per AP radio worden maximaal 200 clients ondersteund maar 75 clients wordt als "gezond" gezien;
- RWS is verantwoordelijk voor interne bekabeling en stroomvoorziening.

Randvoorwaarden

De volgende randvoorwaarden zijn van toepassing:

- Voor het leveren van WIFI is een door RWS CIV IRN Infra Netwerken geleverde en door SP-IB beheerde LAN omgeving, op basis van Power over Ethernet (PoE), in het pand vereist, welke is aangesloten op het RWS netwerk via een vaste VPN aansluiting;
- Afhankelijk van de SSID's die nodig zijn op een locatie zal/zullen ook één of meer van de volgende VPN's aanwezig moeten zijn: RWS:RWS bij RWS-Intern, RWS:GOVROAM bij Govroam en/of WAN-i voor Rijkskantoorgast;
- Verkregen gebouwplattegronden die gebruikt worden voor site survey's en voor intekening van dekkingsmetingen dienen door alle betrokken partijen vertrouwelijk te worden behandeld;
- De bekabeling dient te voldoen aan minimaal CAT5E of CAT6 ten behoeve van het aansluiten van Access Points;
- Bij uitbreiding van het aantal Access Points op basis van capacity management dient rekening te worden gehouden met de aanwezigheid van juiste bekabeling (zie boven) en stroomvoorziening. De gebouwenbeheerder is hier verantwoordelijk voor;
- WIFI is afhankelijk van de dienst die de LAN functionaliteit levert. Deze LAN functionaliteit is geen onderdeel van de dienst Wi-Fi. Het aansluiten van een AP vereist een 1Gbps LAN Aansluiting met PoE.

Open WIFI

Open WIFI Is een optionele dienst onder WIFI die open internet toegang biedt zonder identificatie voor alle gebruikers op de gekozen locatie. Open WIFI kan voor twee doeleinden worden ingezet:

- Voor gastgebruikers zonder een tijdelijk account, die akkoord gaan met de algemene voorwaarden die in de vorm van een disclaimer aan hen wordt voorgelegd. Toegang alleen naar publiek internet op de door RWS aangewezen locaties. Hierbij wordt onderscheid gemaakt tussen Westraven LEF en Open WIFI op andere RWS-locaties;

- Open WIFI maakt het ook mogelijk om apparatuur zonder webbrowser (bv. informatiezuilen) met internet te verbinden. Dit vindt plaats o.b.v. het MAC-adres van deze apparatuur. Activatie van een MAC-adres is niet locatie-gebonden. Als Open WIFI voor een locatie wordt opgeheven, dan moeten de MAC-adressen voor deze locatie apart worden verwijderd.

- Open WIFI is alleen mogelijk op locaties met NNV connectiviteit en waar al WIFI dienstverlening aanwezig is. De dienst kan worden aangevraagd voor de hele locatie (default) of een deel ervan (incidenteel). Het is ook mogelijk om de dienst voor een beperkte periode, met een begin- en einddatum, aan te vragen, om bijvoorbeeld een tijdelijke behoefte i.v.m. een event te kunnen invullen. Gerelateerd daaraan is het ook mogelijk om de standaard SSID (WIFI-naam) ''RijkskantoorGast'' locatie specifiek aan te passen zodat de WIFI-naam herkenbaar is voor de gastgebruikers die aan dat event deelnemen.

De totale Open WIFI-dienstverlening is gedimensioneerd (niet gelimiteerd) op max. 1.000 gelijktijdig operationele devices. Bij overschrijding van dit aantal vervallen de beschikbaarheidsgaranties.

Categorie Eindsystemen
De categorie **Eindsystemen** beschrijft verschillende eindsysteemtoepassingen: de Digitale Video aansluiting (Encoder Analoge Camera), AAA Remote Access Groepsprofiel, PPP, TBMS BUS en Draadloze aansluiting.

Beheren Eindsystemen
RWS onderkent de volgende eindsystemen:
1. DVA – Digitale Video Aansluiting
2. Remote Access groepsprofiel
3. PPP Aansluiting
4. Remote Access Gebruiker
5. TBMS Bus
6. AAA
7. Draadloze aansluiting

Quanza IB voert het beheer uit op deze Eindsystemen conform onderstaande SLA.

Eindsystemen Dienstenmatrix								
Type Eindsysteem	Beschikbaarheid				Storingshersteltijd in 95% van de gevallen			
	99.5%	99.7%	99.95%		Service Window Kantoortijden		Service Window 24/7	
	Onbeschikbaarheid per jaar							
	ca 1d20u	ca 1d2u	ca 4u28m		8 uur	4 uur	8 uur	4 uur
DVA – Digitale Video aansluiting		V						V
Remote Access Groepsprofiel			V					V
PPP Aansluiting	NVT				redelijke effort			
Remote Access Gebruiker	NVT				redelijke effort			
TBMS Bus	NVT				redelijke effort			

Tabel 18 Beschikbaarheids eisen Eindsystemen

Bestelbare items en levertijd
Voor de **Eindsysteem toepassingen** gelden de in onderstaande tabel weergegeven bestelbare items met bijbehorende standaard levertijden.

Eindsystemen			
Eenmalige dienst	**Toelichting**	**Levertijd in werkdagen (door SP-O&A)**	**SSR (door SP-IB)**
Digitale Video Aansluiting (Encoder Analoge Camera)			
Opheffen incl. installatie	Opheffen dienst op eindsysteem inclusief installatie	10	

Eindsystemen			
Opheffen	Opheffen dienst op eindsysteem exclusief installatie	10	
Wijzigen	Wijzigen instelling Digitale Video aansluiting	5	
PPP aansluiting			
Opheffen	Opheffen PPP aansluiting	10	
Wijzigen	Wijzigen PPP aansluiting	10	
TBMS BUS			
Opheffen	Opheffen TBMS BUS	10	
Remote Access groepsprofiel			
Aanvragen	Aanvragen RAS profiel	20	
Opheffen	Opheffen RAS profiel	5	
Wijzigen	Wijzigen RAS profiel	5	Ja
AAA Ras gebruiker			
Aanvragen	Aanvragen RSA Token	5	
Opheffen	Opheffen RSA Token	5	
Wijzigen	Wijzigen RSA Token	Direct	Ja
AAA NAC Profiel			
Aanvragen	Aanvragen AAA toegang voor devices, applicaties of eindgebruikers	Maatwerk	
Opheffen	Opheffen AAA toegang voor devices, applicaties of eindgebruikers	Maatwerk	
Wijzigen	Wijzigen AAA toegang voor devices, applicaties of eindgebruikers	Maatwerk	
Draadloze aansluiting			
Opheffen	Opheffen Draadloze aansluiting op afstand	5	
Wijzigen	Wijzigen instelling bestaande Draadloze aansluiting op afstand	10	

Tabel 19 Bestelbare items categorie Eindsystemen

Levering gebeurt door Quanza – O&A met uitzondering van de Standaard Service Requests, die door Quanza – IB worden uitgevoerd. Voor alle werkzaamheden op locatie wordt SPIE aangestuurd.

AAA RAS gebruiker, Remote Access groepsprofiel en AAA NAC Profiel

Het doel van de dienst Authenticatie, Autorisatie en Accounting (AAA) is om op gecontroleerde wijze toegang tot het netwerk en/of applicaties van RWS mogelijk te maken.

De dienst AAA doet de controle en verificatie aan de hand van de authenticatie/autorisatie gegevens en bestaat uit de volgende onderdelen:

- **Authenticatie:** de verificatie van de aanmeldgegevens, (de identiteitsgegevens van de eindgebruikers die toegang vragen tot het netwerk of applicaties op het netwerk);
- **Autorisatie:** toekennen van toegangsrechten aan de eindgebruiker;
- **Accounting**: consistente administratie en het kunnen verstrekken van aanmeldinformatie over de eindgebruiker en het gebruik.

De dienst AAA biedt:

- Gecontroleerde toegang voor (netwerk)componenten, applicaties en/of eindgebruikers tot de AAA dienstverlening;
- Gecontroleerde toegang tot het netwerk van RWS voor een gebruiker, of RWS beheer mobiel apparaat voorzien van een RWS-certificaat;
- Gecontroleerde toegang tot het netwerk voor IDV-G (Rijkskantoorroam) waarbij de authenticatie wordt afgehandeld door de IDV-G organisatie. RWs is IDV-P in deze situatie.
- Gecontroleerde toegang tot het netwerk en/of applicaties van RWS voor een gebruiker voor het gebruik van Token of SMS Authenticatie.
- Gebruikersauthenticatie met een RSA token;
- Gebruikersauthenticatie met SMS One Time Password (OTP);
- User account synchronisatie met RWS Active Directory ldap(s);
- Selfservice voor RSA tokens (HTTPS).

AAA RAS gebruiker

Deze dienst biedt de mogelijkheid om iemands identiteit met hoge zekerheid, volgens de 'two-factor authenticatie' methodiek vast te stellen en aan de hand hiervan toegang te geven tot het RWS netwerk.

Hierbij wordt gebruik gemaakt van:

1. Gebruikersnaam (accountnaam);
2. Iets wat een gebruiker 'weet' (kennis);
3. Iets wat een gebruiker 'bezit' (token).

Tokens

Er zijn twee soorten tokens beschikbaar:



1. SMS via de eigen telefoon. De verificatie vindt plaats via het versturen van een S naar het voor die gebruiker in de AD van RWS vastgelegde 06-nummer.
2. Een persoonlijke RSA token voorzien van een unieke code die op het scherm van dat token wordt gepresenteerd.



Remote Access Groepsprofiel

Wat een gebruiker of component, na succesvolle authenticatie, mag benaderen op het RWS netwerk wordt bepaald aan de hand van profielen. Deze profielen zijn onderdeel van de dienst Remote Access groepsprofiel. Door het aanvragen van het juiste groepsprofiel is het

mogelijk om via het Internet vanaf een willekeurige locatie en willekeurig apparaat veilig met de binnen het profiel vrijgegeven interne systemen en applicaties van RWS te kunnen werken via een versleutelde verbinding. De dienst is niet bedoeld als machine to machine communicatiemedium.

De dienst Remote Access groepsprofiel is randvoorwaardelijk voor het gebruikmaken van de AAA dienst RAS gebruiker. AAA RAS gebruiker voorziet de gebruiker van een token om succesvol te kunnen authentiseren. In het RAS Profiel zijn de toepassingen en systemen waarvan gebruik gemaakt kan worden gespecificeerd.
Om veiligheidsredenen is de set aan toepassingen en systemen beperkt volgens het 'need to access' principe. In combinatie met de dienst AAA, die een koppeling legt tussen een RAS Profiel, een specifieke Active Directory (AD) user-account en een RAS Token, wordt het mogelijk om succesvol via de RAS dienst op het RWS netwerk in te loggen en de in het RAS profiel beschikbaar gestelde applicaties te gebruiken. Na het succesvol inloggen krijgt de gebruiker een specifieke pagina te zien met daarop de snelkoppelingen (hyperlinks) naar de beschikbaar gestelde interne applicaties en systemen. De inhoud van deze pagina komt overeen met hetgeen in het RAS Profiel was gespecificeerd.
In de RAS server worden RAS profielen conform aanvraag vanuit RWS geconfigureerd. De RAS profielen geven zogezegd toegang tot interne RWS applicaties. De autorisatie van een RAS gebruiker tot een RAS profiel vindt plaats via role mapping.

Voor de dienst RAS Groepsprofiel gelden de in Tabel 20 volgende applicatie en toepassingsvoorwaarden:

Applicatie	Randvoorwaarden gebruiker/randapparaat
Web services (gebaseerd op de http(s) protocollen)	○ Applicaties moeten middels http(s) kunnen werken.
Citrix	○ Citrix ICA Client op Randapparaat
Windows Fileshare/Directories	○ Read-Only (default) of Read-Write. ○ Naar specifieke Share op specifieke Server. ○ Optioneel ook alleen vanaf een specifieke directory (en alle daaronder gelegen directories). ○ Read-Write alleen op basis van een specifieke Risico Analyse. En dit vereist een browser met Java die de Network Connect (*) applicatie kan draaien.
Windows Terminal Services (RDP protocol)	○ Remote Desktop client applicatie (bijvoorbeeld mstsc.exe), ○ user only; hiermee kan men dus niet als admin aanloggen op een remote systeem.
SSH	○ Alleen voor karakter gebaseerde / Virtual Terminal communicatie. ○ Tunneling van andere protocollen is niet toegestaan.

Applicatie	Randvoorwaarden gebruiker/randapparaat
Overige applicaties alleen op basis van transparante netwerktoegang	○ RWS is zeer terughoudend in het toegang verlenen via deze methode, i.v.m. hogere risico's. Deze vorm vereist een specifieke Risico Analyse. ○ Directe communicatie tussen netwerken (Transit verkeer) is expliciet verboden. Hiervoor dient gebruik gemaakt te worden van de dienstbouwsteen Externe Koppeling. ○ Toegang wordt verleend naar specifiek(e) IP adres(sen), Protocol en poort nummer(s). ○ Vereist een browser met Java die de Network Connect applicatie kan draaien.

Tabel 20 Applicatie en toepassingsvoorwaarden RAS Groepsprofiel

De volgende voorschriften gelden voor het definiëren en gebruiken van RAS profielen:

- RAS profielen dienen maximaal van applicatie beveiligingsproxies (bedoeld worden de standaard applicaties zoals rdp, ssh e.d.) gebruik te maken en minimaal van transparante toegang;
- RAS Profielen mogen alleen toegewezen worden aan RAS gebruikers die voor alle applicaties en systemen in het RAS profiel geautoriseerd zijn;
- Het ontsluiten van RWS interne Applicaties en Systemen via de RAS dienst verloopt via een risico afweging en toets ten opzichte van security baseline(s);
- De systeem eigenaar/product manager van de beschikbaar gestelde applicaties, systemen, netwerken en informatie dient expliciet toestemming te geven voor deze netwerk toegang;
- Indien een RAS profiel gebruikt wordt door gebruikers van derde partijen dan moet deze derde partij voldoen aan de NNV aansluitvoorwaarden;
- Ieder RAS profiel dient een benoemde functioneel beheerder te hebben.

Autorisatie middels AAA SMS authenticatie

Voor AAA SMS authenticatie (OTP) wordt voor de profielen de AD benaderd middels LDAPs en is de autorisatie afhankelijk van de AD groepen waar deze gebruiker of dit component deel van uitmaakt. De dienst AAA is beschikbaar voor Verkeersmanagement (VM), het Ministerie van Infrastructuur en Waterstaat (IenW), RWS CIV IRN Infra, BOS en Scheepvaartmanagement (SVM).

De dienst AAA heeft de volgende uitgangspunten:

- De dienst maakt gebruik van een aantal interfaces:
  PIN authenticatie
  - Gebruikers moeten een PIN authenticatie uitvoeren in geval van een RSA-token.

  Token authenticatie
  - De RAS server communiceert met token authenticatie systemen via de RADIUS server;
  - De token authenticatie systemen verifiëren op hun beurt of gebruikers bestaan via een eigen koppeling met de RWS Active Directory;

  - https ingang voor eindgebruikers via een self service portal (SSP) om tokenmanagement uit te voeren (bv pin reset of opgeven van een aflever adres);
  - radius ingang voor de component RAS voor authenticatie en autorisatie van de RAS gebruikers. De autorisatie is een RADIUS attribuut dat de RAS component gebruikt bij mapping op een RAS profiel (met bijbehorende permissies);
  - LDAP(s) uitgang naar de RWS AD omgeving voor het authentiseren van gebruikers die op de SSP inloggen, en voor het synchroniseren van de gebruikersdatabase.
- De dienst ondersteunt de volgende protocollen: TACACS+, RADIUS, LDAPs (Light Weight Directory Access Protocol) en gebruik in combinatie met onder ander PPP , PAP, CHAP, EAP, PEAP, TLS en in bredere zin toegangscontrole middels 802.1x.
- Voor andere componenten en diensten zal per stuk bekeken moeten worden welke interfaces geschikt zijn om van AAA gebruik te kunnen maken. Gebruik van RADIUS of koppeling met de AD middels LDAP(s) behoren tot de mogelijkheden.

Voor de dienstcomponenten van AAA gelden de in Tabel 21 weergegeven voorwaarden:

Dienst component	Voorwaarden
RWS Active Directory	• Gebruiker moet reeds een actief **User-account** hebben in RWS Active Directory. • Bij SMS authenticatie dient het user account ook over een bruikbaar **telefoonnummer** attribuut te beschikken • Bij SMS authenticatie dient het user account ook te zijn opgenomen in een AD groep die correspondeert met een RAS profiel.
Token	• De gebruiker moet een **RSA Token** hebben of krijgen en het serienummer dient daarvan bekend te zijn. Dit is niet van toepassing indien gebruik wordt gemaakt van SMS authenticatie.
Applicaties Autorisatie	• De Gebruiker moet **autorisatie** hebben om de systemen en applicaties te mogen benaderen.
Firewall Rule	• De **Firewalls** dienen de juiste en geautoriseerde toegang mogelijk maken
<ICT-Middelen>	• De Gebruiker moet zelf voorzien in een **internet verbinding**.
	• De Gebruiker moet zelf voorzien in een **ICT-Middel**, zoals een PC, laptop, PDA, smartphone of tablet. De telefoon is essentieel wanneer de gebruiker SMS authenticatie toepast.
	• Het ICT-Middel dient altijd gevrijwaard te zijn van virussen, malware en key loggers; en te voldoen aan het vigerende RWS beveiligingsbeleid.
	• Het ICT-Middel ondersteunt minimaal een standaard **webbrowser** (zoals Internet Explorer of Firefox) met een recente versie (< 3 jaar oud) om de inlogprocedure voor de Remote Access Verbinding te volbrengen.
RAS Gebruiker	• In geval van authenticatie met een 'RSA token', zijn per gebruiker de RWS Active Directory username, het Token-nummer en het RAS Profiel met elkaar gekoppeld. • Wanneer gebruik wordt gemaakt van SMS authenticatie vindt de koppeling plaats via groepslidmaatschap in de RWS active directory en valt de koppeling buiten de dienstbouwsteen

Tabel 21 Voorwaarden dienstcomponenten AAA

Aanvullend geldt het volgende:

- Voor het gebruik van de RSA-Token moet de gebruiker de "Bruikleenovereenkomst ICT-middel" ondertekend hebben. Dit kan middels een notificatie pagina op de Remote Access Service zelf. Dit is niet van toepassing bij het gebruik van SMS tokens;
- RSA tokens en/of telefoons (t.b.v. SMS token codes) mogen niet uit handen gegeven worden;
- RSA tokens dienen niet zichtbaar opgeborgen te worden zodat de gegenereerde tokencodes en het serienummer maximaal afgeschermd zijn voor ongeoorloofde ogen;
- Gebruikers worden geacht geïnformeerd over en bekend te zijn met de fenomenen Social Engineering en Phishing: methoden van afkijken en hoe dit te voorkomen;
- Gebruikers mogen nooit het Token serienummer, PIN-code, tokencode, passcode of wachtwoorden prijsgeven, ook niet aan een helpdesk;
- Gebruikers moeten alert zijn bij het gebruik van sociale media, zodat gevoelige informatie niet indirect prijsgegeven wordt;

- Tokens mogen alleen gebruikt worden op een werkplek met adequate beveiliging tegen malware, keyloggers en screencapture/screenrecorders door middel van anti-malware software;
- Tokens mogen niet gebruikt worden in publieke ruimten zoals cybercafes of op openbare computers;
- Gebruikers moeten bij vermoedens van onrechtmatig gebruik van hun toegang[6], of pogingen daartoe zoals social engineering, dit als security incident melden bij de corporate servicedesk alsmede een directe blokkade aanvragen.

AAA NAC Profiel
Een NAC profiel is een vooraf vastgestelde combinatie van gebruiker, device en gegevens (certificaat/gebruikersnaam-wachtwoord) die bepaalt in welke compartiment (RWS:RWS, WANi, Govroam) dit device of deze gebruiker bij gebruik van de juiste inloggegevens toegang wordt gegeven tot bijbehorende netwerkfaciliteiten (compartiment). Onafhankelijk of deze toegang bedraad of draadloos gevraagd wordt.

Omdat de set gegevens kan wijzigen is het in de PDC mogelijk gemaakt om aanvraag, wijziging en verwijderen van NAC-profielen te bestellen. RWS kan besluiten om gebruik te maken van een nieuw type certificaat, dan betreft het een aanvraag. Ook kan het bijvoorbeeld voor komen dat een realm in een bestaand certificaat type wordt aangepast, dan dient een profiel gewijzigd te kunnen worden. Als RWS besluit om een certificaat type, of authenticatie methode niet meer toe te passen dient deze verwijderd te kunnen worden uit het NAC-profiel.
Het opstellen van een NAC-profiel kan alleen in samenwerking met een Infra adviseur RWS uitgevoerd worden, en bij testen en uitrollen van het NAC-profiel zal RWS middelen ter beschikking dienen te stellen.

Digitale Video aansluiting (niet meer te bestellen)
De Digitale Video aansluiting, weergegeven in Fout! Verwijzingsbron niet gevonden., ten b ehoeve van Analoge Camera's is bedoeld om analoge Pan Tilt Zoom camera's aan te sluiten op digitale apparatuur. De PTZ camera's worden op afstand bestuurd en kunnen worden gedraaid, in- en uitgezoomd en gekanteld. Als onderdeel van deze dienst worden camerabeelden ge-encodeerd en PTZ-signalen gedecodeerd. Het analoge videosignaal type Phase Alternating Line(PAL) wordt standaard omgezet naar een digitaal MPEG2 over IP signaal en het PTZ signaal wordt omgezet naar een serieel RS-485 signaal. Hierdoor kunnen de videobeelden van deze camera's worden bekeken in de Verkeerscentrales. De dienst is geschikt voor inzet in ongeconditioneerde ruimtes. Daarnaast wordt Multicasting ondersteund waardoor er met meerdere monitoren tegelijkertijd naar één camera gekeken kan worden. Deze dienst gaat altijd vergezeld van een LAN Aansluiting.

De Digitale Video aansluiting kent vier varianten:

[6] Bijvoorbeeld als men een logincode ontvangt via SMS, terwijl men niet aan het telewerken is.

- Variant 1: De Camera is gemonteerd op het portaal en wordt middels koperkabel (COAX) aangesloten op de encoder in de bijbehorende wegkantkast.
- Variant 2: De Camera is gemonteerd op een mast. De encoder is gemonteerd in de camera-aansluitkast en wordt middels multi-mode glasvezelkabel aangesloten op de dichtstbijzijnde wegkantkast.
- Variant 3: De Camera is gemonteerd op een mast. De encoder is gemonteerd in de camera-aansluitkast en wordt middels single-mode glasvezelkabel aangesloten op de dichtstbijzijnde wegkantkast.
- Variant 4: De Camera is gemonteerd op een portaal of mast en wordt middels een enkele single mode glasvezelkabel aangesloten op de dichtstbijzijnde CVR.

Voor het aansluiten van digitale (IP) camera's is een LAN-aansluiting type CVR / VOR of Wegkant/Waterkant bestelbaar. Het demarcatiepunt van deze aansluiting is de LAN-poort. Bekabeling vanaf de LAN-poort naar de camera en eventuele media convertor zijn geen onderdeel van de dienst.

PPP aansluiting (niet meer te bestellen)
Deze dienst biedt een serieel (RS232) koppelvlak voor de weg- of waterkanttoepassingen naar de Backbone bedoeld voor communicatie met de Verkeerscentrale. Deze dienst werd typisch toegepast bij DRIPs, TDIs, VRIs en GMS2 en is geschikt voor ongeconditioneerde ruimtes.

Deze dienst in niet langer te bestellen. Er kunnen nog wel wijzigingen aangevraagd worden en de dienst kan opgezegd worden. De opvolgers van deze dienst zijn de Draadloze VPN Aansluiting en de LAN Aansluiting die beiden uitgaan van een LAN koppelvlak.
De Special "PPP met huurlijnverlenging" kan niet worden aangevraagd noch gewijzigd, deze kan alleen worden opgezegd.

TBMS BUS (niet meer te bestellen)
TBMS staat voor Token Bus Master Slave en is een op 802.4 (Token passing) gebaseerd protocol met een door RWS gemodificeerde TCP/IP stack (VOPP) bedoelt voor de specifieke eisen van de wegkantsystemen ((M)WKS).
Deze netwerktoegangsdienst maakt het mogelijk dat wegkantstations, die gebruik maken van partylines, voor de applicatie 'Monica' via het TBMS protocol gekoppeld kunnen worden aan het generieke op ethernet/IP gebaseerde RWS netwerk.

Deze dienst in niet langer te bestellen en er kunnen geen wijzigingen meer aangevraagd worden. De dienst kan uitsluitend opgezegd worden. De SLA van de TBMS dienstverlening is op basis van 'redelijke inspanning'. Onbeschikbaarheid van spare apparatuur kan ertoe leiden dat een storing niet meer kan worden opgelost en een verstoorde TBMS-dienst daarom niet meer operationeel gekregen kan worden.

Draadloze aansluiting (niet meer te bestellen)
De Draadloze aansluiting betreft een aansluiting gebaseerd op een serieel koppelvlak en TCP/IP PPP (point to point protocol) en werd toegepast voor het aansluiten van weg- of waterkant toepassingen als DRIPs, TDI's en Meetnetaansluitingen met een serieel koppelvlak. Omdat er gestreefd wordt naar een all-IP netwerk, wordt dit koppelvlak als 'legacy' gecategoriseerd en is niet meer bestelbaar. De Draadloze aansluiting bestaat uit een (ruggedized) draadloos modem + SIM (Wireless 2G/RS232).

Voor inbouw in weg- of waterkanttoepassingen gelden veelal specifieke montagevoorschriften. Zie hiervoor de desbetreffende documentatie (beschikbaar op de VPR).

Categorie Overig
De categorie Overig biedt een overzicht van de informatie diensten glas en netwerk, ontwerp diensten, impact analyses en RijkskantoorRoam: Rijksverzamelkantoor netwerk functionaliteit op een RWS Kantoor (Provider) en RWS netwerk functionaliteit op een niet RWS (Rijks)Overheid Kantoor (Gebruiker) gebaseerd op standaard PDC Diensten.

Gepland werk Glas
Indien bij aanleg- of renovatieprojecten mutaties in het glasvezelnetwerk van RWS noodzakelijk zijn, dienen aannemers deze activiteiten uit te voeren op basis van een glasadvies van SP-O&A.

Er wordt onderscheid gemaakt tussen de volgende gradaties gepland werk (Tabel 22):

Gepland Werk Glas		
Type	**Kenmerken**	**Deliverables**
Eenvoudig (zonder additionele kosten aan te vragen als RFI)	Als elk punt van toepassing is: * < 4 uur analyse * < 4 uur begeleiding * Begeleiding tijdens kantooruren * * Max. één overleg met RWS-Opdrachtnemer Verwachte tijdsbesteding max 16 uur	* Overzicht van de bezette vezels in de betrokken kabels * Opsomming welke PDC-diensten 'geraakt' worden * Enkelvoudig gerouteerd, zoals camera's * Dubbel gerouteerd, zoals aansluiting via ELDW * Aansluitingen van derden in beheer bij OPSI * Aansluitingen van derden niet in beheer bij OPSI * Onbekende aansluitingen (bezet zonder bekende PDC-dienst of naam gebruiker) * Analyse of de geraakte dubbel-gerouteerde PDC-diensten niet 'toevallig' ook betrokken zijn bij andere werkzaamheden of lopende incidenten. * Analyse welke andere SI's dan DVM-Droog worden geraakt waardoor ook derden geïnformeerd moeten worden en mogelijk CAB ingeschakeld moet worden. * Review Plan van Aanpak RWS-ON * Begeleiden her-indienststelling switches * Informeren SI's en afstemmen met CAB
Standaard	Als één punt van toepassing is: * > 4 uur analyse * > 4 uur begeleiding * Begeleiding buiten kantooruren * * Meer dan één overleg met RWS-Opdrachtnemer Verwachte tijdsbesteding max 40 uur	

Gepland Werk Glas		
Type	**Kenmerken**	**Deliverables**
Projectmatig Small	Als van toepassing is: *Projectmatige begeleiding gewenst en *Vooronderzoek ter plaatse of vooraf testen en/of fysiek vrij schakelen van verbindingen of lokale begeleiding tijdens de werkzaamheden. *Eén dagdeel een monteursteam van 2 man. *Werkzaamheden gedurende max één dag op één tracé. Verwachte tijdsbesteding totaal max 80 uur.	* De onder 'eenvoudig' en 'standaard' genoemde deliverables, en tevens: * Projectcoördinator voor voorbereiding en begeleiding van de werkzaamheden; * Verificatie vooraf in technische ruimtes (CVR e.d.) of bezetting van de kabels overeenkomst met administratie. Control met 'lichttang' of vezels daadwerkelijk bezet zijn. * Verificatie vooraf in technische ruimtes (CVR e.d.) of het vrij schakelen van een verbinding het verwachte effect heeft (testen). * Test op redundantie van verbindingen vooraf (op locatie en/of via beheerssysteem) * Vooraf omsteken van verbindingen in technische ruimtes (CVR e.d.) indien dit uit oogpunt van handhaven verbinding gewenst is. * Vrij schakelen en terugschakelen van verbindingen op de dag van uitvoering. * Tijdens de uitvoering zijn monteurs en een projectcoördinator op locatie aanwezig. * Tijdens de uitvoering zijn een netwerkbeheerder en een back-up beschikbaar voor test en controle via de netwerkmanagementsystemen. Niet inbegrepen is het opgraven, openen en onderzoeken van kabelputten. Dit kan als meerwerk uitgevoerd worden.
Projectmatig Medium	Als van toepassing is: *Projectmatige begeleiding gewenst en *Vooronderzoek ter plaatse of vooraf testen en/of fysiek vrij schakelen van verbindingen of lokale begeleiding tijdens de werkzaamheden. *Drie dagdelen een monteursteam van 2 man. *Werkzaamheden gedurende max één dag op één tracé. Verwachte tijdsbesteding totaal max 130 uur.	
Projectmatig Large	Als één punt van toepassing is: * Meer dan drie dagdelen inzet van een monteursteam. *Werkzaamheden gedurende meerdere dagen *Werkzaamheden op meerdere tracés. Verwachte tijdsbesteding totaal > 130 uur.	

Tabel 22 Gepland werk Glas

Glasadvies

Het glasadvies is bedoeld om in een project, voorafgaand aan de bestelling van PDC-diensten, de aanvrager te ondersteunen in het maken van de juiste keuzes. Uitgangspunt is dat er uitgegaan kan worden van bestaande netwerkarchitectuur, technologie en apparatuur.
Daarnaast wordt beoogd:

- Adequate voorbereiding te doen voor de datanetwerken in een RWS-project om latere bestelling en levering van PDC-diensten snel, effectief en efficiënt mogelijk te maken;
- De opdrachtnemer van RWS te ondersteunen in het maken van de juiste keuzes bij het aanleggen van glasvezelinfrastructuur of benutten van bestaande glasvezelinfrastructuur voor datanetwerken, waarmee een goed te beheren en toekomst vast datanetwerk ontstaat.

Er wordt onderscheid gemaakt tussen drie type adviezen:

Glasadvies		
Type	Kenmerken	Deliverables
Eenvoudig	* <= 2 overleggen *<= 4 lassenleiding tijdens kantooruren * *<= 20km netwerk * Bestaande technologie * Bestaande beheeromgeving	* Advies routering nieuwe infra * Advies gebruik bestaande infra * Advies posities glasvezelkabelputten en kasten * Lasschetsen en routeringsschema uit Cocon * Aanwijzing gebruik glasvezellades in CVR e.d. * Advies te bestellen typen PDC-items * Advies en bestemming over eventuele fasering uitvoering * Afstemming met andere lopende projecten * Adviesrapport
Complex	* <= 4 overleggen *<= 10 lassenleiding tijdens kantooruren * *<= 50km netwerk * Bestaande technologie * Bestaande beheeromgeving	

Maatwerk	* Meer afstemming
	* Groter netwerk
	* Afwijkende technologie
	* Nieuwe beheeromgeving
		Als hierboven, aangevuld met:
		* Inventariseren afwijkende bedrijfsmiddelen
		* Advies posities glasvezelkabelputten en kasten
		* Advies hoe om te gaan met niet-acceptabele afwijkingen
		* Afstemmen en inregelen:
		  * Incidentbehandeling
		  * Onderhoud
		  * Changemanagement
		* Inventariseren gebruik glas door niet-PDC-diensten
		* Eventueel opstellen maatwerk-DAP

Tabel 23 Glasadviezen

Netwerkadviezen
In de RWS Topdesk SelfServicePortal kan via PDC IRN INFRA > NETWERK > NETWERK ADVIES > NETWERKADVIES TYPE EENVOUDIG een Advies aangevraagd worden om te bepalen of een functionele behoefte ingevuld kan worden met PDC leveringen en/of de inzet van SP-O&A medewerk(st)ers.

Dit resulteert in een Advies van het type 'eenvoudig'. Indien blijkt dat de functionele behoefte niet ingevuld kan worden met PDC leveringen dan dient het Service Portfolio Management proces gestart te worden om te komen tot een nieuwe of gewijzigde dienst.

Uurtarieven
Als onderdeel van de dienstverlening biedt SP-O&A de inzet van medewerkers aan bij Projecten en Leveringen. De uurtarieven van onderstaande rollen zijn beschikbaar in het Prijzenblad. In het geval van Leveringen wordt gebruik gemaakt van een strippenkaartconstructie. In een 'Strippenkaart' wordt een aantal uren per rol aangeboden, welke op basis van werkelijk gemaakte uren worden verrekend. De afnemer wordt tijdig op de hoogte gebracht bij dreigende overschrijding van de geplande uren.

Rol	Specificatie
Senior Engineer	Senior netwerk engineer
Engineer	Medior netwerk engineer verantwoordelijk voor het uitvoeren van wijzigingen
Projectleider	De projectleider coördineert PDC- aanvragen en projecten
Project Coördinator	Project Coördinatoren worden ingezet in dienstontwikkelingstrajecten, zowel in de pre-sales als in de projectfase voor het coördineren van dienstontwikkelingsprojecten.
Project Support	Ondersteuning van projecten, zoals PMO-rollen

Tabel 24 Uurtarieven

Bestelbare items en levertijd Informatie- en ontwerpdiensten

Informatie en ontwerp diensten		
Eenmalige dienst	**Toelichting**	**Levertijd in werkdagen (door SP-O&A)**
RFI Glas	Informatieverzoek m.b.t. het RWS glasvezelnetwerk	5
Impactanalyse Glas	Beschrijft de impact van een wijziging aan de RWS glasvezel-infrastructuur	20
Glasadvies	Technisch advies over een wijziging aan de RWS glasvezel-infrastructuur	20
Glasontwerp	Technisch detailontwerp voor een wijziging aan de RWS glasvezelinfrastructuur	20
RFI Netwerk	Informatieverzoek m.b.t. de RWS IT-netwerkinfrastructuur	5
Impactanalyse Netwerk	Beschrijft de impact van een wijziging aan de RWS IT-netwerkinfrastructuur	20
Netwerkadvies	Technisch advies over een wijziging aan de RWS IT-netwerkinfrastructuur	20

Informatie en ontwerp diensten		
Netwerkontwerp	Technisch detailontwerp voor een wijziging aan de RWS IT-netwerkinfrastructuur	20

Tabel 25 Bestelbare items Informatie en Adviesdiensten

Levering gebeurt door Quanza – O&A met uitzondering van de Standaard Service Requests, die door Quanza – IB worden uitgevoerd. Voor alle werkzaamheden op locatie wordt SPIE aangestuurd.

Rijkskantoorroam

De dienst Rijkskantoorroam maakt het mogelijk om RWS panden die zijn aangewezen als Rijksverzamelkantoor te voorzien van een Generieke netwerk infrastructuur Connectivity (RijkskantoorRoam). Anderzijds wordt met deze dienst ook de mogelijkheid geboden om RWS medewerkers gebruik te laten maken van de Generieke netwerk infrastructuur Connectivity in Rijksverzamelkantoren van andere Rijksoverheidsorganisaties.
Rijkskantoorroam is een zogenaamde geïntegreerde dienst; hij wordt samengesteld uit de reeds bestaande diensten VPN aansluiting, WIFI, KA LAN, Virtual Firewall, AAA. Om het de afnemer eenvoudig te maken om Rijkskantoorroam te bestellen hoeft hij alleen in Topdesk de keuze te maken voor een van de twee mogelijkheden en daarna zal SP-O&A benodigde diensten/activiteiten aanbieden:

- Aanvraag/opzegging RijkskantoorRoam RWS Kantoor
- Aanvraag/opzegging RijkskantoorRoam RWS koppeling Rijksorganisatie

Bestelbare items en levertijd RijkskantoorRoam

RijkskantoorRoam		
Eenmalige dienst	**Toelichting**	**Levertijd in werkdagen**
Aanvraag RijkskantoorRoam Provider	standaard Netwerk type Kantoor (redundant en inclusief Wifi) aangevuld met eventuele extra diensten VPN, Virtual Firewall, VPN aansluiting, NAC Profiel, LAN aansluiting type KA en WIFI	In overleg
Opheffen RijkskantoorRoam Provider	Opheffen geïntegreerde diensten	In overleg
Aanvraag RijkskantoorRoam Gebruiker	Een ander (Rijks)Overheid Netwerk aangevuld met de diensten Virtual Firewall en NAC Profiel	In overleg
Opheffen RijkskantoorRoam Gebruiker	Opheffen geïntegreerde diensten	In overleg

Tabel 26 Bestelbare items Rijkskantoorroam

Levering gebeurt door Quanza – O&A. Voor alle werkzaamheden op locatie wordt SPIE aangestuurd.

Beheren IT-netwerkdiensten (Specials)

De Specials bestaan uit:

Verbindingen Lichteiland Goeree – Europlatform

SP-IB levert connectiviteit op de RWS platformen voor de kust van Rotterdam. Ten behoeve van het transport van meetgegevens op de Noordzee wordt gebruik gemaakt van een straalverbinding tussen twee lichteilanden: Lichteiland Goeree (LEG) en Europlatform (EPL).

Service level element	Service level
Beschikbaarheid	
Doelbeschikbaarheid	99,5%
Servicewindow	E8 (365*7*24)
Openstellingtijden servicedesk	24*7 per e-mail en telefonisch
Storingshersteltijd gerekend vanaf vertrek helikopter	95% binnen 16 uur bij dienst verstoord 95% binnen 8 uur bij dienst onderbroken
Maintenance Window	10:00-15:00 in overleg met MKO
Capaciteit	
Throughput	LEG: 10Mb/s EPL: 2Mb/s
Prestaties	
MTU	1.500 Bytes
Packet loss	< 2%
Delay (RTT) typical	< 2ms
Jitter	Delay+jitter < max delay
Convergentiesnelheid	<60s
Multicast support	Ja

Tabel 27 LEG EPL Special

CCM aansluiting

De CCM aansluiting is een VPN Aansluiting Serieel op de CCM server. Het betreft een server die in VicNet staat ten behoeve van camerabediening PTZ. Deze Special kan niet worden aangevraagd of gewijzigd.

Eenmalige Dienst	Toelichting	Levertijd in werkdagen
Opheffen	Beheer Verbindingen LEG-EPL	In overleg
Opheffen	CCM Aansluiting	In overleg

Tabel 28 Bestelbare items Specials

Totaal overzicht SLA Matrix

SLA MATRIX STORINGSHERSTELTIJDEN									
Diensten	Storingshersteltijd in 95% van de gevallen								
	verstoord					onderbroken			
	service window kantoortijden			service window "24/7"		service window kantoortijden		service window "24/7"	
	16	8	4	8	4	8	4	8	4
IDS/IPS				V					V
DWDM				V					V
Mailrelay				V					V
Forward webproxy				V					V
VPN		V		V		V			V
Virtual firewall				V					V
DDI - DHCP & DNS				V					V
DDI - IPAM				V					V
DMZ en DMZ client				V					V
VPN aansluiting				V			V		V
Draadloze VPN aansluiting				V					V
Externe koppeling	V					V			
RKN aansluiting		V							V
Lan aansluiting type Gebouw	V			V			V		V
Lan aansluiting type KA	V			V			V		V
Lan aansluiting type Rekencnt	V			V					V
Lan aansluiting type SPAN	V			V			V		V
Lan aansluiting type CVR/VOR				V					V
Lan aansluiting type Callcenter				V					V
Lan aansluiting type Wegkant/Waterkant				V					V
Lan aansluiting type Offshore	-	-	-	-	-	-	-	-	-
Lan aansluiting type ODC				V					V
KA LAN				V			V		V
WIFI		V				V			
Open WIFI		V				V			
Digitale Video Aansluiting				V					V
Remote Access groepsprofiel				V					V
AAA RAS Gebruiker		V					V		
AAA NAC Profiel				V					V
PPP aansluiting*	-	-	-	-	-	-	-	-	-
TBMS BUS*	-	-	-	-	-	-	-	-	-
Draadloze aansluiting*	-	-	-	-	-	-	-	-	-
LEG EPL				V					V
CCM aansluiting				V					V

*	Op basis van 'redelijke inspanning'

Tabel 29 Storingshersteltijden van de verschillende netwerkdiensten

Bijlage A Afkortingen en Begrippen

Afkortingen

Overzicht van de in deze catalogus gebruikte afkortingen en hun betekenis.

Afkortingen	
RWS	Rijkswaterstaat
RWS CIV IRN Infra Netwerken	Rijkswaterstaat Centrale Informatie Voorziening Infrastructuur Netwerken
NNV	Nieuwe Netwerk Voorzieningen
VPN	Virtual Private Network
DDI	De dienst die bestaat uit DHCP DNS en IPAM
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Services
IPAM	Internet Protocol Adres Management
DMZ en DMZ Client	een Demilitarised Zone (beveiliging laag) en Demilitarised Zone Client (DMZ Aansluiting)
NTP	Network Time Protocol
WoL	Wake on LAN
IPsec	Internet Protocol Security
VO LAN	VPN Ontsluiting LAN
CE	Client Edge
LAN	Local Area Network
KA-LAN	Kantoor Automatisering LAN
CVR	Centrale VicNet Ruimte
VOR	VicNet Object Ruimte
ODC	Overheid Data Center
VC/VP	Verkeerscentrale/Verkeerspost
VLAN	Virtueel LAN (VLAN)
DRIP	Dynamisch Route Informatie Paneel
DOV	Dynamische Openbare Verlichting
TDI	Toerit Dosering Installatie
VRI	VerkeersRegel Installatie
VAD	Vluchthaven Aanwezigheid Detectie
WIM	Weigh in Motion (ten behoeve van het wegen van vrachtwagens)
CADO	Calamiteiten Doorsteek
MTV	Motorway Traffic Video
UWP	Universeel Wegkant Platform
LEF	Het Future Center van RWS waar innovatie centraal staat. LEF is geen afkorting, maar staat voor lef, durf en moed. Voor het verleggen van grenzen
SSID	Service Set Identifier
AP's	Access Points
QoS	Quality of Service
APN	Access Point Name
Wi-Fi	Wireless Fidelity

Afkortingen	
AAA	Authenticatie Autorisatie Accounting
WLAN	Wireless Local Area Network
LCM	Lifecycle Management
FEP	Front End Processor
PTZ	Pan Tilt Zoom
PAL	Phase Alternating Line
IP	Internet Protocol
SIM	Subscriber Identity Module
MTM	Motorway Traffic Management
PLCS	Party Line Crossover Switch
ON	Opdracht Nemer
RSA	Merknaam
RAS	Remote Access Services
OTP	One Time Password
AD	Active Directory
RDP	Remote Desktop Protocol
LDAP	Lightweight Directory Access Protocol
VWS	Verkeersmanagement Services
IenW	Infrastructuur en Waterstaat
SVM	Scheepvaart Management
SSP	Self Service Portal
GMS	Gladheidsmeldsystemen
TBMS	Token Bus Master Slave
WKS	Wegkant Systemen
MWKS	Mobiele Wegkant Systemen

Tabel 30 Afkortingen

Begrippen

Toelichting op de in deze catalogus gebruikte begrippen.

Begrippen	
Prijzenblad	Overzicht van alle bestelbare items inclusief eenmalige kosten en abonnementen
Categorie VPN	Alle diensten welke onderdeel uitmaken van de categorie Virtual Private Network
Categorie VPN Aansluiting	Alle diensten welke onderdeel uitmaken van de categorie Virtual Private Network Aansluiting
Categorie LAN Aansluiting	Alle diensten welke onderdeel uitmaken van de categorie Local Area Network
Categorie Eindsysteem	Alle diensten welke onderdeel uitmaken van de categorie Eindsysteem (toepassingen voor eindsystemen)
Categorie Backbone	Alle diensten welke onderdeel uitmaken van de categorie Backbone/Core/CV omdat deze onderdeel uitmaken van het backbone netwerk van Rijkswaterstaat en uitsluitend door RWS CIV te bestellen zijn
Categorie Special	Alle diensten welke geen onderdeel uitmaken van de Categorie VPN, VPN Aansluiting, LAN Aansluiting, Eindsysteem en Backbone en uitsluitend door RWS CIV te bestellen zijn

Begrippen	
RWS netwerk	Het netwerk van Rijkswaterstaat voorheen bekend als "Rijkswaterstaat Nieuwe Netwerk Voorzieningen"
Object Access Netwerken	Object LAN
Kunstwerken	Rijkswaterstaat benaming voor objecten als bruggen, sluizen, tunnels
Huurlijnen	Transmissielijnen van andere partijen dan Rijkswaterstaat zelf, waarover verkeer van Rijkswaterstaat loopt
Aansluitvoorwaarden NNV (CIV)	De voorwaarden waaraan moet worden voldaan om gebruik te maken van het RWS netwerk
Topdesk	De Service Portal van Rijkswaterstaat. Via deze portal kunnen bestelbare
Bulklevering	Levering van een groot aantal bestelbare items in één bestelling
Service Portfolio Management proces	Het proces ingericht om het dienstenportfolio up to date te houden, nieuwe diensten te ontwikkelen, bestaande diensten aan te passen en verouderde diensten uit te faseren
Internet Access	De VPN functie die het mogelijk maakt om toegang tot het internet te verkrijgen
DDI	De dienst die bestaat uit DHCP DNS en IPAM
Mail relay	Configuratie die het mogelijk maakt e-mail berichten te versturen via een SMTP-server
Virtual Firewall	Firewall service in een virtuele omgeving die doormiddel van software communicatie controleert
NTP	Network Time Protocol: maakt het mogelijk om de interne klok van computers met elkaar te kunnen synchroniseren
RWS Backbone	Centrale netwerk-infrastructuur van Rijkswaterstaat
Ruggedized	Verharde apparatuur geschikt voor ongeconditioneerde ruimten
Shaping	Methode om bandbreedte te verdelen zodat data niet verloren gaat en er geen capaciteitstekort ontstaat
Transmissie	Doorlaten van verkeer via verbinding
Wake on LAN	Netwerkstandaard waarmee het mogelijk is een computer op afstand te benaderen
Encrypted Tunnel	Een beveiligde Internet verbinding waarover data versleuteld verzonden wordt
IPsec	Internet Protocol Security
IPsec Gateway	Internet Protocol Security netwerkpunt dat voorziet in toegang tot een netwerk
Externe locatie	Locatie buiten het RWS netwerk
CE domein	Een Custom Edge Router domein
VO LAN	VPN Ontsluiting LAN Configuratie op de router om de LAN-aansluiting te ontsluiten naar het VPN
VPR	RWS SharePoint
LAN domein	Gescheiden deel van het Local Area Network
Routering	Het bepalen van de route die door informatie via het netwerk wordt afgelegd
Centrale VicNet Ruimte	voornamelijk kleine gebouwen op knooppunten van snelwegen waarbinnen een geconditioneerde ruimte aanwezig is voor actieve netwerk apparatuur.

Begrippen	
	Dit betreft een oude benaming die voorlopig vanwege de herkenbaarheid wordt gehandhaafd.
VicNet Object Ruimte	dit zijn geconditioneerde ruimtes voor actieve netwerk apparatuur binnen objecten zoals tunnels, sluizen, bruggen, radarposten en dergelijke. Dit betreft een oude benaming die voorlopig vanwege de herkenbaarheid wordt gehandhaafd.
LAN ontsluiting	de logische koppeling naar een specifiek VPN
VLAN	Virtueel LAN in de fysieke infrastructuur (bijvoorbeeld de switches)
LAN Aansluiting	de fysieke poort die toegang biedt naar het virtuele LAN
Ethernet infra	dit is de fysieke infrastructuur (bekabeling en switches)
RWS Netwerk LAN	Alle LAN Aansluitingen in het Rijkswaterstaat netwerk met uitzondering van KA-LAN, ODC LAN en WIFI
Duplex instelling	Het protocol voor verzenden en ontvangen van informatie op de LAN Aansluiting
Trunking	Meerdere VLAN's op één fysieke poort
Port channeling	Combineren van de capaciteit switches
Spanning-tree protocol	Protocol dat er voor zorgt dat er slechts één pad mogelijk is voor het zenden van informatie, waarmee ontvangst gegarandeerd wordt.
loop-free topologie	Netwerk waarin loopvorming niet mogelijk is
PTZ Camera	op afstand bestuurbare camera die kan worden gedraaid, in- en uitgezoomd en gekanteld

Tabel 31 Begrippen

Bijlage B Overzicht tabellen

Tabel 1 Beschikbaarheid Backbone diensten 8
Tabel 2 Overzicht CVR locaties in scope 14
Tabel 3 Bestelbare items IDS/IPS 16
Tabel 4 Dienstenmatrix VPN – diensten 17
Tabel 5 Bestelbare items VPN diensten 24
Tabel 6 Bestelbare items categorie LAN aansluiting 28
Tabel 7 IT-netwerkdiensten CIV Klant 33
Tabel 8 VPN functionaliteiten 36
Tabel 9 Dienstenmatrix VPN – diensten 37
Tabel 10 Bestelbare items VPN diensten 38
Tabel 11 Dienstenmatrix categorie VPN - aansluiting 39
Tabel 12 Bestelbare items categorie VPN aansluiting 41
Tabel 13 Vaste verbindingen ODIDO 53
Tabel 14 Beschikbaarheids eisen LAN aansluiting 55
Tabel 15 Bestelbare items categorie LAN aansluiting 56
Tabel 16 Opties type KA LAN 59
Tabel 17 Overzicht gebruikersgroepen WIFI en Open WIFI 62
Tabel 18 Beschikbaarheids eisen Eindsystemen 64
Tabel 19 Bestelbare items categorie Eindsystemen 65
Tabel 20 Applicatie en toepassingsvoorwaarden RAS Groepsprofiel 68
Tabel 21 Voorwaarden dienstcomponenten AAA 70
Tabel 22 Gepland werk Glas 74
Tabel 23 Glasadviezen 75
Tabel 24 Uurtarieven 76
Tabel 25 Bestelbare items Informatie en Adviesdiensten 77
Tabel 26 Bestelbare items Rijkskantoorroam 77
Tabel 27 LEG EPL Special 78
Tabel 28 Bestelbare items Specials 78
Tabel 34 Storingshersteltijden van de verschillende netwerkdiensten 79
Tabel 35 Afkortingen 81
Tabel 36 Begrippen 83

Bijlage C Overzicht figuren

Figuur 1 Scope IT-netwerkdiensten 5
Figuur 2 DWDM in het netwerk 11
Figuur 3 LAN infrastructuur ODC 26
Figuur 4 Dark Fiber uitvoering 29
Figuur 5 Aansluitvariant Handhole 30
Figuur 6 Aansluitvariant Patchpaneel 31
Figuur 7 Schematische weergave van de VPN aansluiting 41
Figuur 8 Beschikbaarheid VPN Aansluiting 43
Figuur 9 Standaard routering VPN Aansluiting 44
Figuur 10 Statische routering VPN Aansluiting 44
Figuur 11 Dynamische routering - VPN Aansluiting Connect 45
Figuur 12 Dynamische routering - VPN Aansluiting InterConnect 46
Figuur 13 Schematische weergave draadloze VPN Aansluiting 48
Figuur 14 IPSEC 50
Figuur 15 IPsec + MCPE 51
Figuur 16 Voorbeeld redundante vaste verbinding 51

Bijlage R Bijlagen Bedrijfsvoering Elektrische Installaties RWS

Rijkswaterstaat
Ministerie van Infrastructuur en Waterstaat

Bijlage R Bijlagen Bedrijfsvoering Elektrische Installaties

Bijlage bij Vraagspecificatie Proces

D&C Vervanging Verlichting Schipholtunnel
Zaaknummer: 31212908

Bijlage R1: NEN 3140 Veiligheidshandboek Rijkswaterstaat
Bijlage R2: NEN 3140 Veiligheidshandboek Rijkswaterstaat addendum
Bijlage R3: NEN 3840 Veiligheidshandboek Rijkswaterstaat

Bijlage R1 NEN 3140 Veiligheidshandboek Rijkswaterstaat

Rijkswaterstaat
Ministerie van Infrastructuur en Milieu

NEN 3140 Veiligheidshandboek
Rijkswaterstaat

Werken met en aan laagspanningsinstallaties

Voor intern- en extern gebruik

Datum Februari 2015
Versie 2.0
Status Definitief

Functie	Naam	Paraaf	Datum
Opsteller	G. Bruggink		25-02-2015
Gecontroleerd	C. Wilschut		25/2/2015
Vrijgegeven	P.A.M. Smeets		25/2/15
Opdrachtgever	T.F.J. Van de Gazelle		13/3/15

Rijkswaterstaat
Ministerie van Infrastructuur en Milieu

Colofon

Uitgegeven door	Rijkswaterstaat
Informatie	G. Bruggink, C. Wilschut
Telefoon	088-7972144, 088-7973468
Fax	
Uitgevoerd door	G. Bruggink – RWS-GPO C. Wilschut – RWS-GPO N. Brouwer – externe bij RWS-WVL M. Hollanders – RWS-PPO
Opmaak	
Datum	Februari 2015
Status	Definitief
Versienummer	2.0

Revisiehistorie

Versie	Datum	Beschrijving wijzigingen	Uitgevoerd	Distributie
0.1	2009	Initieel document van RWS-DZH	RWS-DZH	Intern
0.2	2011	Aangepast document van RWS-DNB en aangepast aan de nieuwe NEN 3140:2011	RWS-DNB	Intern
0.3	Maart 2012	Aanpassingen aan ontwikkeling kader-BEI	M. Hollanders	Intern
0.4	Oktober 2012	Aanpassingen aan kader-BEI	N. Brouwer	Intern
1.0	November 2012	Layout RWS-standaard	G. Bruggink	In/Extern
1.1	Januari 2013	De taken en verantwoordelijkheden van de NEN3140-functies in hoofdstuk 5 toegevoegd, zodat dit document zonder de "Handleiding BEI" extern kan worden gebruikt.	G. Bruggink	In/Extern
1.2	Mei 2013	Benamingen gesynchroniseerd	G. Bruggink	In/Extern
1.3	Juli 2013	Type objecten alomvattend gemaakt, aanpassen aan OP2015	G. Bruggink	Opdrachtgever
2.0	Februari 2015	Kleine verbeteringen met verwijzingen naar norm, overdracht naar COP BEI	G. Bruggink	RWS

Inhoud

1 Inleiding 6
1.1 Doel, doelgroep en scope van dit document 6
1.2 Status document en gebruik 6
1.3 Aanleiding en achtergrond 6
1.4 Plaats binnen arbo 6
1.5 Leeswijzer 6
1.6 Openstaande punten 6
2 Werken met elektriciteit 7
2.1 Normen en wetgeving voor een veilige bedrijfsvoering van elektrische installaties en elektrische arbeidsmiddelen 7
2.2 NEN 3140:2011 bij Rijkswaterstaat 8
2.3 NEN 3840:2011 bij Rijkswaterstaat 8
3 Termen en definities 9
3.1 Algemeen 9
3.1.2 Elektrisch arbeidsmiddel 9
3.1.3 Bedrijfsvoering 10
3.1.4 Risico 10
3.1.6 Letsel (elektrisch) 10
3.1.101 Elektrisch arbeidsmiddel 10
3.1.102 Actief deel 11
3.2.1 Functioneel Installatieverantwoordelijke (F-IB) en Technisch Installatieverantwoordelijke (T-IV) 11
3.2.2 Werkverantwoordelijke (WV) 11
3.2.3 Vakbekwaam persoon (VP) 12
3.2.4 Voldoend onderricht persoon (VOP) 12
3.2.5 Leek 12
3.2.6 Bericht of aanwijzing [vervallen in 3140:2011] 12
3.3 Werkzones 13
3.3.1 Werkplek 13
3.3.2 Gevarenzone 13
3.3.3 Nabijheidszone [vervallen in 3140:2011] 13
3.3.101 Aanrakingsveilig 13
3.4 Arbeid 13
3.4.1 Werkzaamheden 13
3.4.2 Elektrotechnische werkzaamheden 13
3.4.3 Niet-elektrotechnische werkzaamheden 13
3.4.4 Onder spanning werken 14
3.4.5 Werken in de nabijheid van actieve delen [vervallen in 3140:2011] 14
3.4.6 Scheiden 14
3.4.7 Spanningsloos 14

3.4.8 Spanningsloos werken 14
3.5 Beschermingsvoorzieningen 14
3.5.1 Scherm 14
3.5.2 Afscherming 14
3.5.3 Isolerend omhulsel 14
3.5.4 Omhulsel [vervallen in 3140:2011] 15
3.6 Spanningen 15
3.6.1 Extra lage spanning (ELV) 15
3.6.2 Lage spanning (LV) 15
3.6.101 S-keten 16
3.101 Toezicht 16
3.101.1 Ononderbroken toezicht 16
3.101.2 Regelmatig toezicht 16
4 Onderwerp en toepassingsgebied 17
5 Functies volgens NEN3140 19
5.1 De installatieverantwoordelijke 19
5.2 Werkverantwoordelijke 20
5.3 Vakbekwaam Persoon 21
5.4 Voldoende Onderricht Persoon 21
5.5 Ploegleider [alleen bij hoogspanninginstallaties] 22
5.6 Bedieningsdeskundige [alleen bij hoogspanninginstallaties] 22
5.7 Leek 22
6 Voorschriften van de voldoende onderrichte personen in dienst van Rijkswaterstaat 23
7 Overdracht taken aan contractpartijen: aanvullende eisen 25
7.1 Het aanwijzen van personeel van contractpartijen 25
7.2 Het veilig uitvoeren van werkzaamheden 26
7.3 Bevoegdheden en verantwoordelijkheden van extern personeel 27
8 Algemene werkvoorschriften en werkprocedures 28
8.1 Algemene Veiligheidsmaatregelen 28
8.2 Werkprocedures 29
8.2.1 Spanningsloos werken 30
8.2.2 Volledig scheiden 30
8.2.3 Beveiligen tegen wederinschakeling 31
8.2.4 Controleren of de installatie spanningsloos is 31
8.2.5 Aarding en kortsluiting 31
8.2.6 Bescherming ten opzichte van naastgelegen actieve delen 31
8.2.7 Toestemming om met de werkzaamheden te beginnen 31
8.2.8 Opnieuw inschakelen na de werkzaamheden 31
8.2.9 Onder spanning werken 32
8.2.10 Werken in de nabijheid van niet voldoende geïsoleerde actieve delen 32
8.3 Werkzaamheden bij risicoverhogende omstandigheden 32
8.3.1 Werkzaamheden in ongunstige weersomstandigheden 32

8.3.2 Werkzaamheden in vochtige omgevingen 32
8.3.3 Werkzaamheden in accuruimten, accukasten en acculaadstations 33
8.3.4 Werkzaamheden in omgevingen met ontploffingsgevaar 33
8.3.5 Brandpreventie en brandbestrijding 34
8.4 Sleutelplan 34
8.5 Rapportage 35
8.6 Risicoanalyses 35
8.7 Verantwoordelijkheid 35
8.8 Tekeningen en documenten 35
9 Bepalingen met betrekking tot inspecties, inspectiefrequenties en steekproeven 36
9.1 Toe te passen normen 36
9.2 De inspectiefrequentie 37
9.3 Het toepassen van steekproeven 37
9.4 De inspectie 37

Bijlage A Hulplijst voor vragen in een RIE bij Rijkswaterstaat 40

Bijlage B Handreiking voor het door de ON op te stellen Werkplan BEI voor een object of regio 42
B.1 Doel 42
B.2 Voor welk object of regio? 42
B.3 Algemene normen, richtlijnen en overige documenten 42
B.4 Inzet van personeel en gereedschappen 42
B.5 Invulling van de bedrijfsvoering 43
B.6 Procedures 43
B.7 Rapportages 43
B.8 Escalatiemodel 43
B.9 Overzicht van tekeningen en documenten 43
B.10 Calamiteiten 44
B.11 Storingswerkzaamheden 44

1 Inleiding

1.1 Doel, doelgroep en scope van dit document

Dit document heeft als doel dat de veiligheid van werken met en aan elektrische installaties op een hoog niveau wordt gebracht en op dat hoge niveau blijft gehandhaafd ten einde ongevallen als gevolg van elektriciteit te voorkomen.

1.2 Status document en gebruik

Het document Veiligheidshandboek Rijkswaterstaat NEN 3140 heeft in het verleden enkele regionale voorgangers gehad die als dan niet met behulp van externen zijn opgesteld. Het gebruik van dit document is vooral bedoeld voor:

- internen Rijkswaterstaat: diegenen die met elektriciteit omgaan, zowel procesmatig als in beheer en onderhoud (objectbeheerders, weginspecteurs, contractbeheerders, bedienaars)
- externen: diegenen die in opdracht van Rijkswaterstaat werkzaamheden verrichten met of aan elektrische installaties.

1.3 Aanleiding en achtergrond

De aanleiding van dit document is het brengen van eenheid binnen Rijkswaterstaat van alle documenten die op dit gebied in de loop van de tijd zijn ontstaan en niet aan de nieuwste normen zijn aangepast.

De achtergrond van dit document is het arbobesluit die voorschrijft dat een eigenaar van een asset, waar elektriciteit gebruikt wordt, veilig met zijn installaties omgaat en zorgt draagt voor een goede inrichting van zijn beheer van deze installaties. De nieuwe NEN 3140:2011 geeft hiervoor een goede opzet. Deze is waar nodig specifiek aan de organisatie van Rijkswaterstaat aangevuld en verwoord in dit document.

1.4 Plaats binnen arbo

Bij Rijkswaterstaat worden de Arbeidsomstandighedenwet en het Arbeidsomstandighedenbesluit uitgevoerd. Dit document geeft de normering voor het veilig beheer van elektrische installaties en elektrische arbeidsmiddelen weer.

1.5 Leeswijzer

In hoofdstuk 2 is een algemene tekst over werken met elektriciteit.
In hoofdstuk 3 worden de te hanteren definities binnen de NEN 3140:2011 nader toegelicht voor de specifieke organisatie van Rijkswaterstaat.
In hoofdstuk 4 wordt het toepassingsgebied gedefinieerd.
In hoofdstuk 5 wordt een invulling van de installatieverantwoordelijkheid bij Rijkswaterstaat gegeven.
In hoofdstuk 6 wordt nader ingegaan hoe medewerkers van Rijkswaterstaat en Opdrachtnemers moeten acteren.
Hoofdstuk 7 geeft kort weer de invulling van het overdragen van taken aan externen.
In hoofdstuk 8 worden de algemene procedures en voorschriften weergegeven.
Hoofdstuk 9 geeft het proces van inspecteren weer.
De bijlage A geeft een hulpvragenlijst voor het maken van een RIE.
Tot slot geeft Bijlage B een aanwijzing wat een door de Opdrachtnemer te maken werkplan BEI voor inhoud moet hebben.

1.6 Openstaande punten

Geen.

2 Werken met elektriciteit

Bij het gebruik van en het werken aan elektrische installaties en bij het gebruik van elektrische arbeidsmiddelen bestaat een zeker risico op letsel. Letsel kan worden veroorzaakt door:

- elektrische schokken
- elektrische verbrandingen
- brand voortkomend uit elektrische energie
- explosies voortkomend uit elektrische energie
- krachten die vrijkomen bij sluitingen

Om deze risico's te beperken moeten elektrische installaties en elektrische arbeidsmiddelen voldoen aan een groot aantal veiligheidseisen. Deze eisen staan in verschillende normen, regels en richtlijnen vermeld.

Voor de veilige bedrijfsvoering van elektrische installaties en elektrische arbeidsmiddelen is de norm NEN 3140:2011 van toepassing.

2.1 Normen en wetgeving voor een veilige bedrijfsvoering van elektrische installaties en elektrische arbeidsmiddelen

Sinds 1991 is er een geaccepteerde norm voor het werken aan en met elektrische laagspanningsinstallaties en elektrische apparaten. Dit is momenteel de NEN 3140:2011 (Laagspanningsinstallaties, bedrijfsvoering van elektrische installaties, vierde druk).

Het doel van NEN 3140:2011 is voor Nederland de algemene eisen voor de veilige bedrijfsvoering van en werkzaamheden aan, met of nabij elektrische installaties te geven.

Bedrijfsvoering van elektrische installaties omvat zowel het gebruik van elektrische installaties in het arbeidsproces, het kunnen laten functioneren van elektrische arbeidsmiddelen als het werken aan of nabij installaties vanwege aanleg, onderhoud, reparaties, uitbreidingen en sloop.

In 2011 is van de norm NEN 3140 een vierde druk verschenen. Er zijn diverse redenen waarom de norm ingrijpend moest veranderen:

- de ervaring van het werken met de norm sinds 1991
- de gewijzigde Arbowetgeving
- de gegroeide praktijk
- de Europese normering

De Nederlandse normering op het gebied van laagspanningsinstallaties en elektrische arbeidsmiddelen heeft betrekking op:

- de veilige bedrijfsvoering
- het onderhoud
- de inspectie
- het beheer

Normen zijn vastgelegde technische en procedurele afspraken waarover de betrokken belanghebbende groeperingen het eens zijn. Het feit dat normen bestaan, betekent niet automatisch dat men verplicht is om de normen toe te passen.

Het Arbeidsomstandighedenbesluit (Arbobesluit) is een geïntegreerd besluit van alle besluiten die momenteel behoren bij de Arbeidsomstandighedenwet.

In de beleidsregel bij het Arbobesluit zijn de relevante elektrotechnische normen aangegeven. Indien de genoemde normen voor de verschillende elektrische

installaties zijn toegepast, is voldaan aan de verplichtingen van het Arbobesluit. Ook de NEN 3140:2011 wordt in de beleidsregel genoemd.

Ook indien niet op enige wijze schriftelijk is vastgelegd dat de NEN 3140:2011 moet worden toegepast, kan op grond van gewoonte en gebruik de rechter van oordeel zijn dat deze norm had moeten worden toegepast. We noemen dit het 'gewoonterecht'. Naarmate de norm steeds meer algemeen wordt gebruikt, zal het gewoonterecht belangrijker worden.

2.2 NEN 3140:2011 bij Rijkswaterstaat

Bij Rijkswaterstaat worden de Arbeidsomstandighedenwet en het Arbeidsomstandighedenbesluit uitgevoerd. Ook met betrekking tot de normering voor het veilig beheer van elektrische installaties en elektrische arbeidsmiddelen.

De normering voor laagspanningsinstallaties is vastgelegd in de NEN 3140:2011, vierde druk. Voor Rijkswaterstaat is de toepassing van deze norm, op grond van het beleid verplicht op alle elektrotechnische werkzaamheden en bij het gebruik van elektrische arbeidsmiddelen.

Binnen Rijkswaterstaat bestaat de verplichting een aanwijzing te geven aan de F-IB (functioneel installatiebeheerder) en de T-IV (technisch installatieverantwoordelijke). Nadere uitgangspunten van deze twee rollen zijn vermeld in het (intern Rijkswaterstaat-)document "Handleiding Bedrijfsvoering Elektrische Installaties". De benodigde informatie hieruit is opgenomen in hoofdstuk 5.

Een aanwijzing is een schriftelijke bevestiging dat het inzicht en de vaardigheid aanwezig zijn om bepaalde werkzaamheden uit te voeren.

Een goed veiligheidsbeleid kan alleen maar worden gevoerd als vooraf wordt bepaald wie welke werkzaamheden mag uitvoeren en welke instructies daarvoor nodig zijn. Bij de aanwijzing van personen moet rekening worden gehouden met opleiding, ervaring en de omstandigheden waaronder gewerkt moet worden.

Normalisatie is een voortdurend proces van veranderen. Ieder die verantwoordelijkheid draagt voor een veilige bedrijfsvoering en een veilig beheer van elektrische installaties en elektrische arbeidsmiddelen, moet zich voortdurend op de hoogte houden.

Dit veiligheidshandboek is een invulling van de norm NEN 3140:2011 in het veiligheidsbeleid van Rijkswaterstaat. Alleen die onderdelen van de norm die van toepassing zijn voor Rijkswaterstaat zijn in dit veiligheidshandboek opgenomen.

De verplichting tot het naleven van de NEN 3140:2011 is onderdeel van de arbeidsovereenkomst of de detacheringsovereenkomst of onderdeel van de overeenkomst tot het verrichten van diensten of aanneemovereenkomsten voor het uitvoeren van werkzaamheden, in welke vorm dan ook als niet expliciet naar deze normen wordt verwezen.

Waar in individuele overeenkomsten nog niet specifiek naar deze wettelijke verplichting wordt verwezen kan eenvoudig worden verwezen naar dit Veiligheidshandboek Rijkswaterstaat.

Dit veiligheidshandboek is een onderdeel van de huisregels welke gelden op alle (elektrotechnische) installaties waar Rijkswaterstaat de verantwoordelijkheid draagt voor veilige arbeidsomstandigheden.

2.3 NEN 3840:2011 bij Rijkswaterstaat

Hoogspanning is dermate specialistisch en is niet in dit NEN 3140 Veiligheidshandboek beschreven.

3 Termen en definities

In dit hoofdstuk worden een aantal definities gegeven van begrippen uit de NEN 3140:2011, die in dit veiligheidshandboek worden gebruikt. Indien noodzakelijk wordt de definitie daarna verder uitgediept om het begrip, in het kader van dit veiligheidshandboek, te verduidelijken.

3.1 Algemeen

3.1.1 Elektrische installatie

De elektrische installatie omvat al het elektrisch materieel ten behoeve van de opwekking, het transport, de omzetting, de distributie en het gebruik van elektrische energie. Inbegrepen zijn energiebronnen zoals accu's, batterijen, condensatoren en alle andere bronnen van opgeslagen elektrische energie. [Cursieve tekst komt uit de norm NEN 3140:2011]

Toelichting

De norm NEN 3140:2011 is van toepassing op al het elektrisch materieel. Ook het elektrische materieel dat niet aangesloten is of nooit aangesloten wordt op een vaste elektrische installatie, valt onder deze norm.
De elektrische uitrusting van machines, zoals die geregeld is met NEN-EN 60204-1, valt ook onder de definitie van de elektrische installatie binnen het werkingsgebied van de norm NEN 3140:2011.

3.1.2 Elektrisch arbeidsmiddel

Een elektrisch arbeidsmiddel is elk op de arbeidsplaats gebruikte machine, gereedschap, apparaat en hulpmiddel, dat door de aard van hun gebruik of omgevingsomstandigheden een elektrisch veiligheidsrisico kan opleveren.

Toelichting

Onder elektrische arbeidsmiddelen valt alles dat wordt gebruikt in een arbeidsomgeving, waarbij elektrische energie wordt toegepast. Het maakt daarbij niet uit of het arbeidsmiddel vast is aangesloten of is aangesloten met stekker en contactdoos en een flexibele leiding. Ook apparatuur die tijdens gebruik niet wordt gevoed vanuit een installatie, valt onder het begrip van de elektrische arbeidsmiddelen, voorbeelden van deze accu-apparatuur zijn de gsm-telefoon en de zaklamp.

We moeten bij elektrische arbeidsmiddelen niet alleen denken aan boormachines, bouwlampen of elektrisch gereedschap, maar aan alle elektrische apparatuur die binnen Rijkswaterstaat gebruikt wordt.

Zo gebruiken medewerkers ondermeer computers en kopieerapparaten.

Op werkplekken staan vaak elektrische koffiezetapparaten, waterkokers en elektrische kachels.

Een radio, een TV, een elektrische straalkachel, een elektrische handendroger zijn andere voorbeelden van elektrische apparaten die bij de arbeid worden toegepast en dus tot de elektrische arbeidsmiddelen behoren.

Tenslotte is het van belang om te weten dat ook verlengsnoeren, snoercentrales (de zogenaamde verdeeldoos of slof) en haspels tot de elektrische arbeidsmiddelen worden gerekend.

Al deze apparaten worden tot de elektrische arbeidsmiddelen gerekend.

Het is de zorg van Rijkswaterstaat, dat de apparaten veilig zijn. Eventueel kan deze zorg worden overgedragen aan derden. Hiervoor moeten dan in contracten met de betreffende bedrijven afspraken gemaakt worden.

3.1.3 Bedrijfsvoering

Onder bedrijfsvoering verstaan we alle handelingen met inbegrip van werkzaamheden die noodzakelijk zijn om de elektrische installatie onder alle omstandigheden te kunnen laten werken. Tot deze handelingen behoren schakelen, regelen, bewaken en onderhoud evenals elektrotechnische en niet-elektrotechnische werkzaamheden met elektrotechnische gevaren.

3.1.4 Risico

Onder risico verstaan we een combinatie van de waarschijnlijkheid en de mate van mogelijk letsel of schade aan de gezondheid van een persoon die is blootgesteld aan een of meer gevarenbronnen.

Toelichting

Storingen en foutief menselijk handelen kunnen de veiligheid van een elektrische installatie nadelig beïnvloeden. Om de veiligheid van een elektrische installatie te bepalen moet een risicoanalyse uitgevoerd worden. Bij een risicoanalyse moeten alle mogelijke risico's onderzocht worden.

De grootte van een risico wordt bepaald door de kans dat er iets fout gaat in de elektrische installatie en de schadelijke effecten die ontstaan ten gevolge van het falen van de elektrische installatie.

3.1.5 Elektrisch gevaar

Onder elektrisch gevaar verstaan we het risico van letsel veroorzaakt door een elektrische installatie.

Toelichting

In vergelijking met andere gevarenbronnen zijn elektrische gevaren moeilijk waarneembaar. Een gaslek is te ruiken, rook en vuur zijn zichtbare verschijnselen van een brand en hoge temperaturen zijn voelbaar als warmte-uitstraling of zichtbaar als gloeiverschijnselen. Een elektrisch gevaar wordt vaak niet opgemerkt totdat het te laat is. Dit geldt zeker voor personen die weinig of geen kennis hebben van elektriciteit. Om ongelukken te voorkomen is het noodzakelijk dat de elektrische installatie of de elektrische arbeidsmiddelen veilig zijn.

Enkele voorbeelden van een bron van mogelijk letsel of gezondheidsrisico die aanwezig is in een elektrische installatie zijn verbranding, elektrocutie en verwondingen die ontstaan door de krachten die vrij komen bij kortsluitingen in installaties.

3.1.6 Letsel (elektrisch)

Onder letsel verstaan we een ongeval met persoonlijk letsel of dodelijke afloop veroorzaakt door een elektrische schok, elektrische verbranding, vlambogen of door brand of ontploffing die voortkomt uit elektrische energie als gevolg van werkzaamheden aan, met of nabij een elektrische installatie.

Toelichting

Uiteraard kunnen letsels ook ontstaan door allerlei andere oorzaken. Indien we echter in dit Veiligheidshandboek Rijkswaterstaat NEN 3140 spreken over letsels worden letsels bedoeld die direct of indirect veroorzaakt zijn door elektriciteit.

3.1.101 Elektrisch arbeidsmiddel

Op de werkplek gebruikt arbeidsmiddel, hulpmiddel of persoonlijk beschermingsmiddel dat een elektrisch gevaar kan opleveren of verminderen

OPMERKING Voorbeelden van elektrische arbeidsmiddelen zijn:

— elektrische gereedschappen;

— elektrische machines;

— handlampen en andere verplaatsbare lampen;

— stroomverbruikende toestellen, zoals: koelkasten, koffiezetters, laboratoriumapparatuur, pc's, printers en stofzuigers;
— verplaatsbare leidingen;
— verplaatsbare elektrische meetinstrumenten;
— persoonlijke beschermingsmiddelen;
— handgereedschappen voor het onder spanning werken;
— verplaatsbare schakel- en verdeelinrichtingen;
— medische elektrische toestellen.

3.1.102 **Actief deel**

Geleider of geleidend deel bestemd om bij normaal bedrijf onder spanning te staan, met inbegrip van de nulleiding, maar volgens afspraak niet een PEN-leiding, een PEM-leiding of een PEL-leiding [2.12.08 NEN 1010:2007+C1:2008]

3.2 Personeel, organisatie en communicatie

In de norm NEN 3140:2011 worden verschillende personen gedefinieerd met betrekking tot elektrische werkzaamheden aan, met of nabij elektrische installaties of elektrische arbeidsmiddelen. Elke persoon heeft zijn eigen werkzaamheden, bevoegdheden en verantwoordelijkheden.

3.2.1 **Functioneel Installatieverantwoordelijke (F-IB) en Technisch Installatieverantwoordelijke (T-IV)**

Nadere definitie van deze twee rollen is vermeld in hoofdstuk 2 van het document "Handleiding Bedrijfsvoering Elektrische Installaties", versie 1.1.

Bij Rijkswaterstaat zijn de F-IB en de T-IV normaal medewerkers van de eigen organisatie. Hierop zijn uitzonderingen mogelijk, de T-IV kan worden belegd bij de opdrachtnemer, die zorgt draagt voor een aanwijzing van een eigen deskundig persoon die werkzaamheden op zich kan nemen. Wel dient deze aanwijzing instemming te hebben van RWS, zie 3.2.6.

Bij bepaalde elektrotechnische installaties bij Rijkswaterstaat kunnen substantiële delen van de verantwoordelijkheid worden overgedragen aan een contractpartij. Bij het overdragen van de verantwoordelijkheid aan een contractpartij moet ervoor worden gewaakt dat steeds voor één taak één verantwoordelijke is aangewezen. Hierbij moet rekening worden gehouden met het feit dat taken zich ook kunnen onderscheiden door plaats en tijd.

De eindverantwoordelijkheid van de BEI van een object ligt bij de F-IB.

3.2.2 **Werkverantwoordelijke (WV)**

De werkverantwoordelijke is iemand die is aangewezen als direct verantwoordelijk persoon voor de leiding over werkzaamheden. Voor zover noodzakelijk mogen delen van deze verantwoordelijkheid worden overgedragen aan anderen.

Toelichting

Bij Rijkswaterstaat wordt de verantwoordelijkheid voor de werkzaamheden overgedragen aan een externe contractpartij.

Bij het overdragen van de verantwoordelijkheid aan een contractpartij moet ervoor worden gezorgd dat door de contractpartij steeds voor één taak één werkverantwoordelijke is aangewezen. Hierbij moet rekening worden gehouden met het feit dat taken zich ook kunnen onderscheiden door plaats en tijd.

Voor de bij Rijkswaterstaat in dienst zijnde voldoend onderrichte personen (VOP-ers) wordt de installatieverantwoordelijke van Rijkswaterstaat tevens als werkverantwoordelijke voor deze personen aangewezen.

Het personeel dat betrokken wordt bij de werkzaamheden aan, met of nabij elektrische installaties, moet goed zijn geïnstrueerd over de veiligheidseisen, de

veiligheidsregels en de bedrijfsvoorschriften, zoals die gelden voor de werkzaamheden. Het is de taak van de werkverantwoordelijke van de contractpartij om erop toe te zien dat aan alle eisen, regels en instructies is voldaan, voordat met de werkzaamheden begonnen wordt en dat gewerkt wordt volgens die voorschriften. Daarnaast moet de werkverantwoordelijke ervoor zorgen dat alle personen die bij werkzaamheden zijn betrokken, zijn geïnstrueerd over eventuele bijzondere gevaren die door deze personen niet zonder meer kunnen worden herkend.

3.2.3 Vakbekwaam persoon (VP)

Een vakbekwaam persoon is iemand met een relevante elektrotechnische opleiding waardoor hij of zij in staat is gevaren te voorkomen die door elektriciteit kunnen worden veroorzaakt.

Toelichting

Vakbekwame personen die bij Rijkswaterstaat elektrotechnische werkzaamheden uitvoeren zijn niet in dienst van Rijkswaterstaat maar in dienst van een externe contractpartij. Ze staan met betrekking tot de veiligheid tijdens de werkzaamheden onder verantwoordelijkheid van de werkverantwoordelijke van de betreffende contractpartij. Een uitzondering is gemaakt voor RWS-medewerkers die een taak op een RWS-schip uitvoeren als machinist/stuurman. Zij mogen direct nodige werkzaamheden aan de elektrische installatie zelf uitvoeren en zijn hiervoor ook opgeleid en geïnstrueerd

3.2.4 Voldoend onderricht persoon (VOP)

Een voldoend onderricht persoon is iemand die voldoende is geïnstrueerd door vakbekwame personen waardoor hij of zij in staat is gevaren te voorkomen die door elektriciteit kunnen worden veroorzaakt.

Toelichting

Bij Rijkswaterstaat zijn voldoend onderrichte personen in dienst die eenvoudige elektrotechnische werkzaamheden mogen verrichten. De installatieverantwoordelijke van de elektrische installaties, waaraan de werkzaamheden moeten worden verricht, wordt voor deze personen tevens aangewezen als werkverantwoordelijke. Dit houdt in dat de betreffende installatieverantwoordelijke tevens de taken van de werkverantwoordelijke op zich moet nemen, zoals het instrueren over de mogelijke gevaren die de werkzaamheden met zich meebrengen en de te nemen veiligheidsmaatregelen om deze gevaren te voorkomen.

3.2.5 Leek

Een leek is een persoon die niet in staat moet worden geacht gevaren te voorkomen die door elektriciteit kunnen worden veroorzaakt.

Toelichting

Zonder specifieke aanwijzing wordt binnen Rijkswaterstaat iedereen als leek beschouwd. Dit geldt ook voor medewerkers die wel elektrotechnisch zijn opgeleid maar niet zijn aangewezen voor werkzaamheden onder verantwoordelijkheid van Rijkswaterstaat.

Een leek mag een ruimte waar een elektrische gevarenbron aanwezig is, alleen betreden mits hij onder toezicht staat van minimaal één voldoend onderricht persoon na goedkeuring door de werkverantwoordelijke of de installatieverantwoordelijke.

3.2.6 Bericht of aanwijzing [vervallen in 3140:2011]

Aanvulling:

Te allen tijde mag Rijkswaterstaat er zich van vergewissen dat een dergelijke aanwijzing volgens de norm NEN 3140:2011, voor allen die op enige wijze betrokken zijn bij werkzaamheden, op juiste gronden heeft plaatsgevonden.

3.3 Werkzones

Om het risico van het aanraken van niet of slecht geïsoleerde delen van een elektrische installatie in te kunnen schatten is in NEN 3140:2011 elke werkplek ingedeeld in zones.

3.3.1 Werkplek

De werkplek is de plaats of plaatsen waar werkzaamheden worden, zijn of nog moeten worden uitgevoerd.

3.3.2 Gevarenzone

De gevarenzone is een bepaalde ruimte rondom actieve delen waarin het isolatieniveau ter voorkoming van elektrisch gevaar niet is gewaarborgd, wanneer deze ruimte zonder beschermingsvoorzieningen wordt binnengegaan.

Toelichting

In de definitie wordt gesproken over actieve delen waar het isolatieniveau niet is gewaarborgd. Hiermee worden onder spanning staande niet of slecht geïsoleerde delen van de elektrische installatie bedoeld.

Voor werkzaamheden aan installaties met spanningen tot 1.000 V is de gevarenzone gedefinieerd als het gebied waarin de afstand naar de ongeïsoleerde actieve delen kleiner is dan 200 mm. Afhankelijk van het risico in een bepaalde situatie kan het noodzakelijk zijn om een veel grotere afstand aan te houden.

3.3.3 Nabijheidszone [vervallen in 3140:2011]

3.3.101 Aanrakingsveilig

Een beschermingsgraad van ten minste IPXXB of IP2X.

Toelichting

Bij Rijkswaterstaat is dit objectafhankelijk en zal door de T-IV per object/onderdeel worden vastgelegd.

In de NEN 3140:2011 is in paragraaf 6.1 worden werkinstructies met betrekking tot de aanrakingsveiligheid nader uitgewerkt.

3.4 Arbeid

Alle definities in deze paragraaf hebben direct of indirect betrekking op de aanwezigheid van een elektrische gevarenbron.

3.4.1 Werkzaamheden

Onder werkzaamheden verstaan we elke vorm van elektrotechnische of niet-elektrotechnische werkzaamheden waarbij een elektrische gevarenbron aanwezig kan zijn.

3.4.2 Elektrotechnische werkzaamheden

Elektrotechnische werkzaamheden zijn werkzaamheden aan, met of nabij een elektrische installatie, zoals beproeven en meten, repareren, vervangen, aanpassen, uitbreiden, installeren en inspecteren.

3.4.3 Niet-elektrotechnische werkzaamheden

Niet elektrotechnische werkzaamheden zijn werkzaamheden nabij een elektrische installatie, zoals bouwen, graven, schoonmaken en schilderen.

Toelichting

Elektrotechnische werkzaamheden zoals het aanbrengen van kabeldraagsystemen, het leggen van (grond)kabels, het leggen van buizen en het plaatsen van lichtmasten kunnen onder bepaalde omstandigheden, indien bij de werkzaamheden geen elektrotechnische gevaren kunnen bestaan, beschouwd worden als niet-elektrotechnische werkzaamheden.

3.4.4 Onder spanning werken

Onder spanning werken zijn alle werkzaamheden waarbij een persoon actieve delen kan aanraken of met delen van zijn of haar lichaam of met gereedschappen, hulpmiddelen of (persoonlijke) beschermingsmiddelen, waarmee wordt gewerkt, terechtkomt in de gevarenzone.

Toelichting

Werkzaamheden aan actieve delen van installaties met zeer lage spanningen vallen eveneens onder de definitie van werken onder spanning. Deze installaties werken met een spanningsgebied waarbinnen de nominale waarde van de spanning niet hoger is dan 50 V bij wisselspanning of 120 V bij gelijkspanning.

In Nederland is in het arbeidsomstandighedenbesluit bepaald dat het werken onder spanning niet is toegestaan. Alleen in zeer uitzonderlijke omstandigheden en na extra procedures en maatregelen mag onder spanning gewerkt worden, maar altijd geldt dat het onder spanning werken zoveel mogelijk moet worden voorkomen.

3.4.5 Werken in de nabijheid van actieve delen [vervallen in 3140:2011]

In de NEN 3140:2011 is in paragraaf 6.1 worden werkinstructies met betrekking tot werken in de nabijheid van actieve delen nader uitgewerkt.

3.4.6 Scheiden

Volledig vrijmaken van een toestel of stroomkring van andere toestellen of stroomkringen.

3.4.7 Spanningsloos

Spanningsloos is een spanningswaarde van (vrijwel) 0 V, dat wil zeggen zonder aanwezige spanning en/of lading.

3.4.8 Spanningsloos werken

Spanningsloos werken is het werken aan een elektrische installatie die zonder spanning of lading is en waarbij de werkzaamheden worden uitgevoerd nadat alle maatregelen ter voorkoming van elektrisch gevaar zijn genomen.

Toelichting

Bij spanningsloos werken moet de werkplek tijdens de duur van de werkzaamheden spanningsloos en daardoor veilig zijn. Hiervoor moet aan essentiële voorwaarden worden voldaan. Deze staan vermeld in de norm onder par. 6.2 "spanningsloos werken". Uitgangspunt is "niet onderspanning werken" en als het niet anders kan dan altijd met schriftelijke toestemming van WV.

3.5 Beschermingsvoorzieningen

Om onder spanning staande delen van een elektrische installatie te beveiligen tegen toevallige aanraking zijn verschillende beschermingsvoorzieningen toepasbaar. De meest toepasbare worden hier besproken.

3.5.1 Scherm

Een scherm is een voorziening, al of niet geïsoleerd, die wordt gebruikt om nadering van materieel of een deel van een elektrische installatie dat gevaar kan opleveren, te voorkomen.

3.5.2 Afscherming

Een afscherming is een voorziening die bescherming biedt tegen directe aanraking vanuit elke gebruikelijke richting van benadering.

3.5.3 Isolerend omhulsel

Een isolerend omhulsel is een starre of flexibele voorziening van isolerend materiaal die wordt gebruikt om toevallige aanraking te voorkomen van actieve en/of spanningsloze delen en/of naastgelegen delen.

3.5.4 Omhulsel [vervallen in 3140:2011]

Aanvulling BEI Rijkswaterstaat:
Volgens de Machinerichtlijn (versie 2011) en NEN-EN 60204 moeten omhulsels personen of dieren beschermen tegen toegang tot gevaarlijke delen. In NEN 3140:2011 wordt geen aandacht besteed aan de gevaren voor dieren.

Voorbeelden van omhulsels zijn een kast of doos, een compartiment en een omhulde ruimte.

3.6 Spanningen

In dit Veiligheidshandboek NEN 3140 Rijkswaterstaat wordt onderscheid gemaakt tussen drie spanningsniveaus, namelijk:

- extra lage spanning (ELV)
- lage spanning (LV)
- hoge spanning (HV)

De NEN 3140:2011 geeft de aanvullende Nederlandse bepalingen voor laagspanningsinstallaties. Dit betreft alle elektrische installaties met extra lage spanning (ELV) of lage spanning (LV).

Het NEN 3140 Veiligheidshandboek Rijkswaterstaat is niet van toepassing voor elektrische installaties met hoge spanning (HV). Voor dergelijke installaties geldt de NEN 3840 (Bedrijfsvoering van elektrische installaties – Aanvullende Nederlandse bepalingen voor hoogspanningsinstallaties).

Voorbeelden van installaties met hoge spanning zijn:

- zware elektrisch aangedreven pompen (gemalen Panheel, Zedemuden, IJmuiden), deze worden gevoed via hoogspanningstransformatoren
- Verdelingen Stormvloedkeringen, grote sluiscomplexen (IJmuiden, Terneuzen)
- Aansluitingen verdeling voeding tunnels (ook step-up transformatoren)

Rijkswaterstaat streeft ernaar de hoogspanningsinstallaties onder te brengen bij energieleveranciers/netbeheerders, doch in het kader van beschikbaarheid en veiligheid zullen er nog steeds hoogspanningsinstallaties in eigendom van Rijkswaterstaat zijn.

3.6.1 Extra lage spanning (ELV)

Een extra lage spanning is een spanning die normaal niet hoger is dan 50 V bij wisselspanning of 120 V rimpelvrij bij gelijkspanning tussen geleiders of naar aarde.

Toelichting

Onder extra lage spanning vallen diverse ketens, zoals PELV (Protective Extra Low Voltage), SELV (Safety Extra Low Voltage) en FELV (Functional Extra Low Voltage). Deze worden hier niet verder behandeld.

In het Veiligheidshandboek Rijkswaterstaat NEN 3140 zullen we verder geen onderscheid maken tussen de verschillende soorten ketens met extra lage spanning, maar uitsluitend spreken over ELV-ketens.

Voorbeelden van apparaten met extra lage spanning zijn:

- laptops
- inkjetprinters en scanners
- mobiele telefoons
- zaklantaarns

3.6.2 Lage spanning (LV)

Een lage spanning is een spanning die normaal niet hoger is dan 1.000 V bij wisselspanning of 1.500 V bij gelijkspanning.

Voorbeelden van apparaten met lage spanning zijn:

- desktop computers
- kantoorverlichting
- boormachines

3.6.101 **S-keten**

Elektrisch gescheiden stroomketen waarvan actieve delen op geen enkel punt met andere stroomketens, met aarde of met een beschermingsleiding zijn verbonden en met een maximale spanning van 500 V.

Rijkswaterstaat heeft in principe geen S-ketens in haar areaal.

3.101 Toezicht

OPMERKING: voor aanvullende informatie zie NEN3140:2011, bijlage C.

3.101.1 **Ononderbroken toezicht**

Toezicht met als doel dat werkzaamheden veilig worden uitgevoerd en dat gedurende de werkzaamheden altijd aanwezig is.

De T-IV en de WV bepalen in onderling overleg of er ononderbroken toezicht benodigd is.

3.101.2 **Regelmatig toezicht**

Toezicht met als doel dat werkzaamheden veilig worden uitgevoerd en dat gedurende de werkzaamheden regelmatig wordt uitgevoerd.

De T-IV en de WV bepalen in onderling overleg of er regelmatig toezicht benodigd is.

4 Onderwerp en toepassingsgebied

Dit veiligheidshandboek is gebaseerd op de norm NEN 3140:2011 en is van toepassing op de bedrijfsvoering van en de werkzaamheden aan, met of nabij elektrische installaties en elektrische arbeidsmiddelen.

Omdat op alle objecten van Rijkswaterstaat elektrische installaties en elektrische arbeidsmiddelen ruimschoots aanwezig zijn is dit veiligheidshandboek van belang voor alle medewerkers. Het maakt daarbij niet uit of de medewerkers in dienst zijn van de eigen organisatie, zijn ingeleend of een arbeidsrelatie hebben met een contractpartij.

De elektrische installaties zijn ontworpen voor de opwekking, het transport, de omzetting, de distributie en het gebruik van elektrische energie. De meeste van deze elektrische installaties zijn permanent en vast aangebracht, zoals een installatie voor de distributie van elektrische energie in een tunnel of een sluis. Andere installaties zijn tijdelijk, zoals op bouwplaatsen en kunnen worden verplaatst wanneer zij onder spanning staan of in bedrijf zijn.

De norm NEN 3140:2011 geeft de eisen weer voor de veilige bedrijfsvoering van en de werkzaamheden aan, met of nabij elektrische laagspanningsinstallaties. Onder bedrijfsvoering wordt verstaan alle handelingen en werkzaamheden die noodzakelijk zijn om de elektrische installatie te kunnen laten werken zoals schakelen, regelen, bewaken en onderhoudswerkzaamheden.

De norm gelden voor alle elektrotechnische en niet-elektrotechnische werkzaamheden, zoals bouwwerkzaamheden en graafwerkzaamheden als in de omgeving elektrische leidingen aanwezig zijn die onder spanning staan.

De norm is ook van toepassing op het gebruik, het onderhoud, de inspectie en het beheer van elektrische arbeidsmiddelen.

Onder een elektrisch arbeidsmiddel wordt verstaan elke op de arbeidsplaats gebruikte machine, gereedschap, apparaat, hulpmiddel en persoonlijk beschermingsmiddel dat door de aard van hun gebruik of de omgevingsomstandigheden een elektrisch veiligheidsrisico kan opleveren.

De norm NEN 3140:2011 heeft betrekking op elektrische installaties en elektrische arbeidsmiddelen, met een spanningsniveau van extra lage spanning tot en met lage spanning.

Dit veiligheidshandboek is **niet van toepassing** op het gebruik van installaties, toebehoren en (hulp)middelen (bijvoorbeeld: afstandsbedieningen (niet zijnde "Bediening op Afstand"), klein elektrisch gereedschap zoals accuboormachines) door leken, mits de installaties, toebehoren en hulpmiddelen zijn ontworpen en geïnstalleerd voor gebruik door leken en voldoen aan de vereiste normen.

Deze bepaling legt een taak bij de installatieverantwoordelijke. Hij / zij moet bij voortduring controleren of de elektrotechnische voorzieningen aan de vereiste normen blijven voldoen en of die voorzieningen op de juiste wijze en in de juiste omgeving worden gebruikt.

De NEN 3140:2011 is **niet specifiek ontwikkeld** voor onderstaande elektrische installaties:

- elektronische telecommunicatie- en informatiesystemen zoals brugbediening op afstand, marifoon
- elektronische instrumentatie-, besturings- en automatiseringssystemen

Aanbevolen wordt echter dat personen die verantwoordelijk zijn voor deze installaties, de norm NEN 3140:2011 hanteren als leidraad bij het opstellen van hun eigen normen en regels.

LET OP

De hiervoor staande uitsluiting geldt alleen voor de specifiek genoemde installaties.

Elektrische installaties in gebouwen en op machines worden vervaardigd volgens verschillende normen die vaak ook nog in meerdere versies bestaan.

Enkele voorbeelden zijn:

- NEN 1010 voor elektrische laagspanningsinstallaties op wegen, terreinen en in gebouwen (spanningsverlies /afschakeling).
  De meeste installaties bij Rijkswaterstaat moeten voldoen aan deze norm.
- NEN-EN 60204 voor installaties van machines zoals liften, stapelaars, elektrische poorten, noodstroomgeneratoren, brandpompen, pompkamers en bedieningen van sluisdeuren.

Normen veranderen doordat producten veranderen. Hierdoor ontstaan steeds weer nieuwe normen zodat de producten kunnen innoveren.

Welke norm relevant is hangt onder andere af van de normen die gebruikt zijn bij het vervaardigen van de installatie of het product.

Naast de verschillende normen zijn ook tal van Europese regels en richtlijnen van toepassing op de verschillende elektrische installaties en elektrische arbeidsmiddelen, zoals de laagspanningsrichtlijn, de machinerichtlijn en de EMC-richtlijn.

5 Functies volgens NEN3140

5.1 De installatieverantwoordelijke

De installatieverantwoordelijke is een persoon die is aangewezen, door of namens de hoogste verantwoordelijke voor de naleving van de ARBO-wet, als direct verantwoordelijke voor de veilige bedrijfsvoering van de elektrische installatie en de veiligheid van de elektrische arbeidsmiddelen *(Bron: NEN 3140, par. 3.2.2, par 4.2.101 en NEN 3840, par. 3.2.2).*

Verantwoordelijkheden

De installatieverantwoordelijke is verantwoordelijk voor:

1. De elektrische installaties en elektrische arbeidsmiddelen *(Bron: NEN 3140, Bijlage F.2);*
   NB: De IV kan eigen personeel zijn of tot een andere organisatie behoren *(Bron: NEN 3140, par 4.2.102 en NEN 3840, par. 4.2.102)*. Bij uitbesteding of aanneming kan een rechtspersoon worden aangewezen, anders moet het een natuurlijke persoon zijn *(Bron: NEN 3140, par. 4.3)*;
2. Het in stand houden van de veiligheid van elektrische installaties en elektrische arbeidsmiddelen, door regelmatige inspecties en tijdig herstel van gevonden gebreken *(Bron: NEN 3140, Bijlage F.2);*
   NB: De IV bepaalt uit te voeren inspecties met frequentie, uit te voeren representatieve steekproeven, te gebruiken meetmethoden en instrumenten voor arbeidsmiddelen en (delen van) elektrische installaties, rekening houdend met voorschriften fabrikant *(Bron: NEN 3140, par 5.101.5, 5.102.6 en NEN 3840, par. 5.3.3.1.202);*
   NB: Aanvullende maatregelen kunnen op grond van gewijzigd gebruik of gewijzigde omstandigheden noodzakelijk zijn *(Bron: NEN 3140, par 4.3.107)*;
3. Het opzetten van een toegangsregeling voor ruimten met elektrisch gevaar *(Bron: NEN 3140, par 4.3 en, Bijlage F.2)*;
4. Het vaststellen van procedures voor bediening en onderhoud van de installatie *(Bron: NEN 3140, Bijlage F.2)*;
   NB: met bediening wordt bedoeld het in- en uitschakelen van een installatie of het aansluiten en losmaken van materieel. Niet te verwarren met het bedienproces van bijv. bruggen, tunnels of sluizen;
5. Het goedkeuren van plannen voor de uitvoering van werkzaamheden, maar niet hoe om te gaan met de werkrisico's *(Bron: NEN 3140, par 4.3, en Bijlage F.2)*;
6. Het toestemming geven voor de aanvang van werkzaamheden *(Bron: NEN 3140, Bijlage F.2)*;
7. Het goedkeuren van bedieningshandelingen en functionele handelingen *(Bron: 3140, par 5.1);*
8. Afspraken met andere installatieverantwoordelijke wanneer installaties of elektrische arbeidsmiddelen zich in elkaars nabijheid bevinden *(Bron: NEN 3140, par. 4.3 en NEN 3840, par. 4.3)*;
9. Instemmen met het inschakelen na werkzaamheden *(Bron: NEN 3140, par 6.2.7);*
10. Het goedkeuren van de onderhoudswerkzaamheden *(Bron: NEN 3140, par 7.2.1);*
11. Bij spanningsloos werken:
    a. Het spanningsloos maken van een deel van een installatie *(Bron: NEN 3140, Bijlage F.4.1).*
       NB: Dat wil niet zeggen dat de IV dit zelf uitvoert *(Bron: NEN 3140, Bijlage F.4.1 en NEN 3840 par. 6.2.2.201).*

b. Het in gebruik nemen van een installatie, na werkzaamheden *(Bron: NEN 3140, Bijlage F.4.4).*
NB: Dat wil niet zeggen dat de IV dit zelf uitvoert *(Bron: NEN 3140, Bijlage F.4.4 en NEN 3840 par. 6.2.2.201).*

NB: Delen van de taken van de installatieverantwoordelijke kunnen worden gedelegeerd *(bron: NEN 3140, par. 4.2.103 en NEN 3840 par. 3.2.2).*

Binnen RWS heeft ervoor gekozen de taken van de installatieverantwoordelijke te belegd bij (in het algemeen) 2 functionarissen: de functioneel beheerder (F-IB) en de technische installatieverantwoordelijke (T-IV). Dit geldt voor zowel de laagspanning als de hoogspanning. Er is echter een uitzondering mogelijk dat de T-IV wordt belegd bij een opdrachtnemer. Dit wordt geregeld in het contract met deze opdrachtnemer.

De punten 1, 3, 5, 6 en 8 zijn zaken die een sterke relatie hebben met beleid en worden daarom belegd bij de F-IB.

De overige punten, inclusief de punten 5 en 8, zijn technisch georiënteerd en kunnen bij de T-IV belegd worden. Punten 5 en 8 worden door de F-IB en T-IV beoordeeld.

De eindverantwoordelijkheid van de BEI van een object ligt bij de F-IB.

Afhankelijk van een contract, kunnen taken van de T-IV bij een marktpartij worden neergelegd. Dit is verwoord in de projecteigen vraagspecificatie.

5.2 Werkverantwoordelijke

Definitie

De werkverantwoordelijke is een persoon die is aangewezen, door of namens de hoogste verantwoordelijke voor de naleving van de ARBOwet, als direct verantwoordelijke voor de veiligheid van de werkzaamheden *(Bron: NEN 3140, par. 3.2.1 en NEN 3840, par. 3.2.1).*

Verantwoordelijkheden

De werkverantwoordelijke is verantwoordelijk voor:

- Elektrische veiligheid bij alle werkzaamheden *(Bron: NEN 3140, par. 3.2.1 en NEN 3840, par. 3.2.1)*;
  NB: De WV kan eigen personeel zijn of tot een andere organisatie behoren;
  NB: De WV toetst of aan alle regels en instructies is voldaan;
- Het vaststellen van de risico's verbonden aan werkzaamheden *(Bron: NEN 3140, Bijlage F.3)*;
- Het opstellen van plannen voor werkzaamheden *(Bron: NEN 3140, Bijlage F.3)*;
- Het kiezen van de juiste uitvoerenden voor werkzaamheden *(Bron: NEN 3140, Bijlage F.3)*;
- Het bepalen van de juiste werkwijze, hulpmiddelen en beschermingsmiddelen *(Bron: NEN 3140, Bijlage F.3 en NEN 3840 par. 4.2)*;
- Het instrueren van de uitvoerenden bij werkzaamheden *(Bron: NEN 3140, Bijlage F.3 en NEN 3840 par. 4.2)*;
- Het verzorgen van toezicht bij werkzaamheden *(Bron: NEN 3140, Bijlage C.3 & F.3 en NEN 3840, Bijlage C.3)*;
- Informeren van de installatieverantwoordelijke over aard, plaats, veiligheidsmaatregelen en gevolgen werkzaamheden *(Bron: NEN 3140, par. 6.1 en NEN 3840 par. 6.1);*
- Bij spanningsloos werken:
  - veiligheid op de werkplek *(Bron: NEN 3140, Bijlage F.4.2 en NEN 3840, par. 6.2.2 – 6.2.6);*
  - inspectie van installatie voor ingebruikname, ook als deel van de installatie hiervoor van spanning moet zijn voorzien *(Bron: NEN 3140, Bijlage F.4.3 en NEN 3840, par. 6.2.7);*

NB: Dat wil niet zeggen dat de WV dit zelf uitvoert *(Bron: NEN 3140, Bijlage F.4.3);*

- Bij onder spanning werken:
  - schriftelijk opdracht geven voor werken onder spanning en zorgen voor veilige uitvoering *(Bron: NEN 3140, Bijlage F.5).*

NB: Delen van de taken van de werkverantwoordelijke kunnen worden gedelegeerd *(Bron: NEN 3140, par. 4.2.103 en NEN 3840 par. 3.2.1).*

Opleiding

De Werkverantwoordelijken heeft ten minste een middelbaar elektrotechnisch niveau verkregen door opleiding en/of ervaring. De WV is verantwoordelijk voor de uitvoering van het eigen takenpakket en moeten zich daarvoor kunnen verantwoorden. Tot de verantwoordelijkheid kunnen planning, administratie, beheer en/of ontwikkeling horen. De werkzaamheden worden meestal zelfstandig en zonder toezicht verricht *(Bron: NEN 3140, par. 4.2.103 en NEN 3840 par. 4.2.204).*

NB: Hieraan kan worden voldaan met een WEB-niveau 4 *(Bron: NEN 3140, par. 4.2.103.*

Overzichtelijke installaties

Een vakbekwaam persoon mag worden aangewezen als werkverantwoordelijke voor:

- overzichtelijke installaties of delen van overzichtelijke installaties;
- overzichtelijke werkzaamheden.

NB: Voorbeelden van overzichtelijke installaties zijn installaties waarbij:

- geen terugvoeding mogelijk is;
- geen parallelschakeling aanwezig is;
- geen noodstroomsysteem aanwezig is *(Bron: NEN 3140, par. 4.2.107).*

5.3 Vakbekwaam Persoon

Definitie

Een Vakbekwaam Persoon is een persoon die is aangewezen en met een relevante opleiding en ervaring waardoor hij in staat is gevaren die door elektriciteit kunnen worden veroorzaakt te onderkennen en te voorkomen *(Bron: NEN 3140, par. 3.2.3 en NEN 3840, par. 3.2.3).*

Opleiding

Vakbekwame personen hebben ten minste een lager elektrotechnisch niveau verkregen door opleiding en/of ervaring. Ze zijn verantwoordelijk voor de uitvoering van het eigen takenpakket en moeten zich daarvoor kunnen verantwoorden. Ze werken meestal zelfstandig onder indirect toezicht en soms onder direct toezicht *(Bron: NEN 3140, par. 4.2.104 en NEN 3840 par. 4.2.205).*

NB: Hieraan kan worden voldaan met een WEB-niveau 2 *(Bron: NEN 3140, par. 4.2.104).*

5.4 Voldoende Onderricht Persoon

(zie ook hoofdstuk 6)

Definitie

Een Voldoende Onderricht Persoon is een persoon die is aangewezen en die voldoende is geïnstrueerd voor specifieke taken, werkzaamheden en het gebruik van elektrische arbeidsmiddelen waardoor hij in staat is gevaren die door elektriciteit kunnen worden veroorzaakt te onderkennen en te voorkomen *(Bron: NEN 3140, par. 3.2.4 en NEN 3840, par. 3.2.4).*

Werkzaamheden

Voorbeelden van werkzaamheden die voldoende onderrichte personen, na instructie, kunnen uitvoeren zijn:

- vervangen van lampen;
- aan- en afkoppelen van elektromotoren;
- resetten van beveiligingen;
- monteren van contactstoppen aan leidingen;
- vervangen van wandcontactdozen en lichtschakelaars;
- monteren van verlichtingsarmaturen;

- inspecteren van elektrische arbeidsmiddelen;
- aanbrengen en verwijderen van bepaalde smeltpatronen;
- het gebruiken van elektrische arbeidsmiddelen in specifieke situaties *(Bron: NEN 3140, par. 4.2.105).*

Opleiding/ervaring

Voldoende onderrichte personen zijn, door instructie, in staat om bij hun werkzaamheden elektrische gevaren te vermijden. Ze kunnen, na instructie, bedrijfsspecifieke werkzaamheden uitvoeren waarvan de elektrische risico's beperkt zijn *(Bron: NEN 3140, par. 4.2.105 en NEN 3840 par. 4.2.206).*

5.5 Ploegleider [alleen bij hoogspanninginstallaties]

Een ploegleider is een vakbekwaam persoon die ter plaatse met de leiding van werkzaamheden is belast *(Bron: NEN 3840 par. 3.2.202).*

Een ploegleider heeft de leiding over de uitvoering van werkzaamheden wanneer de Werkverantwoordelijke deze bij afwezigheid heeft gedelegeerd aan de ploegleider *(Bron: NEN 3840 par. 6.2.0.201)*.

5.6 Bedieningsdeskundige [alleen bij hoogspanninginstallaties]

Een bedieningsdeskundige is een persoon die is aangewezen als direct verantwoordelijk persoon voor bedieningshandelingen, waarbij deze handelingen worden gecoördineerd vanuit één punt *(Bron: NEN 3840 par. 3.2.203).*

Bedieningshandelingen in complexe installaties, waarbij de bediening wordt gecoördineerd vanuit één punt, mogen worden uitgevoerd door een bedieningsdeskundige. Hierbij gaat het om het (op afstand) uitvoeren van bedieningshandelingen of het opdracht geven tot bedieningshandelingen om de continuïteit van het proces en de veiligheid van het personeel te waarborgen.

Deze bedieningshandelingen moeten worden uitgevoerd volgens bedrijfsinstructies, die zijn goedgekeurd door de installatieverantwoordelijke.

Bedieningsdeskundigen mogen binnen het raamwerk van deze instructie ook opdrachten geven voor bedieningshandelingen die niet op afstand kunnen worden uitgevoerd *(Bron: NEN 3840 par. 5.2.1.203).*

5.7 Leek

Een leek is een persoon die geen installatieverantwoordelijke, werkverantwoordelijke, vakbekwaam persoon, voldoende onderricht persoon, ploegleider (alleen NEN 3840) en bedieningsdeskundige (alleen NEN 3840) is van de desbetreffende installatie *(Bron: NEN 3140, par. 3.2.5 en NEN 3840, par. 3.2.5).*

Een leek mag slechts:

- een ruimte met elektrisch gevaar betreden, onder toezicht van ten minste VOP *(Bron: NEN 3140, par. 4.3.101 en NEN 3840, par. 4.3.202)*;
- metingen uitvoeren aan een elektrische installatie, onder toezicht van ten minste VP (Bron: NEN 3140, par. 5.3.1.1 en NEN 3840, par. 5.3.1.1);
- beproevingen uitvoeren aan een elektrische installatie, onder toezicht van ten minste VP (Bron: NEN 3140, par. 5.3.2.1 en NEN 3840, par. 5.3.2.1);
- vervangen smeltpatronen (DI en DII), lampen en uitneembare toebehoren, mits aanrakingsveilig *(Bron: NEN 3140, par. 7.4.101 & 7.4.2)*.

6 Voorschriften van de voldoende onderrichte personen in dienst van Rijkswaterstaat

Binnen de organisatie van Rijkswaterstaat worden ook, in zeer geringe mate, elektrotechnische werkzaamheden uitgevoerd door eigen medewerkers. Het betreffen dan altijd eenvoudige elektrotechnische werkzaamheden zoals het vervangen van zekeringen en lampen, het betreden van elektrotechnische bedrijfsruimten of het openen en sluiten van elektrotechnische schakelkasten.

Deze werkzaamheden worden uitgevoerd door bijvoorbeeld (weg)inspecteurs.

De installatieverantwoordelijke is voor deze personen, die alleen eenvoudige elektrotechnische werkzaamheden mogen uitvoeren, tevens de werkverantwoordelijke.

Medewerkers die deze eenvoudige elektrotechnische werkzaamheden uitvoeren moeten schriftelijk zijn aangewezen als voldoende onderrichte persoon. Ze moeten zijn opgeleid en geïnstrueerd volgens de aanwijzingen van de betreffende installatie-/werkverantwoordelijke.

Voldoende onderrichte personen mogen alleen werkzaamheden uitvoeren waarvoor zij instructie hebben ontvangen. Dit moet schriftelijk zijn vastgelegd. Voorbeelden van werkzaamheden die door voldoend onderrichte personen, na instructie, kunnen worden uitgevoerd zijn:

- Het uitschakelen van openbare verlichting onder bepaalde voorwaarden.
- Het uitschakelen van VRI's onder bepaalde voorwaarden.

Nimmer mogen werkzaamheden met een elektrotechnisch gevaar worden uitgevoerd als de medewerkers niet zijn aangewezen door de installatie-/werkverantwoordelijke.

Dit geldt voor zowel inspecteurs binnen de droge als de natte infrastructuur.

Van het eigen personeel en van personeel van derden moet worden geëist dat het zich houdt aan de eisen, regels en instructies, zoals deze door Rijkswaterstaat zijn opgesteld. Er kunnen disciplinaire maatregelen worden genomen tegen eigen personeel dat zich niet aan de eisen, regels en instructies houdt. Voor personeel van contractpartijen kan een regeling worden vastgesteld in de aanneemovereenkomst.

Het is noodzakelijk dat schriftelijk wordt vastgelegd op welke wijze is beoordeeld dat bij de voldoend onderrichte persoon voldoende kennis en ervaring aanwezig is om de werkzaamheden uit te voeren. Ten minste moet beoordeeld worden of de personen die de werkzaamheden uitvoeren, voldoende:

- Kennis van elektriciteit bezitten.
- Ervaring met de betreffende elektrotechnische werkzaamheden hebben.
- Inzicht hebben in mogelijke gevaren tijdens de werkzaamheden en de in acht te nemen voorzorgsmaatregelen.
- Vaardigheid bezitten om te allen tijde te onderkennen of het veilig is om de werkzaamheden voort te zetten.

Dit is van toepassing op al het personeel dat op enige wijze betrokken is bij alle soorten werkzaamheden aan elektrische installaties.

Ook worden deze eisen gesteld aan de personen die op enige wijze werken met elektrotechnische installaties of werken in de omgeving van elektrotechnische installaties. Dit geldt voor elektrotechnische werkzaamheden, voor bedieningswerkzaamheden maar ook voor niet-elektrotechnische werkzaamheden waarbij elektriciteit wordt gebruikt.
Het aanwijzingsdocument voor de voldoend onderrichte persoon in dienst van Rijkswaterstaat moet ten minste de volgende punten bevatten:

- De naam en de geboortedatum of het personeelsnummer van de persoon.

- De functie van de persoon binnen het bedrijf en de afdeling.
- De ingangsdatum en eventueel de einddatum van de aanwijzing.
- De werkzaamheden die de persoon mag uitvoeren.
- De omstandigheden waaronder de persoon de werkzaamheden mag uitvoeren.
- De ruimte(n) waarin de persoon de werkzaamheden mag uitvoeren.
- De installatie(s) of delen van installatie(s) waaraan de persoon de werkzaamheden mag uitvoeren.
- De verantwoordelijkheden en bevoegdheden die de persoon krijgt.
- De gereedschappen, hulpmiddelen en (persoonlijke) beschermingsmiddelen waarover de persoon de beschikking krijgt.
- De plaats en datum van de aanwijzing.
- De naam en de functie van de persoon die aanwijst.
- De handtekening van de persoon die aanwijst en de handtekening van de persoon die wordt aangewezen.

Het verdient aanbeveling op het aanwijzingsformulier ruimte te reserveren voor de argumenten die geleid hebben tot de aanwijzing.

7 Overdracht taken aan contractpartijen: aanvullende eisen

Het overgrote deel van de elektrotechnische werkzaamheden die bij Rijkswaterstaat uitgevoerd moeten worden, wordt uitbesteed aan externe contractpartijen. Werkverantwoordelijken, vakbekwame personen en voldoend onderrichte personen die deze werkzaamheden uitvoeren zijn in dienst van deze contractpartijen.

Rijkswaterstaat heeft geen werkverantwoordelijken en geen vakbekwame personen in dienst.

Uitzonderingen hierop zijn de installatieverantwoordelijken die tevens als werkverantwoordelijken zijn aangewezen voor de bij Rijkswaterstaat in dienst zijnde voldoend onderrichte personen of personeel aan boord van RWS-schepen.

Ook voor de contractpartijen geldt dat conform de NEN 3140:2011 gewerkt moet worden.

Rijkswaterstaat vraagt inzage in de activiteiten die door een externe contractpartij worden verricht, door in het contract te vragen naar een door de opdrachtnemer op te stellen werkplan BEI.

Voor het opstellen van dit werkplan is een handreiking beschikbaar, die als bijlage 2 aan dit veiligheidshandboek toegevoegd.

7.1 Het aanwijzen van personeel van contractpartijen

Voor het uitvoeren van elektrotechnische werkzaamheden maakt Rijkswaterstaat uitsluitend gebruik van externe installateurs op basis van contracten. De aanwijzing van de werkverantwoordelijke, de vakbekwame personen en de voldoend onderrichte personen zoals die zijn beschreven in de NEN 3140:2011 is een taak van de contractpartij.

Besteedt Rijkswaterstaat werkzaamheden uit aan een contractpartij en is de overdracht van de verantwoordelijkheid niet schriftelijk vastgelegd, dan is de contractpartij toch verantwoordelijk voor het aanwijzen van zijn personeel voor het uitvoeren van de werkzaamheden.

De werkverantwoordelijken en de vakbekwame personen worden door de externe contractpartij aangewezen. Deze contractpartij is er verantwoordelijk voor dat de aangewezen personen aan de criteria voldoen.

Nadat alle criteria zijn getoetst, kan de persoon worden aangewezen. De aanwijzing moet schriftelijk geschieden.

Het is noodzakelijk de argumenten die bij een aanwijzing een rol hebben gespeeld, eveneens schriftelijk vast te leggen.
Het is de verantwoordelijkheid van de directie van de contractpartijen om ervoor te zorgen dat de aanwijzing van haar personeel geheel overeenkomstig dit veiligheidshandboek plaatsvindt.

Rijkswaterstaat vertrouwt erop dat de contractpartij uitsluitend personeel werkzaamheden laat verrichten dat de gevaren van het werken aan elektrische installaties en met elektrische energie kent en dat haar personeel op de juiste wijze is aangewezen en voldoende is geïnstrueerd.

Rijkswaterstaat heeft het recht op volledige inzage in het aanwijzingsbeleid van de contractpartij. Elke aanwijzing door de contractpartij kan door Rijkswaterstaat worden ingezien. Bovendien kan Rijkswaterstaat bezwaar tegen een aanwijzing maken.

Werkverantwoordelijken, vakbekwame personen en voldoend onderrichte personen die bij Rijkswaterstaat elektrotechnische werkzaamheden verrichten, worden door de contractpartij aangewezen voor die werkzaamheden. Personen kunnen ook

uitsluitend worden aangewezen voor werkzaamheden aan bepaalde installaties of installatiedelen.

De aanwijzing van deze personen kan voor verschillende installaties of installatieonderdelen verschillend zijn.

Een persoon kan voor een bepaalde installatie worden aangewezen als vakbekwaam persoon, terwijl hij voor een andere installatie slechts een voldoend onderrichte persoon is. Dit betekent dat de betreffende persoon gelijksoortige werkzaamheden aan de ene installatie wel en aan de andere installatie niet mag uitvoeren.

Indien elektrotechnische werkzaamheden met in- en/of uitleenkrachten plaatsvinden gelden de volgende voorwaarden:

Beide werkgevers moeten sluitende afspraken maken over de aanwijzing van de genoemde personen en hun onderlinge gezagsrelatie.

Werkverantwoordelijken, vakbekwame personen en voldoend onderrichte personen waarmee een gezagsverhouding bestaat en aan wie werkzaamheden zijn opgedragen, zoals bij inlenen en bij uitzendkrachten, door de contractpartij, moeten door de inlener schriftelijk zijn aangewezen.

Met deze twee voorwaarden wordt ingespeeld op de vergaande flexibilisering van de arbeidsovereenkomsten. De bedoeling hiervan is duidelijk. De kwaliteit van de arbeidsovereenkomst mag geen invloed hebben op het aanwijzingsbeleid. Daar waar werkzaamheden worden verricht, moet een eenduidig aanwijzingsbeleid worden gevoerd.

7.2 Het veilig uitvoeren van werkzaamheden

Externe contractpartijen die elektrotechnische werkzaamheden verrichten voor Rijkswaterstaat moeten niet alleen overeenkomstig de NEN 3140:2011 werken, maar moeten zich ook houden aan de huisregels en de veiligheidsvoorschriften die bij Rijkswaterstaat van toepassing zijn.

Ook van het personeel van derden ingezet door een contractpartij moet worden geëist dat het zich houdt aan de eisen, regels en instructies, zoals deze door Rijkswaterstaat zijn opgesteld. Er kunnen disciplinaire maatregelen worden genomen tegen personeel dat zich niet aan de eisen, regels en instructies houdt. Voor personeel van contractpartijen kan dit worden vastgelegd in de aanneemovereenkomst.

Bij de organisatie van het werk moet rekening worden gehouden met de samenstelling van de werkploeg. Op elke werkplek moet een voldoende aantal mensen aanwezig zijn dat nodig is om te werken aan, met of nabij een elektrische installatie.

De externe contractpartij moet controleren dat personeel dat zij naar een karwei stuurt, veilig kan werken in die omgeving waarin het karwei moet worden uitgevoerd. Deze bepaling is niet alleen van belang voor de elektrotechnische gevaren maar voor alle gevaren die bij werkzaamheden kunnen optreden.

In de NEN 3140:2011 staat dat iemand die om veiligheidsredenen bezwaar heeft om een opdracht op te volgen of werkzaamheden uit te voeren, de mogelijkheid moet worden geboden deze bezwaren meteen ter kennis te brengen van de werkverantwoordelijke.

De werkverantwoordelijke moet de situatie onderzoeken en, indien noodzakelijk, een hogere instantie raadplegen om tot een beslissing te komen. Ook in de Arbeidsomstandighedenwet vinden we een dergelijke bepaling.

Het is van belang dat de verantwoordelijkheid voor ieder die bij de werkzaamheden is betrokken vaststaat. Een collegiale gedachtewisseling of een aanvulling van een ter zake deskundig persoon blijft altijd mogelijk. De eindverantwoording blijft echter bij de werkverantwoordelijke liggen.

Voor ieder in de organisatie moet het duidelijk zijn door wie, welke werkzaamheden mogen worden verricht en hoe deze werkzaamheden moeten worden uitgevoerd.

7.3 Bevoegdheden en verantwoordelijkheden van extern personeel

Bij het uitvoeren van werkzaamheden op basis van een overeenkomst is eveneens de verantwoordelijkheid voor een veilige uitvoering van die werkzaamheden overgedragen.

Uitsluitend indien in een contract schriftelijk is vastgelegd dat de verantwoordelijkheid voor de veiligheid bij de werkzaamheden bij Rijkswaterstaat blijft, zal Rijkswaterstaat erop toezien dat de ingehuurde medewerkers capabel zijn.

Rijkswaterstaat is, zonder schriftelijke vastlegging van de verantwoordelijkheden, nimmer verantwoordelijk voor de elektrotechnische veiligheid bij werkzaamheden die worden uitgevoerd door personeel van derden.

De veiligheid van alle werkzaamheden behoort tot de verantwoordelijkheid van de werkverantwoordelijke. De werkverantwoordelijke kan een natuurlijke of een rechtspersoon zijn doch is nagenoeg altijd een persoon die verbonden is met een externe contractpartij.

Voor alle elektrotechnische werkzaamheden wordt de taak van de werkverantwoordelijke opgedragen aan de contractpartij die de werkzaamheden uitvoert.

Bij verdeling van de werkzaamheden kan het noodzakelijk zijn iemand aan te wijzen die verantwoordelijk is voor de veiligheid van elk gedeelte, waarbij het geheel valt onder de verantwoordelijkheid van één coördinerende werkverantwoordelijke.

Doordat Rijkswaterstaat elektrotechnische werkzaamheden uitbesteedt aan externe installateurs zal de werkverantwoordelijke een medewerker van de externe installateur zijn, of van een andere derde, terwijl de installatieverantwoordelijkheid nagenoeg altijd bij een medewerker van Rijkswaterstaat is belegd.

In een dergelijke situatie moeten de verantwoordelijkheden goed vastgelegd worden. Ook moet aandacht besteed worden aan de beheer- en werkprocedures. Tegenstrijdigheden in handelingswijzen tussen beide personen moeten voorkomen worden, een goede samenwerking is noodzakelijk.

Indien een werkverantwoordelijke het noodzakelijk vindt om een elektrische installatie of een gedeelte van de elektrische installatie uit te schakelen om de werkzaamheden veilig uit te voeren, moet hij hiervoor de bevoegdheid hebben.

Deze beslissing mag nimmer door een medewerker van Rijkswaterstaat teniet gedaan worden.

Uiteraard moet overleg plaatsvinden tussen de externe werkverantwoordelijke en de installatieverantwoordelijke van Rijkswaterstaat die de betreffende installatie onder zijn / haar beheer heeft.

Deze verantwoordelijken moeten afstemmen welke werkzaamheden, wanneer moeten worden uitgevoerd en welke veiligheidsmaatregelen noodzakelijk zijn.

Zo kunnen werkzaamheden op een gunstig tijdstip gepland worden, echter steeds gaat de veiligheid boven de continuïteit.

Het is zaak de werkafspraken goed te bespreken en in een register van de contractpartij vast te leggen.

8 Algemene werkvoorschriften en werkprocedures

Om de veiligheid van iedereen die aan of nabij elektrische installaties of aan en met elektrische arbeidsmiddelen werkt te waarborgen, moeten een aantal algemene eisen aan het beheer en de werkzaamheden gesteld worden.

In dit hoofdstuk worden deze eisen besproken. Aan bod komen:

- de algemene veiligheidsmaatregelen
- de werkprocedures
- de werkzaamheden bij risicoverhogende omstandigheden
- het sleutelplan
- de vastlegging of rapportage

8.1 Algemene Veiligheidsmaatregelen

Voor bepaalde handelingen die regelmatig voorkomen is het niet noodzakelijk om elke keer dat ze uitgevoerd worden een risico-inventarisatie en –evaluatie uit te voeren. De NEN 3140:2011 stelt dat voor dergelijke processen standaard bedrijfsvoeringprocedures ontwikkeld mogen worden.

Bedrijfsvoeringprocedures kunnen bijvoorbeeld worden opgesteld bij standaard bedieningshandelingen en bij functionele controles.

Bedieningshandelingen zijn bedoeld om de elektrische toestand van een elektrische installatie te wijzigen. Er bestaan twee soorten bedieningshandelingen:

Bedieningshandelingen bedoeld om de elektrische toestand van een elektrische installatie te wijzigen, om (elektrisch) materieel te gebruiken, om materieel, dat is ontworpen om zonder risico te worden gebruikt, aan te sluiten of los te nemen, aan of uit te zetten, voor zover dit in de praktijk redelijkerwijs mogelijk is.

Uitschakeling of wederinschakeling van installaties in samenhang met de uitvoering van werkzaamheden.

Bedieningshandelingen kunnen ter plaatse of op afstand worden uitgevoerd.

In de bedrijfsvoeringprocedures kan bijvoorbeeld staan dat geschikte gereedschappen moeten worden gebruikt om elektrisch gevaar voor personen te voorkomen.
Het gebruik van de juiste gereedschappen lijkt vanzelfsprekend. In de praktijk wordt regelmatig geïmproviseerd met verkeerd gereedschap. Door dit verkeerde gereedschap kan direct gevaar ontstaan.

Geïmproviseerd elektrisch handgereedschap mag bij Rijkswaterstaat niet toegepast worden, tenzij dit gereedschap goedgekeurd is door de installatieverantwoordelijke of de werkverantwoordelijke. Dit geldt ook voor de externe contractpartijen die voor Rijkswaterstaat werkzaamheden uitvoeren.

De elektrische veiligheidsmaatregelen, zoals getroffen voor de oorspronkelijke installatie, moeten ten minste in stand worden gehouden.

De elektrische veiligheidsmaatregelen zoals die getroffen zijn voor de oorspronkelijke installatie, vinden we in de normen, voorschriften, richtlijnen en aansluitvoorwaarden waaraan het ontwerp van de installatie ten grondslag lag.

Dit betekent dat een elektrische installatie volgens het bouwbesluit moet voldoen aan de druk van de NEN 1010, die van toepassing was op het tijdstip van de bouw van de installatie.

Uiteraard kan de installatieverantwoordelijke altijd beslissen dat een hoger veiligheidsniveau nodig is dan strikt noodzakelijk.

Voor installaties of delen van installaties die niet mogen worden gebruikt, omdat ze niet veilig zijn, moet worden voorkomen dat ze onbedoeld in bedrijf kunnen worden genomen.

Aanbevolen wordt ten minste zodanige maatregelen te nemen dat minimaal twee bewuste handelingen moeten worden uitgevoerd alvorens de installatie ingeschakeld kan worden. Daarnaast is altijd een waarschuwingsbord noodzakelijk.

In een ruimte die hoofdzakelijk is bestemd voor het bedrijf van de elektrische installatie mogen alleen voorwerpen aanwezig zijn die dienen voor bedieningswerkzaamheden en elektrotechnische werkzaamheden aan de daar aanwezige elektrische installatie.

8.2 Werkprocedures

Voor alle werkzaamheden moet een plan worden opgesteld. Volgens de uitgangspunten van de NEN 3140:2011 moet de installatieverantwoordelijke of de werkverantwoordelijke ervoor zorgen dat vóór de aanvang en bij de voltooiing van de werkzaamheden specifieke en uitvoerige aanwijzingen worden gegeven aan het personeel dat de werkzaamheden uitvoert.

Veel werkzaamheden zullen worden uitgevoerd op grond van een algemeen plan van aanpak dat bij alle betrokkenen bekend is, zonder dat daar specifiek over wordt gesproken of zonder dat een en ander schriftelijk is vastgelegd. Het is uiteraard niet noodzakelijk dat voor deze algemene werkzaamheden steeds een plan van aanpak moet worden opgesteld.

De installatieverantwoordelijke van Rijkswaterstaat moet erop kunnen vertrouwen dat de algemene werkzaamheden door voldoende geïnstrueerde personen volgens de gebruikelijke regelen der techniek worden uitgevoerd.

Zowel de installatieverantwoordelijke van Rijkswaterstaat als de werkverantwoordelijke moeten er steeds van overtuigd zijn dat er altijd veilig zal worden gewerkt. Bij de geringste twijfel zal ten minste mondelinge instructie moeten worden gegeven. Bij gecompliceerde werkzaamheden is een schriftelijke werkinstructie verplicht.

Voor veelvoorkomende werkzaamheden dienen standaardinstructies te worden opgesteld door de opdrachtnemer van bijv. een onderhoudscontract.

Bij Rijkswaterstaat zullen de instructies bij gecompliceerde werkzaamheden verzorgd worden door de werkverantwoordelijke, die in dienst is van de externe contractpartij.

Vóór de aanvang van de werkzaamheden moet de werkverantwoordelijke de installatieverantwoordelijke van Rijkswaterstaat informeren over de aard, de plaats en de gevolgen van de voorgenomen werkzaamheden voor de elektrische installatie. Deze informatie wordt bij voorkeur schriftelijk verstrekt, vooral als de werkzaamheden gecompliceerd zijn.

Alleen de installatieverantwoordelijke van Rijkswaterstaat mag toestemming geven om met de werkzaamheden te beginnen.

Naast procedures die de aanvang van werkzaamheden vastleggen, moeten gelijksoortige procedures worden opgesteld voor het onderbreken en beëindigen van werkzaamheden.

Een korte onderbreking als gevolg van rustpauzes, weersinvloeden e.d., waarbij de werkplek niet wordt verlaten, wordt niet als onderbreking beschouwd.

Bij werkzaamheden wordt onderscheid gemaakt in drie werkmethoden:

- spanningsloos werken
- onder spanning werken
- werken in de nabijheid van actieve delen.

Al deze procedures zijn gebaseerd op het nemen van beschermende maatregelen tegen directe aanraking en/of de gevolgen van kortsluiting en vlambogen.

8.2.1 Spanningsloos werken

Deze paragraaf behandelt de essentiële eisen die ervoor moeten zorgen dat de elektrische installatie op de werkplek spanningsloos en veilig is tijdens de duur van de werkzaamheden. Daartoe moet de werkplek duidelijk worden bepaald.

Het garanderen van de veiligheid van de werkplek is een taak van de werkverantwoordelijke. Ze worden in deze paragraaf kort aangehaald, omdat de installatieverantwoordelijke van Rijkswaterstaat ook aangewezen kan worden als werkverantwoordelijke voor de eventueel aanwezige VOP-ers in dienst van Rijkswaterstaat.

Nadat de betrokken elektrische installaties zijn bepaald, moeten de volgende vijf essentiële eisen worden aangehouden in de aangegeven volgorde, tenzij er doorslaggevende redenen zijn om daarvan af te wijken:

- volledig scheiden
- beveiligen tegen wederinschakeling
- controleren of de installatie spanningsloos is
- zorgen voor aarding en kortsluiting
- zorgen voor bescherming ten opzichte van naastgelegen actieve delen

De installatieverantwoordelijke van Rijkswaterstaat moet aan de werkverantwoordelijke toestemming geven om met de werkzaamheden te beginnen. Ieder die aan deze werkzaamheden deelneemt, moet vakbekwaam of voldoend onderricht zijn of moet onder toezicht van een vakbekwaam of voldoend onderrichte persoon staan.

Uitschakeling vóór of wederinschakeling na spanningsloos werken moet worden uitgevoerd door vakbekwame of voldoend onderrichte personen die op de hoogte zijn van alle mogelijk optredende gevaren.

Bij Rijkswaterstaat mag uitsluitend worden ingeschakeld en uitgeschakeld na goedkeuring door de werkverantwoordelijke, zie ook de werkafspraken die zijn gemaakt door Rijkswaterstaat met een contractpartij in bijv. een onderhoudscontract.

8.2.2 Volledig scheiden

Het gedeelte van de installatie waaraan wordt gewerkt, moet van alle voedingsbronnen zijn gescheiden. De scheiding moet bestaan uit een luchtweg of een even doelmatige isolatie die ervoor zorgt dat er geen doorslag plaatsvindt op de scheidingsplaats. Delen van de elektrische installatie die na volledige scheiding van de installatie nog spanning voeren moeten worden ontladen met behulp van geschikte voorzieningen.

De nulgeleider is ook een actief deel van de installatie waaraan slechts mag worden gewerkt nadat een volledige scheiding tot stand is gebracht. Bij het ontwerpen van elektrische installaties moet rekening worden gehouden met de noodzaak ook de nulgeleider volledig te kunnen scheiden. Een volledige scheiding komt niet tot stand door alleen zekeringen te verwijderen. Indien er zekerheid bestaat dat op de nulgeleider altijd een aardpotentiaal staat, is het bovenstaande uiteraard niet van toepassing. Dit komt voor bij installaties van geringe omvang waarbij aan het begin van de installatie de aarde en de nulgeleider goed met elkaar zijn verbonden.

Niet alle schakelaars realiseren voldoende scheiding. De schakelaar moet gebruikt kunnen worden als scheider, doordat de afstand tussen de schakelcontacten in geopende stand voldoende groot is. De leverancier van de schakelaar geeft dit aan.

Zijn tweede voedingen aanwezig zoals PV-systemen (zonnepanelen), UPS-systemen, noodgeneratoren en warmtekrachtsystemen, dan moeten ook deze

systemen volledig gescheiden worden van de installatie, voordat met de werkzaamheden wordt begonnen.

8.2.3 Beveiligen tegen wederinschakeling

Al het schakelmaterieel dat is gebruikt om de elektrische installatie tijdens de werkzaamheden te scheiden, moet zijn beveiligd tegen wederinschakeling, bij voorkeur door vergrendeling van het bedieningsmechanisme. Bij afwezigheid van vergrendelingsmogelijkheden moeten gelijkwaardige, in de praktijk beproefde, maatregelen tegen wederinschakeling worden genomen.

Wanneer voor de bediening van het schakelmaterieel een hulpvoedingsbron is vereist, moet deze voedingsbron buiten bedrijf zijn gesteld.

Onbevoegd ingrijpen hierin moet door middel van opschriften worden verboden. Ook kunnen afsluitbare werkschakelaars worden toegepast.

Een beproefde methode is het aanbrengen van waarschuwingsborden nadat de volledige scheiding tot stand is gebracht. Er zal gezorgd moeten worden dat deze waarschuwingsborden niet onbedoeld worden verwijderd, bijvoorbeeld door een goede toegangsregeling voor de elektrische bedrijfsruimte waarin met waarschuwingsborden wordt gewerkt en door goede instructies.

Wanneer toestellen voor afstandsbediening worden gebruikt om wederinschakeling te voorkomen, moet worden verhinderd dat deze ter plaatse met de hand worden bediend. Alle voor dit doel gebruikte toestellen voor signalering en vergrendeling moeten betrouwbaar zijn.

8.2.4 Controleren of de installatie spanningsloos is

De spanningsloze toestand moet worden gecontroleerd aan alle polen en fasen van de elektrische installatie op of zo dicht mogelijk bij de werkplek.

8.2.5 Aarding en kortsluiting

Laagspanningsinstallaties waaraan gewerkt zal gaan worden, moeten altijd geaard en kortgesloten worden wanneer het risico bestaat dat de installatie spanning gaat voeren, bijvoorbeeld:

- bij bovengrondse leidingen die worden gekruist door andere lijnen of die elektrisch worden beïnvloed
- door een noodstroomgenerator.

8.2.6 Bescherming ten opzichte van naastgelegen actieve delen

Indien er zich in de nabijheid van de werkplek delen van een elektrische installatie bevinden die niet spanningsloos kunnen worden gemaakt, moeten er speciale aanvullende voorzorgsmaatregelen worden toegepast voordat wordt begonnen met de werkzaamheden.

8.2.7 Toestemming om met de werkzaamheden te beginnen

De toestemming aan het uitvoerende personeel om met de werkzaamheden te beginnen, mag uitsluitend worden gegeven door de werkverantwoordelijke.

8.2.8 Opnieuw inschakelen na de werkzaamheden

Na voltooiing en inspectie van de werkzaamheden moeten personen die niet langer nodig zijn, worden teruggetrokken. Alle bij de werkzaamheden gebruikte gereedschappen, hulpmiddelen en (persoonlijke) beschermingsmiddelen moeten worden verwijderd. Pas dan mag met de procedure worden begonnen om de installatie opnieuw in te schakelen.

Wanneer de werkverantwoordelijke ervan is overtuigd dat de elektrische installatie opnieuw kan worden ingeschakeld, moet aan de installatieverantwoordelijke van Rijkswaterstaat worden medegedeeld dat de werkzaamheden zijn voltooid en de elektrische installatie gereed is voor wederinschakeling.

De installatieverantwoordelijke van Rijkswaterstaat zal daarna de opdracht tot wederinschakeling geven.

Als de werkzaamheden onderdeel zijn van een generieke opdracht dan hoeft de opdracht niet specifiek door de installatieverantwoordelijke van Rijkswaterstaat gegeven te worden.

In het algemeen zullen de werkverantwoordelijke en de installatieverantwoordelijke deze taak overdragen aan de persoon die ter plaatse met de leiding is belast, mits deze in staat is te beoordelen of veilig kan worden ingeschakeld. Van elke vakbekwame persoon mag dit worden verwacht in eenvoudige omstandigheden. In gecompliceerde situaties zal de werkverantwoordelijke altijd zelf de situatie moeten beoordelen.

Het verdient aanbeveling dat de overdracht schriftelijk wordt vastgelegd. Dat kan ook worden gedaan in algemene werkinstructies die gedurende een langere periode en voor meer werkzaamheden gelden in samenhang met de afspraken voor het uitschakelen.

8.2.9 Onder spanning werken

In Nederland is slechts onder zeer uitzonderlijke omstandigheden en na extra procedures en maatregelen onder spanning werken toegestaan.

Bij Rijkswaterstaat is het onder spanning werken niet toegestaan.

8.2.10 Werken in de nabijheid van niet voldoende geïsoleerde actieve delen

Werkzaamheden in de nabijheid van niet voldoende geïsoleerde actieve delen die tijdens de werkzaamheden aangeraakt kunnen worden, worden beschouwd als werkzaamheden onder spanning. Zie hiervoor paragraaf 7.2.2.

8.3 Werkzaamheden bij risicoverhogende omstandigheden

Bij risicoverhogende omstandigheden worden extra beperkingen aan werkzaamheden aan of nabij elektrische installaties en aan of met elektrische arbeidsmiddelen opgelegd. Tot de risicoverhogende omstandigheden worden gerekend:

- werkzaamheden in ongunstige weersomstandigheden
- werkzaamheden in vochtige omgevingen
- werkzaamheden in accuruimten, accukasten en acculaadstations
- werkzaamheden in omgevingen met ontploffingsgevaar

8.3.1 Werkzaamheden in ongunstige weersomstandigheden

Bij ongunstige omgevingsinvloeden gelden de volgende beperkingen:

Bij het zien van bliksem, het horen van donder of wanneer er een onweersbui nadert moeten, indien dit noodzakelijk is om gevaar te voorkomen, werkzaamheden aan installaties in de open lucht of aan een toestel dat direct is verbonden met een dergelijke installatie onmiddellijk worden gestaakt.
Bij donker weer of mist mogen, wanneer het zicht op de werkplek slecht is, geen werkzaamheden worden begonnen of voortgezet.
Worden werkzaamheden ten gevolge van slechte weersomstandigheden gestaakt, dan moet dit aan de installatieverantwoordelijke van Rijkswaterstaat worden meegedeeld.

8.3.2 Werkzaamheden in vochtige omgevingen

Werkzaamheden in de nabijheidszone of de gevarenzone in een vochtige omgeving, zowel binnen als buiten, mogen alleen bestaan uit metingen en beproevingen waarvoor het noodzakelijk is dat er actieve delen onder spanning staan.

8.3.3 Werkzaamheden in accuruimten, accukasten en acculaadstations

In accuruimten, accukasten en acculaadstations kan een ontplofbaar mengsel ontstaan tijdens en binnen twee uren na het laden van accumulatoren.

Werkzaamheden in accuruimten, accukasten en acculaadstations mogen niet worden uitgevoerd indien een ontplofbaar mengsel kan ontstaan.

Het ontstaan van een ontplofbaar mengsel kan worden voorkomen door voldoende ventilatie.

Verbindingen met accumulatoren mogen niet worden verbroken of gemaakt terwijl de laadketen onder spanning staat of de door de accumulatoren gevoede stroomketen is ingeschakeld.

8.3.4 Werkzaamheden in omgevingen met ontploffingsgevaar

Wanneer elektrotechnische werkzaamheden worden uitgevoerd op plaatsen met ontploffingsgevaar, zouden de volgende aanbevelingen moeten worden uitgevoerd:

- alle werkzaamheden of verbieden of opschorten tot passende maatregelen zijn getroffen om het ontploffingsgevaar te onderdrukken, bijvoorbeeld zorgen dat er geen brandbare gassen vrijkomen of zorgen voor voldoende ventilatie

of

- afhankelijk van de aard van het ontploffingsgevaar, geschikte maatregelen treffen om het ontploffingsgevaar te beheersen, zoals:
- een voortdurende bewaking van de atmosfeer en een verbod op elke energiebron die het ontplofbaar mengsel zou kunnen ontsteken
- een voortdurende ventilatie en bewaking van de atmosfeer
- beperking van de werkzaamheden tot het voorziene gebruik van intrinsiek veilig elektrisch materieel

Elektrotechnische werkzaamheden op plaatsen met explosiegevaar mogen alleen worden uitgevoerd door personen die daarvoor geautoriseerd zijn. Deze bepaling is in Nederland bindend.

Onderstaande informatie kan van toepassing zijn voor het veilig werken op plaatsen waar ontploffingsgevaar kan optreden.

Door de bron van de brandbare gassen of het stof weg te nemen, door ventilatie of door inert gas in te brengen kan men de gevarenzone-indeling tijdelijk veranderen en verkrijgt men een veilige werkplek.

Bij een gasconcentratie groter dan 10 % van de onderste explosiegrens (LEL-waarde) kunnen werkzaamheden worden uitgevoerd indien een ontstekingsbron ontbreekt. Onder de werkzaamheden valt ook het controleren of het desbetreffende deel van de installatie spanningsloos is.
Bij een gasconcentratie kleiner of gelijk aan 10 % van de onderste explosiegrens (LEL-waarde) kunnen werkzaamheden worden verricht waarbij een ontstekingsbron aanwezig is.

- In zone 1 controleert men de gasconcentratie op de werkplek continu.
- In zone 2 controleert men de gasconcentratie op de werkplek regelmatig.

Onder de werkzaamheden valt ook het controleren of het desbetreffende deel van de installatie spanningsloos is.

Het explosiegevaar kan ook worden weggenomen door te anticiperen op de gevarenzone-indeling en door gebruik te maken van de juiste arbeidsmiddelen en de eigenschappen van het geïnstalleerde materieel.

Dit zijn bijvoorbeeld drukvaste lamphouders bij het verwisselen van lampen en lampen met intrinsiek veilige stroombron.

Omhulsels van elektrisch materieel mogen pas worden geopend nadat de in het materieel aanwezige onderdelen zover zijn afgekoeld dat zij geen ontploffingsgevaar kunnen opleveren.

Metingen of beproevingen met elektrische meetinstrumenten in intrinsiek veilige stroomketens mogen alleen worden uitgevoerd indien de meetinstrumenten door hun constructie en gebruik de veiligheid in de zone niet aantasten.
Voor de inspectie en het onderhoud van elektrische installaties (zie NEN-EN-IEC 60079-17).

Voor de reparatie en revisie van elektrische toestellen (zie NEN-EN-IEC 60079-19).

8.3.5 Brandpreventie en brandbestrijding

Tijdens de bedrijfsvoering van elektrische installaties kan de mogelijkheid dat brand ontstaat niet worden uitgesloten.

Wanneer er brand uitbreekt, zouden delen van de elektrische installaties die gevaarlijk zijn of gevaar lopen, moeten worden afgeschakeld, tenzij deze onder spanning moeten blijven voor de brandbestrijding of omdat afschakeling andere gevaren zou veroorzaken.

Om brand in elektrische installaties te kunnen bestrijden, zullen brandblussers en brandblusmiddelen van een type dat geschikt is voor de soort brand en van een type en grootte aangepast aan de installatie, beschikbaar moeten worden gehouden en toegankelijk zijn.

De juiste personen zouden moeten worden geïnstrueerd in het gebruik van brandblussers voor de brandbestrijding, in het bijzonder met betrekking tot spanningvoerende (hulp)middelen. Deze instructie zal regelmatig moeten worden herhaald.

Bij gebruik van brandblussers en blusinstallaties op een elektrische installatie moet de juiste afstand worden aangehouden.

Personeel zal zich ervan bewust moeten zijn dat uit hete en brandende materialen giftige stoffen kunnen vrijkomen.

Zeer brandbare materialen en voorwerpen zullen zo moeten worden geplaatst en opgeslagen dat zij niet gemakkelijk in brand geraken.

8.4 Sleutelplan

De toegang tot alle ruimten waar voor leken een elektrische gevarenbron aanwezig is, moet aan regels zijn gebonden. De wijze van toegangsregeling en -controle behoort tot de verantwoordelijkheid van de installatieverantwoordelijke.

De lijst met sleutels (wie heeft welke sleutel wanneer ontvangen) ligt bij de beheerder.

Zie het document “Handboek beheer sleutelplan Technische Infrastructuur”, versie 1-1-2006.

Deuren die toegang geven tot ruimten waarin een elektrische gevarenbron aanwezig is, moeten zijn afgesloten.

Ruimten, waarin een elektrische gevarenbron aanwezig is, zijn ruimten met niet-voldoende geïsoleerde actieve delen. Onder deze ruimten moeten niet alleen elektrotechnische bedrijfsruimten verstaan worden, maar ook schakel-, verdeel- en regelkasten en bijvoorbeeld opstellingsruimten voor accu’s ten behoeve van de noodverlichting.

Ruimten waar een elektrische gevarenbron aanwezig is, mogen alleen worden betreden door:

- directieleden of daarmee gelijk te stellen functionarissen
- installatieverantwoordelijken
- werkverantwoordelijken

- vakbekwame personen
- voldoend onderrichte personen
- leken mits onder toezicht van een onder b) tot en met e) genoemd persoon

Directieleden, of daarmee gelijk te stellen functionarissen, zijn met betrekking tot hun elektrotechnische kennis gelijkgesteld aan leken. Het is raadzaam dat zij zich bij het betreden van ruimten met een elektrische gevarenbron laten vergezellen door een van de onder b) tot en met e) genoemde personen en dat hun aanwijzingen worden opgevolgd. Op grond van de wetgeving mogen werkgevers alle ruimten betreden.

8.5 Rapportage

Voor een goed beheer van de elektrische installaties en de elektrische arbeidsmiddelen is het noodzakelijk om allerlei informatie schriftelijk vast te leggen. Niet alleen de technische informatie van de installaties en arbeidsmiddelen zijn van belang, maar ook risicoanalyses, aanwijzingen, werk- en veiligheidsprocedures, verantwoordelijkheden en resultaten van inspecties.

8.6 Risicoanalyses

De vastlegging van de beoordeling van de elektrische risico's en van de bedrijfsvoering moet worden bewaard zolang deze van belang is voor de heersende veiligheid.

Het is noodzakelijk en verplicht dat de afwegingen van de risico’s en de bronnen waarop deze afwegingen zijn gebaseerd (plan van aanpak, bestek, proces-verbaal van oplevering), schriftelijk worden vastgelegd.

Zolang een installatie of een arbeidsmiddel blijft bestaan en zolang er geen nieuwe risicoanalyse is gemaakt, zal de schriftelijke vastlegging bewaard moeten blijven. Nieuwe risicoanalyses zullen worden gemaakt als het gebruik van de installatie is veranderd of als de elektrische arbeidsmiddelen onder andere omstandigheden worden toegepast.

8.7 Verantwoordelijkheid

De overdracht van verantwoordelijkheid voor de veiligheid en het tijdstip waarop deze overdracht heeft plaatsgevonden moeten worden vastgelegd.

De overdracht kan bijvoorbeeld worden vastgelegd in een logboek of worden geregeld via de tijdregistratie.

8.8 Tekeningen en documenten

Bijgewerkte tekeningen en documenten van de elektrische installatie, die noodzakelijk zijn voor het veilig beheer van de installatie, moeten beschikbaar zijn.

In de norm NEN-EN 60204 wordt gesteld dat de informatie die noodzakelijk is voor installatie, bedrijf en onderhoud van de elektrische uitrusting van machines, moet worden verstrekt in de vorm van tekeningen, schema's, diagrammen, tabellen en gebruiksaanwijzingen. Deze informatie dient direct bij oplevering te worden verstrekt.

In zowel NEN 1010 als NEN-EN 60204 worden aanvullende eisen gesteld en wordt aangegeven wat in de betreffende documenten ten minste moet worden opgenomen.

De informatie mag uiteraard ook digitaal beschikbaar zijn.

9 Bepalingen met betrekking tot inspecties, inspectiefrequenties en steekproeven

Binnen Rijkswaterstaat worden inspecties uitsluitend uitgevoerd door medewerkers van derden. De medewerkers die inspecties uitvoeren moeten zich aan de in dit hoofdstuk gestelde regels houden.

Het doel van inspectie is te controleren of een elektrische installatie voldoet aan de technische voorschriften en veiligheidsvoorschriften, zoals omschreven in de normen, die van toepassing zijn op de betreffende installatie.

De inspectie kan een controle van de normale toestand van de installatie inhouden.

Nieuwe elektrische installaties evenals wijzigingen en uitbreidingen van bestaande installaties moeten worden geïnspecteerd voordat deze in bedrijf worden genomen. Daarnaast moet een periodieke controle plaatsvinden om gebreken, die na de eerste ingebruikname zijn ontstaan, te detecteren en te verhelpen.

Het vaststellen van de inspectiefrequentie is een taak van de installatieverantwoordelijke. De installatieverantwoordelijke moet ook bepalen of bepaalde onderdelen van de periodieke inspectie met behulp van een steekproef uitgevoerd mogen worden. Is dit het geval dan moet hij/zij ook kiezen welk steekproefmethode toegepast moet worden.

Het inspecteren zelf wordt uitbesteed aan externe inspectiebureaus. Hiervoor is het wel noodzakelijk dat vaststaat volgens welke normen de installatie en/of de arbeidsmiddelen geïnspecteerd moeten worden.

9.1 Toe te passen normen

Het is de taak van de installatieverantwoordelijke van Rijkswaterstaat te bepalen aan welke normen de installatie ten minste moet voldoen. In het algemeen geldt dat de installatie ten minste moet voldoen aan de veiligheidsvoorschriften en normen die van kracht waren op de datum van eerste aanleg van de installatie. De installatie is volgens deze normen ontworpen en geïnstalleerd.

De installatieverantwoordelijke kan ook kiezen voor recentere normen die een hogere veiligheid bieden. Dit zal vooral van belang zijn als in de installatie wijzigingen of uitbreidingen zijn aangebracht.

Uitbreidingen of wijzigingen van betekenende omvang mogen niet worden gerealiseerd overeenkomstig de veiligheidsvoorschriften en normen die van kracht waren op de datum van eerste aanleg, maar moeten voldoen aan de veiligheidsvoorschriften en normen die tijdens de uitbreiding of de wijziging van kracht waren.

Soms worden ook recentere normen geëist op grond van gebruiksvergunningen of omdat Rijkswaterstaat en een externe installateur dit zijn overeengekomen.

Huurt Rijkswaterstaat roerend en/of onroerend goed met elektrische voorzieningen dan moeten in de huurovereenkomst afspraken opgenomen worden met betrekking tot het veilig beheer van die elektrische voorzieningen.

In de praktijk zal men ook worden geconfronteerd met een aantal punten die niet binnen het kader van de NEN 3140:2011, met betrekking tot het veilig omgaan met de elektrische installatie of een elektrisch arbeidsmiddel vallen, zoals:

- wettelijke voorschriften
- eisen, voorschriften en aanbevelingen van leveranciers

Daarnaast is het mogelijk dat een of meer punten, genoemd in het kader van de veiligheid, ook nog vanuit een ander kader, bijvoorbeeld een economisch of verzekeringstechnisch kader, moeten worden meegewogen.

9.2 De inspectiefrequentie

Elektrische installaties moeten met een passende regelmaat worden geïnspecteerd. Het doel van regelmatige inspecties is gebreken te ontdekken die zich na ingebruikstelling kunnen voordoen en de werking kunnen belemmeren of een mogelijke gevarenbron kunnen veroorzaken.

De te hanteren inspectiefrequenties van de elektrische installaties en de elektrische arbeidsmiddelen bij Rijkswaterstaat worden bepaald door het uitvoeren van een risicoanalyse.

Opmerking

De inspectiefrequentie is ook met behulp van NEN 3140:2011 vast te stellen.

In bijlage I van NEN 3140:2011 is een methode gegeven om de inspectiefrequentie van elektrische installaties te bepalen. De inspectiefrequentie van elektrische arbeidsmiddelen kan worden bepaald met bijlage K uit NEN 3140:2011.

9.3 Het toepassen van steekproeven

De installatieverantwoordelijke kan bepalen om bepaalde onderdelen van de elektrische installatie of bepaalde elektrische arbeidsmiddelen met een representatieve steekproef volgens een statistisch verantwoorde methode te laten inspecteren.

Door het hanteren van een steekproef ontstaat het risico dat bepaalde defecten niet gedetecteerd worden. De installatieverantwoordelijke moet aangeven welke theoretische risico's men wil nemen voor de verschillende installaties, installatieonderdelen en elektrische arbeidsmiddelen. Hierbij gelden de volgende voorwaarden:

- Het theoretisch risico, dat door de steekproef ontstaat, mag niet groter zijn dan 1%.
- Het aanvaardbare theoretische risico moet schriftelijk worden vastgelegd.

Bij het toepassen van een steekproef moeten de producten die geïnspecteerd worden aselect, dus zonder te letten op de kwaliteit, uit de totale partij gekozen worden.

In een steekproef mogen alleen gelijkwaardige producten worden opgenomen die onder gelijke omstandigheden worden gebruikt. Dit betekent dat de producten in een steekproef moeten voldoen aan de volgende voorwaarden:

- Ze moeten van hetzelfde type zijn (dezelfde afmetingen en samenstelling).
- Ze moeten in dezelfde tijd en onder dezelfde omstandigheden zijn gemonteerd.
- Ze moeten op dezelfde wijze en onder dezelfde externe condities worden toegepast.

Als een steekproef leidt tot afkeur, moeten de defecte producten worden gerepareerd waarna een nieuwe steekproef kan worden genomen. Deze procedure kan tweemaal herhaald worden. Leidt ook de derde steekproef tot afkeur dan moet de gehele partij geïnspecteerd worden.

Steekproeven bij elektrische arbeidsmiddelen zijn volgens NEN 3140:2011 alleen toegelaten als het gaat om elektrische arbeidsmiddelen met een laag risico die onder gelijke omstandigheden worden gebruikt en waarvan de som van de weegfactoren (bijlage J van NEN 3140:2011) kleiner is dan 25.

9.4 De inspectie

De inspectie van een elektrische installatie kan inhouden:

- een visuele controle
- een meting en/of beproeving

Het inspecteren vindt volgens een vaststaande procedure plaats.

Eerst wordt een pre-inspectie geheel volgens NEN 3140:2011 uitgevoerd. Hieruit kan een lijst met gebreken voortkomen.

Naar aanleiding van deze lijst met gebreken worden reparaties uitgevoerd, waarvoor separaat opdrachten moeten worden gegeven.

Daarna volgt een eindinspectie, gevolgd door een verslag en een ondertekende verklaring dat de installatie veilig is.

Deze verklaring wordt pas verstrekt nadat de gebreken zijn verholpen.

Ten behoeve van een gestructureerde en reproduceerbare uitvoering van de visuele controle en de inspectie door meting en/of beproeving wordt aanbevolen gebruik te maken van controlelijsten of meetprotocollen, in welke vorm dan ook.

Inspecties moeten worden uitgevoerd aan de hand van vereiste elektrotechnische tekeningen en specificaties.

Bij geconstateerde gebreken moeten passende herstelmaatregelen getroffen worden.

Gebreken die een onmiddellijk gevaar vormen, moeten zonder uitstel worden hersteld of defecte delen moeten worden uitgeschakeld en beveiligd tegen opnieuw aansluiten.

Rijkswaterstaat zal met de externe inspecteur afspraken maken over de wijze waarop moet worden gehandeld als tijdens het uitvoeren van inspecties defecten worden geconstateerd die direct gevaarlijk zijn. In geen geval mogen direct gevaarlijke situaties ongewijzigd blijven. Gevaar moet direct worden weggenomen.

Inspecties moeten worden uitgevoerd door vakbekwame personen die ervaring hebben met het inspecteren van gelijksoortige installaties.

Of vakbekwame personen voldoende ervaring hebben om op verantwoorde wijze inspecties uit te voeren moet steeds per situatie beoordeeld worden. Het is daarbij zeker niet voldoende om alleen te letten op opleiding die eventueel wordt bevestigd door een persoonlijk certificaat. Voldoende ervaring moet in de praktijk zijn opgedaan.

Inspecties moeten zodanig worden uitgevoerd dat gevaren worden voorkomen, waarbij, indien nodig, rekening wordt gehouden met beperkingen door de aanwezigheid van ongeïsoleerde onder stroom staande delen van de installatie. De inspectie moet worden uitgevoerd door gebruikmaking van de juiste hulpmiddelen.

Het kan zinvol zijn om op bepaalde delen van installaties of op elektrische arbeidsmiddelen stickers aan te brengen om aan te geven dat deze delen of arbeidsmiddelen zijn geïnspecteerd.

Vermeld op deze sticker ook het tijdstip van de volgende inspectie.

Het resultaat van elke inspectie moet schriftelijk of digitaal vastgelegd worden in een inspectierapport.

Het inspectierapport beoogt de registratie van de resultaten van de veiligheidsinspectie van een bestaande laagspanningsinstallatie of een elektrisch arbeidsmiddel.

Het inspectierapport is bedoeld voor diegene die verantwoordelijk is voor de veiligheid binnen de gebouwen of terreinen van Rijkswaterstaat waar de installatie zich bevindt of waar de elektrische arbeidsmiddelen worden gebruikt.

Gebruikers en eigenaren van de elektrische installatie of de elektrische arbeidsmiddelen kunnen ook rechten ontlenen aan het rapport.

Het rapport moet worden ondertekend door diegene die de inspectie feitelijk heeft uitgevoerd of onder wiens leiding de inspectie is uitgevoerd.

Bijlagen

A. Hulplijst voor vragen in een RIE bij Rijkswaterstaat

B. Handreiking voor het door de ON op te stellen Werkplan BEI voor een object of regio

Bijlage A Hulplijst voor vragen in een RIE bij Rijkswaterstaat

Met behulp van deze (niet uitputtelijke) vragenlijst kan een RIE worden opgesteld van de opzet en uitvoering van de Bedrijfsvoering Elektrische Installatie

1. Weten alle werknemers op welke wijze ze veilig met de elektrische installaties en de elektrische arbeidsmiddelen moeten werken?
2. Is er voor alle medewerkers een scholingsplan en komt daarbij de elektrotechnische veiligheid ook aan de orde?
3. Worden nieuwe medewerkers systematisch op de hoogte gebracht van de geschreven en ongeschreven regels?
4. Is er een introductieboekje voor nieuwe werknemers?
5. Wordt bij Rijkswaterstaat gewerkt door personen van derden, zoals een installatiebedrijf, schoonmaakbedrijf, een cateraar, een hovenier of een beveiligingsbedrijf?
6. Worden nieuwe personen van derden op dezelfde wijze geïnformeerd als eigen personeel?
7. Zijn er medewerkers bij Rijkswaterstaat die extra aandacht vragen bij een goed veiligheidsbeleid? (Denk bijvoorbeeld aan medewerkers die de Nederlandse taal niet goed beheersen.)
8. Is er een procedure aanwezig voor het melden van gevaarlijke situaties bij Rijkswaterstaat en is deze procedure bij alle medewerkers bekend?
9. Zijn er procedures vastgelegd in geval van calamiteiten zoals brand, spanningsuitval en dergelijke?
10. Wordt direct actie ondernomen als gevaarlijke situaties worden gemeld?
11. Worden de gevaarlijke situaties geïnventariseerd en geëvalueerd?
12. Worden de resultaten van die evaluaties gebruikt bij het beleid in de toekomst?
13. Wordt bij de aanschaf van nieuwe materialen gedacht aan de elektrotechnische gevaren?
14. Wordt bij het verstrekken van een installatieopdracht voldoende nagedacht over de elektrotechnische veiligheid?
15. Weet de inkoopafdeling en weten de toeleveranciers welke materialen voor gebruik binnen Rijkswaterstaat geschikt zijn?
16. Worden apparaten of verlichting regelmatig gehuurd bij verhuurbedrijven en zijn deze dan veilig?
17. Zijn bij Rijkswaterstaat afspraken gemaakt over de wijze waarop storingen aan de elektrische voorzieningen moeten worden opgelost?
18. Worden de juiste elektrotechnische arbeidsmiddelen gebruikt?
19. Worden de elektrotechnische installaties en de arbeidsmiddelen periodiek gecontroleerd?
20. Worden niet goedgekeurde arbeidsmiddelen en defecte delen van elektrische installaties uit bedrijf genomen?

21. Zijn de taken, de verantwoordelijkheden en de bevoegdheden met betrekking tot de elektrotechnische installatie en de elektrische arbeidsmiddelen voor alle medewerkers geregeld?
22. Zijn de elektrotechnische medewerkers van Rijkswaterstaat en haar contractpartijen aangewezen?
23. Hebben de elektrotechnische medewerkers van Rijkswaterstaat en van de contractpartijen voldoende middelen, zoals geld en tijd, om de verantwoordelijkheid met betrekking tot de veiligheid voor elektrotechnische installaties te kunnen dragen?
24. Worden de elektrotechnische medewerkers van Rijkswaterstaat en van de contractpartijen, voldoende in de gelegenheid gesteld hun kennis en vaardigheid op peil te houden en te ontwikkelen?
25. Worden de elektrotechnische medewerkers van Rijkswaterstaat en haar contractpartijen regelmatig beoordeeld over de wijze waarop ze hun verantwoordelijkheid dragen met betrekking tot het veilig werken?

Bijlage B Handreiking voor het door de ON op te stellen Werkplan BEI voor een object of regio

B.1 Doel

Het doel van het **ON-werkplan BEI** is Rijkswaterstaat inzage te geven in de activiteiten die de ON zal uitvoeren ten einde een veilige bedrijfsvoering van de elektrische installatie in te vullen. Bij steeds herhalende werkzaamheden kan met een algemeen plan worden gewerkt. Voor de overige bijzonder werkzaamheden (hoog risico, groot impact op doorstroming, werken onderspanning) kan niet worden volstaan met een algemeen werkplan.

B.2 Voor welk object of regio?

Korte beschrijving van het object of de regio, de functie ervan en van welk netwerk (vaarweg, snelweg of watersysteem) het een onderdeel is en welke installaties er binnen het object of de regio zijn.

Met welke aspecten zal er rekening mee worden gehouden, denk hierbij onder andere aan:

- Beschikbaarheideisen van de functies van een object/regio;
- Doorstroming;
- Veiligheid (ARBO), aanwezige RI&E, TRA, etc;
- Veiligheid (bij bijvoorbeeld een waterkering);
- Beschikbare tijd voor planbaar onderhoud om werkzaamheden te kunnen verrichten;
- Specifieke normen (anders dan de NEN 3140/3840) die gebruikt worden voor de uitvoering van deze werkzaamheden.

Verder dienen er beschrijvingen van bijzondere ruimtes (vochtige ruimte, explosiegevaar, nauwgeleidende ruimtes, etc.) opgenomen te zijn als deze aanwezig zijn. Eventueel kunnen de beschrijvingen vanuit DISK worden overgenomen.

B.3 Algemene normen, richtlijnen en overige documenten

De volgende normen en documenten kunnen worden geraadpleegd voor opzetten van dit werkplan BEI:

- De NEN 3140:2011 (laagspanning);
- De NEN 3840:2011 (hoogspanning);
- Het RWS-Veiligheidshandboek (beschikbaar vanaf 2013);
- Overige documenten specifiek in het contract genoemd.

B.4 Inzet van personeel en gereedschappen

Voor de diverse rollen, zoals beschreven in NEN 3140 en NEN 3840, worden eisen gesteld aan opleiding en/of ervaring.

In dit werkplan BEI moet worden opgenomen:

- de eisen die een ON stelt aan zijn personeel voor invulling van een bepaalde rol. Dit kan een eventueel worden overgenomen uit het kwaliteitshandboek van de eigen organisatie;
- Aangegeven hoe overdracht van werkzaamheden en (geven van veiligheids)instructie is geregeld met eigen personeel, personeel van derden;
- Hoe personeel van derden wordt ingezet (bijvoorbeeld van onder-ON) en welke criteria hiervoor zijn;

- Gebruik van gereedschappen en hulpmiddelen van zowel van ON als van OG die bij een kunstwerkhoren. Denk bij het laatst aan aardgarnituren, meetstokken, etc.

B.5 Invulling van de bedrijfsvoering

Hierin dienen te worden opgenomen:

- Bedieningshandelingen:
  Wie moet er geïnformeerd worden als er geschakeld gaat worden en/of wie beslist of er geschakeld mag worden;
- Meten:
  Volgens welke normen, richtlijnen, aangevuld met fabrikantgegevens van de te gebruiken meetapparatuur;
- Beproeven:
  Volgens welke normen, richtlijnen, aangevuld met fabrikantgegevens van de te gebruiken beproevingsapparatuur;
- Inspectie:
  Herhalingstijd (de NEN 3140 geeft de weging is bij een risico-inventarisatie aan, Bijlage K);
- Opleiding:
  Welke mensen worden waarvoor opgeleid, getraind en wat is de herhaling hierbij.

B.6 Procedures

In de procedures moeten zijn opgenomen hoe spanning wordt afgeschakeld en heringeschakeld, dit geschiedt onder meer met:

- Schakelbrieven:
  Voor het afschakelen en spanningsloos maken van delen van een installatie moet bekend zijn hoe dit moet gebeuren. Dit geldt voor zowel hoog- als laagspanning
- Spanningsloos maken;
- Relatie met NEN 3140 en NEN 3840.

B.7 Rapportages

Van de operationele activiteiten moeten er rapportages worden gemaakt. In deze (ON-werkplan)BEI moet onder andere worden beschreven:

- Wordt er gebruik gemaakt van een onderhoudsmanagement systeem?
- Hoe is er geïnspecteerd?
- Welke meetgereedschappen zijn er gebruikt.

B.8 Escalatiemodel

Hiervoor moet een beschrijving worden gemaakt waarin staat wat er moet gebeuren bij een gevaarlijke (elektrische) situatie (denk daarbij in het bijzonder wie moet er geïnformeerd worden, bijvoorbeeld: telefoonlijst).

B.9 Overzicht van tekeningen en documenten

Er moet een overzicht worden gemaakt welke tekeningen en documenten zijn van toepassing zijn en wat de status van deze documenten is.

Er is in principe een overzicht van tekeningen en documenten die bij de bedrijfsvoering van een object of regio horen beschikbaar. Als de status hiervan niet duidelijk is moet worden aangegeven wat er met de tekeningen en documenten moet gebeuren en/of dat er tekeningen of documenten ontbreken.

B.10 Calamiteiten

Zie B.8 Escalatiemodel.

B.11 Storingswerkzaamheden

Storingswerkzaamheden zijn in het algemeen een onderdeel van het (algemeen) werkplan. Voor de specifieke storingswerkzaamheden (hoog risico, groot impact op doorstroming, werken onderspanning) kan niet worden volstaan met het algemene werkplan en moet worden nagedacht welke maatregelen moeten worden getroffen ten einde deze storingswerkzaamheden veilig te kunnen uitvoeren. Bij gecompliceerde werkzaamheden is een werkplan verplicht….EN toestemming vooraf.

Handleiding Bedrijfsvoering Elektrische Installaties (BEI)

Nummer:	5905
Versienummer standaard:	1.0
Versienummer document:	
Status:	In beheer
Type:	Kader
Inhoudelijk beheerder:	Andre Smits
Verantwoordelijke afdeling:	District Midden
Netwerken:	
Rollen:	
Fase:	
Proceseigenaar:	Proceseigenaar Omgeving- en Assetmanagement
Link om te reageren:	*Link*

Bijlage R2 NEN 3140 Veiligheidshandboek Rijkswaterstaat addendum

NEN 3140 Veiligheidshandboek
RWS

NEN3140 Veiligheidshandboek RWS

Addendum

Behoort bij
NEN3140 Veiligheidshandboek RWS versie 2.0 Definitief

status/versie : definitief/2.0

Inhoudsopgave

1 Inleiding 3
2 Aanvullingen en/of Wijzigingen 3
3 Wijziging en releasebeheer 4

1 INLEIDING

Artikel 1.1 Algemeen

Dit document is een addendum op het document 'NEN3140 Veiligheidshandboek RWS 2.0 definitief', verder genoemd als NEN3140 Veiligheidshandboek en is in beheer bij de Community of Practice (CoP) Bedrijfsvoering Elektrische Installaties (BEI) van Rijkswaterstaat.

Dit addendum bevat wijzigingen en/of aanvullingen op de hoofdstukken/artikelen in bovengenoemd document. Hierna aangegeven.

2 AANVULLINGEN EN/OF WIJZIGINGEN

Artikel 2.1 Wijzigingen algemeen

Navolgende wijzigingen kunnen op meerdere plaatsen in het NEN3140 veiligheidshandboek voorkomen.

De zinsnede 'NEN 3140: 2011' in het NEN 3140 Veiligheidshandboek dient te worden vervangen door 'NEN 3140. Vigerende versie'.

De teksten in het NEN3140 Veiligheidshandboek die betrekking hebben op de NEN3840 en verwijzen naar (bron)teksten van de NEN3840 vervallen. Het NEN3840 Veiligheidsboek is hiervoor van toepassing.

Artikel 2.2 Wijzigingen specifiek

De navolgende hoofdstukken 3,5,7 en 8 alsmede onderliggende artikelen verwijzen naar de desbetreffende hoofdstukken en artikelen van het NEN3140 veiligheidshandboek.

3 Termen en definities

Artikel 3.2.1 Functioneel Installatieverantwoordelijke (F-IB) en Technisch Installatieverantwoordelijke (T-IV)

De zin 'Nadere definitie van deze twee rollen is vermeld in hoofdstuk 2 van het document "Handleiding Bedrijfsvoering Elektrische Installaties", versie 1.1' wordt vervangen door:
Rijkswaterstaat kiest ervoor de taken, verantwoordelijkheden en bevoegdheden (TV&B) van de titel Installatieverantwoordelijke op te splitsen naar een functioneel verantwoordelijke en een technisch verantwoordelijke.
Elektrische installaties binnen de objecten van Rijkswaterstaat hebben veelal een rol in de beschikbaarheid en veiligheid van de netwerken (Hoofdwegennet, Hoofdvaarwegennet en Hoofdwatersysteem). Vanuit de maatschappelijke functie van de netwerken staan er allerlei belangen centraal die op gespannen voet kunnen staan met de elektrische arbeidsveiligheid.
Het is daarom van belang dat de taken en verantwoordelijkheden van de installatieverantwoordelijke zodanig worden verdeeld dat enerzijds de maatschappelijke belangen vanuit de netwerken worden vertegenwoordigd en anderzijds de elektrische arbeidsveiligheid van de objecten juist kan worden beheerst.
In het beleid voor het uitvoeren van een goede BEI is er gekozen voor opsplitsen van de titel IV naar een functionele installatiebeheerder [F-IB] en een technische/operationele installatieverantwoordelijke [T-IV]. In deze moet men lezen dat de installatieverantwoordelijkheid NEN 3140/3840 zijn beperkt tot de technische inhoudelijke activiteiten.

5 Functies volgens NEN3140

Artikel 5.1 De Installatieverantwoordelijke
De vervolgende artikelnr's nummer vervangen:
par 5.101.5 vervangen door par 5.101.4
par 5.102.6 vervangen door par 5.102.7

7 Overdracht taken aan contractpartijen: aanvullende eisen

De zinsnede 'Voor het opstellen van dit werkplan is een handreiking beschikbaar, die als bijlage 2 aan dit veiligheidshandboek toegevoegd' vervangen door de zinsnede 'Voor het opstellen van dit werkplan is een handreiking beschikbaar, die als bijlage B aan dit veiligheidshandboek toegevoegd.'

8 Algemene werkvoorschriften en werkprocedures

Artikel 8.4 Sleutelplan
De zinsnede 'Zie het document "Handboek beheer sleutelplan Technische Infrastructuur", versie 1-1-2006' vervalt.

3 WIJZIGING EN RELEASEBEHEER

Artikel 3.1 Algemeen
Ingeval dit document wijzigingen ondergaat en een versie update van toepassing is zal dit door de documentbeheerder bekend worden gemaakt naar de gebruikers van dit document.

Afwijkingen en mogelijk conflicten ten gevolge van dit document dienen gemeld te worden aan de documentbeheerder genoemd in dit document.

Artikel 3.2 Content deskundigen en documentbeheer

Naam	Regio	District	taak
Andre Smits	RWS ZN	District Midden	Content deskundige
Cees Wilschut	RWS GPO		Content deskundige
Patrick v. Vliembergen	RWS PPO		Content deskundige
A. Smits	RWS ZN	Midden	Document beheerder

Artikel 3.3 Versiebeheer

Versie	Datum	Omschrijving
1.0	10 februari 2020	Release voor gebruik
2.0	7 junli 2021	Lay-out en tekstuele mutaties

Handleiding Bedrijfsvoering Elektrische Installaties (BEI)

Nummer:	5905
Versienummer standaard:	1.0
Versienummer document:	
Status:	In beheer
Type:	Kader
Inhoudelijk beheerder:	Andre Smits
Verantwoordelijke afdeling:	District Midden
Netwerken:	
Rollen:	
Fase:	
Proceseigenaar:	Proceseigenaar Omgeving- en Assetmanagement
Link om te reageren:	*Link*

Bijlage R3 NEN 3840 Veiligheidshandboek Rijkswaterstaat

Rijkswaterstaat
Ministerie van Infrastructuur en Milieu

NEN 3840 Veiligheidshandboek Rijkswaterstaat

Werken met en aan hoogspanningsinstallaties

Voor intern en extern gebruik

Datum Februari 2020
Versie 1.0
Status Definitief

Functie	Naam	Paraaf	Datum
Opsteller	C. Wilschut		27-02-2020
Gecontroleerd	A. Smits		27-02-2020
Vrijgegeven	W. R. Jansen		27-02-2020

Rijkswaterstaat
Ministerie van Infrastructuur en Milieu

Colofon

Uitgegeven door	Rijkswaterstaat
Informatie	
Telefoon	
Fax	
Uitgevoerd door	M. Tiellemans – RWS-ON P. Oranje – RWS-ZD C. Wilschut – RWS-GPO A. Smits – RWS ZN
Vrijgegeven door	W.R. Jansen – RWS-GPO
Opmaak	
Datum	Februari 2020
Status	definitief
Versienummer	1.0

Revisiehistorie

Versie	Datum	Beschrijving wijzigingen	Uitgevoerd	Distributie
0.2	Januari 2017	Nen 3840:2015 t/m hoofdstuk 4	M. Tiellemans	
0.2	Januari 2017	Nen 3840:2015 (3.5.4) hoofdstuk 5 en 6	P. Oranje	
0.2	Maart 2017	Nen 3840:2015 8.102.1 tot einde	C. Wilschut	
0.3	Mei 2017	Nen 3840:2015 hoofdstuk 7 t/m 8.102	E. Boots	
1.0	Januari 2020	Alle wijzigingen besproken en verwerkt Nen 2019	C. Wilschut	RWS

Inhoud

1	**Inleiding**	**6**
1.1	Doel, doelgroep en scope van dit document	6
1.2	Status document en gebruik	6
1.3	Aanleiding en achtergrond	6
1.4	Plaats binnen arbo	6
1.5	Leeswijzer	6
1.6	Openstaande punten	6
2	**Werken met elektriciteit**	**7**
2.1	Normen en wetgeving voor een veilige bedrijfsvoering van elektrische installaties en (elektrische) arbeidsmiddelen	7
2.2	NEN 3840 bij Rijkswaterstaat	8
2.3	NEN 3140 bij Rijkswaterstaat	9
3	**Termen en definities**	**10**
3.1	Algemeen	10
3.1.2	Bedrijfsvoering	10
3.1.3	Risico	10
3.1.6	Letsel	11
3.1.201	Elektrische bedrijfsruimte	11
3.1.202	Actief deel	11
3.2.1	Werkverantwoordelijke (WV)	11
3.2.2	Installatieverantwoordelijke (IV)	12
3.2.3	Vakbekwaam persoon (VP)	12
3.2.4	Voldoend onderricht persoon (VOP)	12
3.2.5	Leek	13
3.2.6	Bericht of aanwijzing	13
3.3	Werkzones	13
3.3.1	Werkplek	13
3.3.2	Gevarenzone	13
3.3.3	Nabijheidszone	14
3.3.101	Aanrakingsveilig	14
3.4	Arbeid	14
3.4.1	Werkzaamheden	14
3.4.2	Elektrotechnische werkzaamheden	14
3.4.3	Niet-elektrotechnische werkzaamheden	14
3.4.4	Onder spanning werken	14
3.4.5	Scheiden	14
3.4.6	Spanningsloos	15
3.4.7	Spanningsloos werken	15
3.5	Beschermingsvoorzieningen	15
3.5.1	Scherm	15

3.5.2 Afscherming 15
3.5.3 Isolerend omhulsel 15
3.5.4 Omhulsel 15
3.6 Nominale spanningen 16
3.6.101 Hoogspanning HS 16
3.101 Toezicht 16
3.101.1 Ononderbroken toezicht 16
3.101.2 Regelmatig toezicht 16
4 Onderwerp en toepassingsgebied 17
5 Functies volgens NEN 3840 18
5.1 De installatieverantwoordelijke (IV) 18
5.2 Werkverantwoordelijke [WV] 19
5.3 Vakbekwaam Persoon [VP] 20
5.4 Voldoende Onderricht Persoon [VOP] 20
5.5 Ploegleider [PL] 20
5.6 Bedieningsdeskundige [BD] 21
5.7 Leek 21
6 Voorschriften van personen in dienst van Rijkswaterstaat 22
7 Overdracht taken aan contractpartijen: aanvullende eisen 24
7.101 Het aanwijzen van personeel van contractpartijen 24
7.102 Het veilig uitvoeren van werkzaamheden 25
7.103 Bevoegdheden en verantwoordelijkheden van extern personeel 26
8 Algemene werkvoorschriften en werkprocedures 27
8.101 Algemene Veiligheidsmaatregelen 27
8.102 Werkprocedures 28
8.102.1 Spanningsloos werken [Bron NEN 3840 hoofdstuk 6.2] 29
8.102.2 Volledig scheiden [Bron NEN 3840 hoofdstuk 6.2.1] 29
8.102.3 Beveiligen tegen wederinschakeling [Bron NEN 3840 hoofdstuk 6.2.2] 29
8.102.4 Controleren of de installatie spanningsloos is [Bron NEN 3840 hoofdstuk 6.2.3]30
8.102.5 Aarding en kortsluiting [Bron NEN 3840 hoofdstuk 6.2.4] 30
8.102.6 Toestemming om met de werkzaamheden te beginnen [Bron NEN 3840 hoofdstuk 6.2.6] 30
8.102.7 Opnieuw inschakelen na de werkzaamheden [Bron NEN 3840 hoofdstuk 6.2.7]30
8.102.8 Onder spanning werken 31
8.102.9 Werken in de nabijheid van niet voldoende geïsoleerde actieve delen [Bron NEN 3840 hoofdstuk 6.2.5] 31
8.103 Werkzaamheden bij risicoverhogende omstandigheden 31
8.104 Sleutelplan 31
8.105 Rapportage 32
8.106 Risicoanalyses 32
8.107 Verantwoordelijkheid 32
8.108 Tekeningen en documenten 32

9 Bepalingen met betrekking tot inspecties, inspectiefrequenties en steekproeven 33
9.101 Toe te passen normen 33
9.102 De inspectiefrequentie 34
9.103 De inspectie 34

Bijlage A Hulplijst voor vragen in een RIE bij Rijkswaterstaat 37

Bijlage B Handreiking voor het door de ON op te stellen Werkplan BEI voor een object of regio 39
B.1 Doel 39
B.2 Voor welk object of regio? 39
B.3 Algemene normen, richtlijnen en overige documenten 39
B.4 Inzet van personeel en gereedschappen 39
B.5 Invulling van de bedrijfsvoering 40
B.6 Procedures 40
B.7 Rapportages 40
B.8 Escalatiemodel 40
B.9 Overzicht van tekeningen en documenten 40
B.10 Calamiteiten 41
B.11 Storingswerkzaamheden 41

1 Inleiding

1.1 Doel, doelgroep en scope van dit document

Dit document heeft als doel dat de veiligheid van werken met en aan elektrische installaties op een hoog niveau wordt gebracht en op dat hoge niveau blijft gehandhaafd ten einde ongevallen als gevolg van elektriciteit te voorkomen.

1.2 Status document en gebruik

Het document "NEN 3840 Veiligheidshandboek Rijkswaterstaat" is nieuw opgesteld doch geënt op het "NEN 3140 Veiligheidshandboek Rijkswaterstaat". Het gebruik van dit document is vooral bedoeld voor:

- internen Rijkswaterstaat: diegenen die met elektriciteit omgaan, zowel procesmatig als in beheer en onderhoud (objectbeheerders, weginspecteurs, contractbeheerders, bedienaars)
- externen: diegenen die in opdracht van Rijkswaterstaat werkzaamheden verrichten met of aan elektrische installaties.

1.3 Aanleiding en achtergrond

De aanleiding van dit document is het brengen van eenheid binnen Rijkswaterstaat van alle documenten die op dit gebied in de loop van de tijd zijn ontstaan en niet aan de nieuwste normen zijn aangepast.

De achtergrond van dit document is het arbobesluit dat voorschrijft dat een eigenaar van een asset, waar elektriciteit gebruikt wordt, veilig met zijn installaties omgaat en zorgt draagt voor een goede inrichting van zijn beheer van deze installaties. De NEN 3840 geeft hiervoor een goede opzet. Deze is, waar nodig, specifiek aan de organisatie van Rijkswaterstaat aangevuld en verwoord in dit document.

1.4 Plaats binnen arbo

Bij Rijkswaterstaat worden de Arbeidsomstandighedenwet en het Arbeidsomstandighedenbesluit uitgevoerd. Dit document geeft de normering voor het veilig beheer van elektrische installaties.

1.5 Leeswijzer

- Hst 2: Is een algemene tekst over werken met elektriciteit
- Hst 3: Licht de te hanteren definities binnen de NEN 3840 nader toe voor de specifieke organisatie van Rijkswaterstaat
- Hst 4: Definieert het toepassingsgebied
- Hst 5: Geeft een invulling van de installatieverantwoordelijkheid bij Rijkswaterstaat
- Hst 6: Gaat nader in op hoe medewerkers van Rijkswaterstaat en Opdrachtnemers moeten acteren
- Hst 7: Geeft kort de invulling van het overdragen van taken aan externen weer
- Hst 8: Geeft de algemene procedures en voorschriften weer
- Hst 9: Geeft het proces van inspecteren weer
- Bijlage A: Geeft een hulpvragenlijst voor het maken van een RIE
- Bijlage B: Geeft aanwijzing wat, een door de Opdrachtnemer te maken werkplan BEI, voor een inhoud moet hebben

1.6 Openstaande punten

Geen.

2 Werken met elektriciteit

Bij het gebruik van en het werken aan elektrische installaties en bij het gebruik van elektrische arbeidsmiddelen bestaat een zeker risico op letsel. Letsel kan worden veroorzaakt door:

- elektrische schok
- elektrische verbranding
- vlambogen
- brand voortkomend uit elektrische energie
- explosie voortkomend uit elektrische energie

Om deze risico's te beperken moeten elektrische installaties voldoen aan een groot aantal veiligheidseisen. Deze eisen staan in verschillende normen, regels en richtlijnen vermeld.

Voor de veilige bedrijfsvoering van elektrische installaties in de Hoogspanning zijn de normen NEN-EN 50110-1,-2 en NEN 3840 van toepassing.

2.1 Normen en wetgeving voor een veilige bedrijfsvoering van elektrische installaties en (elektrische) arbeidsmiddelen

Sinds 1998 is er een geaccepteerde norm voor het werken aan en met elektrische hoogspanningsinstallaties. Dit is momenteel en vigerend de NEN 3840:2019 (Hoogspanningsinstallaties, bedrijfsvoering van elektrische installaties).

Het doel van NEN 3840 is, voor Nederland, de algemene eisen voor de veilige bedrijfsvoering van en werkzaamheden aan, met of nabij elektrische installaties te geven.

Bedrijfsvoering van elektrische installaties omvat zowel het gebruik van elektrische installaties in het arbeidsproces als het werken aan of nabij installaties vanwege aanleg, onderhoud, reparaties, uitbreidingen en sloop.

In 2019 is van de norm NEN 3840 een nieuwe druk verschenen. Er zijn diverse redenen waarom de norm ingrijpend moest veranderen:

- de ervaring van het werken met de norm sinds 1998
- de gewijzigde Arbowetgeving
- de gegroeide praktijk
- de Europese normering
- aangepaste Europese norm EN 50110-1:2013.

De Nederlandse normering op het gebied van hoogspanningsinstallaties heeft betrekking op:

- de veilige bedrijfsvoering
- het onderhoud
- de inspectie
- het beheer

Normen zijn vastgelegde technische en procedurele afspraken waarover de betrokken belanghebbende groeperingen het eens zijn. Het feit dat normen bestaan, betekent niet automatisch dat men verplicht is om de normen toe te passen.

Het Arbeidsomstandighedenbesluit (Arbobesluit) is een geïntegreerd besluit van alle besluiten die momenteel behoren bij de Arbeidsomstandighedenwet.

In de ARBO-catalogi zijn de relevante elektrotechnische normen aangegeven. Indien de genoemde normen voor de verschillende elektrische installaties zijn toegepast, is voldaan aan de verplichtingen van het Arbobesluit.

Ook indien niet op enige wijze schriftelijk is vastgelegd dat de NEN 3840 moet worden toegepast, kan op grond van gewoonte en gebruik, de rechter van oordeel zijn dat deze norm had moeten worden toegepast. We noemen dit het 'gewoonterecht'. Naarmate de norm steeds meer algemeen wordt gebruikt, zal het gewoonterecht belangrijker worden.

2.2 NEN 3840 bij Rijkswaterstaat

Bij Rijkswaterstaat worden de Arbeidsomstandighedenwet en het Arbeidsomstandighedenbesluit uitgevoerd. Ook met betrekking tot de normering voor het veilig beheer van elektrische installaties.

De normering voor hoogspanningsinstallaties is vastgelegd in de NEN 3840. Voor Rijkswaterstaat is de toepassing van deze norm, op grond van het beleid, verplicht op alle elektrotechnische werkzaamheden.

Rijkswaterstaat kiest ervoor de taken, verantwoordelijkheden en bevoegdheden (TV&B) van de titel Installatieverantwoordelijke op te splitsen naar een functioneel verantwoordelijke en een technisch verantwoordelijke. Elektrische installaties binnen de objecten van Rijkswaterstaat hebben veelal een rol in de beschikbaarheid en veiligheid van de netwerken (Hoofdwegennet, Hoofdvaarwegennet en Hoofdwatersysteem). Vanuit de maatschappelijke functie van de netwerken staan er allerlei belangen centraal die op gespannen voet kunnen staan met de elektrische arbeidsveiligheid. Het is daarom van belang dat de taken en verantwoordelijkheden van de installatieverantwoordelijke zodanig worden verdeeld dat enerzijds de maatschappelijke belangen vanuit de netwerken worden vertegenwoordigd en anderzijds de elektrische arbeidsveiligheid van de objecten juist kan worden beheerst. In het beleid voor het uitvoeren van een goede BEI is er gekozen voor opsplitsen van de titel IV naar een functionele installatiebeheerder [F-IB] en een technische/operationele installatieverantwoordelijke [T-IV]. In deze moet men lezen dat de installatieverantwoordelijkheid NEN 3840 zijn beperkt tot de technische inhoudelijke activiteiten.

Een aanwijzing is een schriftelijke bevestiging dat de vakkennis, de ervaring, het inzicht en de vaardigheid aanwezig zijn om gevaren te herkennen en bepaalde werkzaamheden uit te voeren.

Een goed veiligheidsbeleid kan alleen maar worden gevoerd als vooraf wordt bepaald wie welke werkzaamheden mag uitvoeren en welke instructies daarvoor nodig zijn. Bij de aanwijzing van personen moet rekening worden gehouden met opleiding, ervaring en de omstandigheden waaronder gewerkt moet worden.

Normalisatie is een voortdurend proces van veranderen. Een ieder die verantwoordelijkheid draagt voor een veilige bedrijfsvoering en een veilig beheer van elektrische installaties, moet zich voortdurend op de hoogte houden.

Dit veiligheidshandboek is een aanvulling op de norm NEN 3840 in het veiligheidsbeleid van Rijkswaterstaat

De verplichting tot het naleven van de NEN 3840 is onderdeel van de arbeidsovereenkomst of de detacheringsovereenkomst of onderdeel van de overeenkomst tot het verrichten van diensten of aanneemovereenkomsten voor het uitvoeren van werkzaamheden, in welke vorm dan ook als niet expliciet naar deze normen wordt verwezen.

Waar in individuele overeenkomsten nog niet specifiek naar deze wettelijke verplichting wordt verwezen kan eenvoudig worden verwezen naar dit Veiligheidshandboek Rijkswaterstaat.

Dit veiligheidshandboek is een onderdeel van de huisregels welke gelden op alle (elektrotechnische) installaties waar Rijkswaterstaat de verantwoordelijkheid draagt voor veilige arbeidsomstandigheden.

2.3 NEN 3140 bij Rijkswaterstaat

Laagspanning is in het "NEN 3140 Veiligheidshandboek Rijkswaterstaat " beschreven.

3 Termen en definities

In dit hoofdstuk worden een aantal definities gegeven van begrippen uit de NEN 3840, die in dit veiligheidshandboek worden gebruikt. Indien noodzakelijk wordt de definitie daarna verder uitgediept om het begrip, in het kader van dit veiligheidshandboek, te verduidelijken.

3.1 Algemeen

[Cursieve tekst komt uit de norm NEN 3840:2019]

3.1.1 Elektrische installatie

Onder de "elektrische installatie" wordt verstaan:

Al het elektrisch materieel ten behoeve van de opwekking, het transport, de omzetting, de distributie en het gebruik van elektrische energie inclusief bronnen van opgeslagen energie zoals accu's, batterijen, condensatoren.

Toelichting:

De norm NEN 3840 is van toepassing op al het elektrisch materieel. Ook het elektrische materieel dat niet aangesloten is of nooit aangesloten wordt op een vaste elektrische installatie, valt onder deze norm.

3.1.2 Bedrijfsvoering

Onder "bedrijfsvoering" wordt verstaan:

Beheer, inclusief alle elektrotechnische en niet-elektrotechnische werkzaamheden, noodzakelijk om de elektrische installatie onder normale en onder abnormale omstandigheden te kunnen laten werken, zoals schakelen, regelen, bewaken en onderhoud..

3.1.3 Risico

Onder risico verstaan we een combinatie van de waarschijnlijkheid en de mate van mogelijk letsel of schade aan de gezondheid van een persoon die is blootgesteld aan een of meer gevarenbronnen.

Toelichting:

Storingen en foutief menselijk handelen kunnen de veiligheid van een elektrische installatie nadelig beïnvloeden. Om de veiligheid van een elektrische installatie te bepalen moet een risicoanalyse uitgevoerd worden. Bij een risicoanalyse moeten alle mogelijke risico's onderzocht worden.

De grootte van een risico wordt bepaald door de kans dat er iets fout gaat in de elektrische installatie en de schadelijke effecten die ontstaan ten gevolge van het falen van de elektrische installatie.

3.1.4 Elektrische gevarenbron

[Vervallen artikel]

3.1.5 Elektrisch gevaar

Onder "elektrisch gevaar" wordt verstaan:

De mogelijkheid op letsel of schade aan de gezondheid, veroorzaakt door elektriciteit.

Toelichting:

In vergelijking met andere gevarenbronnen zijn elektrische gevaren moeilijk waarneembaar. Een gaslek is te ruiken, rook en vuur zijn zichtbare verschijnselen van een brand en hoge temperaturen zijn voelbaar als warmte-uitstraling of zichtbaar als gloeiverschijnselen.

Een elektrisch gevaar wordt vaak niet opgemerkt totdat het te laat is. Dit geldt zeker voor personen die weinig of geen kennis hebben van elektriciteit. Om ongelukken te voorkomen is het noodzakelijk dat de elektrische installatie en de elektrische arbeidsmiddelen veilig zijn.

Enkele voorbeelden van bronnen van mogelijk letsel of gezondheidsrisico die aanwezig is in een elektrische installatie zijn: elektrocutie, brand, explosie, elektromagnetische velden en krachten, onbedoeld inschakelen en uitschakelen en vlambogen.

3.1.6 Letsel

Onder "letsel" wordt verstaan:

Een dodelijk ongeval of persoonlijk letsel veroorzaakt door een elektrische schok, verbranding, vlambogen, explosie of elektromagnetische velden.

Toelichting:

Uiteraard kunnen letsels ook ontstaan door allerlei andere oorzaken. Indien we echter in dit NEN 3840 Veiligheidshandboek Rijkswaterstaat spreken over letsels, worden letsels bedoeld die direct of indirect veroorzaakt zijn door elektriciteit.

3.1.201 Elektrische bedrijfsruimte

Onder een "elektrische bedrijfsruimte" wordt verstaan:

Een ruimte of plaats waarin elektrisch materieel is geïnstalleerd.

- *A) dat geen volledige bescherming heeft*
- *B) dat voornamelijk is bestemd voor het bedrijf van een elektrische installatie óf*
- *C) daar het gevaar van een explosie of vlambogen bestaat.*

3.1.202 Actief deel

Onder een "actief deel" wordt verstaan:

Een geleider of geleidend deel, bestemd om bij normaal bedrijf onder spanning te staan.

3.2 Personeel, organisatie en communicatie

In de NEN 3840 worden verschillende personen gedefinieerd met betrekking tot elektrische werkzaamheden aan, met of nabij elektrische installaties. Elke persoon heeft zijn eigen werkzaamheden, bevoegdheden en verantwoordelijkheden.

3.2.1 Werkverantwoordelijke (WV)

De "werkverantwoordelijke" is:

Een persoon die is aangewezen als direct verantwoordelijke voor de veiligheid van de werkzaamheden (en het gebruik van elektrische arbeidsmiddelen)

Opmerking: Delen van de taken van de verantwoordelijke kunnen worden gedelegeerd.

Toelichting:

Bij Rijkswaterstaat wordt de werkverantwoordelijkheid voor de veiligheid van de werkzaamheden overgedragen aan een externe contractpartij.

Bij het overdragen van de verantwoordelijkheid aan een contractpartij moet ervoor worden gezorgd dat door de contractpartij steeds voor één taak één werkverantwoordelijke is aangewezen. Hierbij moet rekening worden gehouden met het feit dat taken zich ook kunnen onderscheiden door plaats en tijd.

Voor de bij Rijkswaterstaat in dienst zijnde voldoend onderrichte personen (VOP-ers) wordt de T-IV van Rijkswaterstaat tevens als werkverantwoordelijke voor deze personen aangewezen.

Het personeel dat betrokken wordt bij de werkzaamheden aan, met of nabij elektrische installaties, moet goed zijn geïnstrueerd over de veiligheidseisen, de veiligheidsregels en de bedrijfsvoorschriften, zoals die gelden voor de werkzaamheden. Het is de taak van de werkverantwoordelijke van de contractpartij om erop toe te zien dat aan alle eisen, regels en instructies is voldaan, voordat met de werkzaamheden begonnen wordt en dat gewerkt wordt volgens die voorschriften.

Daarnaast moet de WV ervoor zorgen dat alle personen, die bij werkzaamheden zijn betrokken, zijn geïnstrueerd over eventuele bijzondere gevaren die door deze personen niet zonder meer kunnen worden herkend.

3.2.2 Installatieverantwoordelijke (IV)

Een "installatieverantwoordelijke" is:

Een persoon die is aangewezen als direct verantwoordelijke voor de veilige bedrijfsvoering van de elektrische installatie en de veiligheid van de elektrische arbeidsmiddelen.

Opmerking: Delen van de taken van de installatieverantwoordelijke kunnen worden gedelegeerd.

Bij Rijkswaterstaat is de installatieverantwoordelijkheid opgesplitst in twee rollen zie 2.2, te weten:

- de **F**unctioneel **I**nstallatie **B**eheerder (F-IB)
- de **T**echnisch **I**nstallatie **V**erantwoordelijke (T-IV)

Bij Rijkswaterstaat zijn de F-IB en de T-IV normaal medewerkers van de eigen organisatie maar hierop zijn uitzonderingen mogelijk. De T-IV kan worden belegd bij de opdrachtnemer, die zorgt draagt voor een aanwijzing van een eigen deskundig persoon die werkzaamheden op zich kan nemen. De overgedragen werkzaamheden dienen beschreven te worden.

RWS wil zich vergewissen van de deskundigheid van de aangewezen personen, zie 3.2.6.

Bij bepaalde elektrotechnische installaties bij Rijkswaterstaat kunnen substantiële delen van de verantwoordelijkheid worden overgedragen aan een contractpartij. Bij het overdragen van de verantwoordelijkheid aan een contractpartij moet ervoor worden gewaakt dat steeds voor één taak, één verantwoordelijke is aangewezen. Hierbij moet rekening worden gehouden met het feit dat taken zich ook kunnen onderscheiden door plaats en tijd.

De eindverantwoordelijkheid van een object, binnen het kader van de RWS-BEI, ligt bij de F-IB.

3.2.3 Vakbekwaam persoon (VP)

Een "vakbekwaam persoon" is:

Een persoon die is aangewezen en met een relevante opleiding en ervaring waardoor hij/of zij in staat is gevaren die door elektriciteit kunnen worden veroorzaakt te onderkennen en te voorkomen.

Toelichting:

Rijkswaterstaat kent voor de hoogspanning geen "Vakbekwaam persoon".

3.2.4 Voldoend onderricht persoon (VOP)

Een "voldoend onderricht persoon" is:

Een persoon die is aangewezen en die voldoende is geïnstrueerd voor specifieke taken en werkzaamheden en het gebruik van arbeidsmiddelen waardoor hij/zij in staat is gevaren die door elektriciteit kunnen worden veroorzaakt te onderkennen en te voorkomen.

Toelichting:

Bij Rijkswaterstaat zijn geen voldoend onderrichte personen in dienst die elektrotechnische werkzaamheden mogen verrichten. De T-IV van de elektrische installaties waaraan werkzaamheden moeten worden verricht wordt, voor personen, tevens aangewezen als WV.

Dit houdt in dat de betreffende T-IV tevens de taken van de WV op zich moet nemen, zoals het instrueren over de mogelijke gevaren die de werkzaamheden met zich meebrengen en de te nemen veiligheidsmaatregelen om deze gevaren te voorkomen.

3.2.5 Leek

Een "leek" is:

Een persoon die geen installatieverantwoordelijke, werkverantwoordelijke, vakbekwaam persoon, ploegleider, voldoende onderricht persoon of bedieningsdeskundige is.

Toelichting:

Zonder specifieke aanwijzing wordt binnen Rijkswaterstaat iedereen als leek beschouwd. Dit geldt ook voor medewerkers die wel elektrotechnisch zijn opgeleid maar niet zijn aangewezen voor werkzaamheden onder verantwoordelijkheid van Rijkswaterstaat.

Een leek mag een ruimte waar een elektrische gevarenbron aanwezig is, alleen betreden mits hij/zij onder toezicht staat van minimaal één voldoend onderricht persoon, na goedkeuring door de werkverantwoordelijke of de T-IV.

3.2.6 Bericht of aanwijzing

Te allen tijde mag Rijkswaterstaat er zich van vergewissen dat een aanwijzing volgens de norm NEN 3840, voor alle die op enige wijze betrokken zijn bij werkzaamheden, op juiste gronden heeft plaatsgevonden. Toets opleiding en kwalificaties, bijv. Stipel, etc.

3.3 Werkzones

Om het risico van het aanraken van niet of slecht geïsoleerde delen van een elektrische installatie in te kunnen schatten is in de NEN 3840 elke werkplek ingedeeld in zones.

3.3.1 Werkplek

Onder de "werkplek" wordt verstaan:

De plaats waar werkzaamheden worden, zijn of nog moeten worden uitgevoerd.

3.3.2 Gevarenzone

Onder de "gevarenzone" wordt verstaan:

Een beperkte ruimte rondom actieve delen.

Toelichting:

In de definitie wordt gesproken over actieve delen waar het isolatieniveau niet is gewaarborgd. Hiermee worden onder spanning staande niet of slecht geïsoleerde delen van de elektrische installatie bedoeld.

3.3.3 **Nabijheidszone**

Onder de "nabijheidszone" wordt verstaan:

Een beperkte ruimte rondom de gevarenzone.

3.3.101 **Aanrakingsveilig**

Toelichting:

Bij Rijkswaterstaat is dit objectafhankelijk en zal door de T-IV per object/onderdeel moeten worden vastgelegd.

3.4 Arbeid

Alle definities in deze paragraaf hebben direct of indirect betrekking op de aanwezigheid van een elektrische gevarenbron.

3.4.1 **Werkzaamheden**

Onder "werkzaamheden" wordt verstaan:

De vorm van elektrotechnische of niet-elektrotechnische werkzaamheden waarbij een elektrische gevarenbron aanwezig kan zijn.

3.4.2 **Elektrotechnische werkzaamheden**

Onder "elektrotechnische werkzaamheden" wordt verstaan:

Werkzaamheden aan, met of nabij een elektrische installatie, zoals beproeven en meten, repareren, vervangen, aanpassen, uitbreiden, installeren, onderhouden en inspecteren.

3.4.3 **Niet-elektrotechnische werkzaamheden**

Onder "niet-elektrotechnische werkzaamheden" wordt verstaan:

Werkzaamheden nabij een elektrische installatie, zoals bouwen, graven, schoonmaken en schilderen.

Toelichting:

Elektrotechnische werkzaamheden zoals het aanbrengen van kabeldraagsystemen, en het leggen van (grond)kabels kunnen onder bepaalde omstandigheden, indien bij de werkzaamheden geen elektrotechnische gevaren kunnen bestaan, beschouwd worden als niet-elektrotechnische werkzaamheden.

3.4.4 **Onder spanning werken**

Onder "onder spanning" werken wordt verstaan:

Alle werkzaamheden waarbij een persoon met delen van zijn of haar lichaam, met gereedschappen, hulpmiddelen of (persoonlijke) beschermingsmiddelen, waarmee wordt gewerkt, terecht kan komen in de gevarenzone.

Toelichting:

In Nederland, dus ook bij Rijkswaterstaat, is in het arbeidsomstandighedenbesluit bepaald dat het werken onder spanning niet is toegestaan. Werken in de nabijheid van actieve delen

Onder "werken in de nabijheid van actieve delen" wordt verstaan:

Alle werkzaamheden waarbij een persoon met delen van zijn lichaam, met gereedschap of met een ander voorwerp terecht kan komen in de nabijheidszone zonder nog binnen te dringen in de gevarenzone.

3.4.5 **Scheiden**

Onder "scheiden" wordt verstaan:

Het volledig vrijmaken van een toestel of stroomkring van andere toestellen of stroomkringen.

3.4.6 **Spanningsloos**

Onder "Spanningsloos" wordt verstaan:

Een spanningswaarde van (vrijwel) 0 V, dat wil zeggen zonder aanwezige spanning en/of lading.

Toelichting:

In de actuele U.C.T.E. richtlijn is de aanduiding "Spanningsloosheid aantonen" voor de hoogspanningsinstallaties vervangen door de aanduiding "Aantonen afwezigheid van bedrijfsspanning".

3.4.7 **Spanningsloos werken**

Onder "Spanningsloos werken" wordt verstaan:

Werkzaamheden aan een elektrische installatie die zonder spanning of lading is en die worden uitgevoerd nadat allen maatregelen ter voorkoming van elektrisch gevaar zijn genomen.

Toelichting:

Bij spanningsloos werken moet de werkplek tijdens de duur van de werkzaamheden spanningsloos en daardoor veilig zijn.

Hiervoor moet aan essentiële voorwaarden worden voldaan. Deze staan vermeld in de norm NEN 3840 onder paragraaf 6.2 "Spanningsloos werken".

3.5 Beschermingsvoorzieningen

Om onder spanning staande delen van een elektrische installatie te beveiligen tegen toevallige aanraking zijn verschillende beschermingsvoorzieningen toepasbaar. De meest toepasbare worden hier besproken.

3.5.1 **Scherm**

Onder "scherm" wordt verstaan:

Een voorziening, al of niet geïsoleerd, die wordt gebruikt om nadering van materieel of een deel van een elektrische installatie dat gevaar kan opleveren, te voorkomen.

3.5.2 **Afscherming**

Onder "afscherming" wordt verstaan:

Een voorziening die bescherming biedt tegen directe aanraking vanuit elke gebruikelijke richting van benadering.

3.5.3 **Isolerend omhulsel**

Onder een "isolerend omhulsel" wordt verstaan:

Een starre of flexibele voorziening van isolerend materiaal die wordt gebruikt om toevallige aanraking te voorkomen van actieve en/of spanningsloze delen en/of naastgelegen delen.

3.5.4 **Omhulsel**

Onder een "omhulsel" wordt verstaan:

Een voorziening ter bescherming van materieel tegen bepaalde uitwendige invloeden en ter bescherming tegen directe aanraking naar alle richtingen.

3.6 Nominale spanningen

3.6.101 Hoogspanning HS

Spanning die normaal hoger is dan 1 000 V bij wisselspanning of 1 500 bij gelijkspanning

Voor hoogspanningsinstallaties geldt de NEN 3840 (Bedrijfsvoering van elektrische installaties – Aanvullende Nederlandse bepalingen voor hoogspanningsinstallaties).

Voorbeelden van installaties met hoogspanning zijn:

- Zware elektrisch aangedreven pompen (gemalen Panheel, Zedemuden, IJmuiden, Eefde), deze worden gevoed via transformatoren
- Verdelingen Stormvloedkeringen, grote sluiscomplexen (IJmuiden, Terneuzen)
- Aansluitingen verdeling voeding tunnels (ook step-up transformatoren)

Rijkswaterstaat streefde tot voor kort ernaar de hoogspanningsinstallaties onder te brengen bij energieleveranciers/netbeheerders/derden. Doch in het kader van beschikbaarheid en veiligheid zullen er steeds meer hoogspanningsinstallaties in eigendom van Rijkswaterstaat zijn/komen.

3.101 Toezicht

OPMERKING: voor aanvullende informatie zie NEN3840, bijlage C.

3.101.1 Ononderbroken toezicht

Onder "Ononderbroken toezicht" wordt verstaan:

Toezicht met als doel dat werkzaamheden veilig worden uitgevoerd en dat gedurende de werkzaamheden altijd aanwezig is.

Toelichting:

De T-IV en de WV bepalen in onderling overleg of er ononderbroken toezicht benodigd is.

3.101.2 Regelmatig toezicht

Onder "Regelmatig toezicht" wordt verstaan:

Toezicht met als doel dat werkzaamheden veilig worden uitgevoerd en dat gedurende de werkzaamheden regelmatig wordt uitgevoerd.

Toelichting:

De T-IV en de WV bepalen in onderling overleg of er regelmatig toezicht benodigd is.

4 Onderwerp en toepassingsgebied

Deze norm is van toepassing op alle bedrijfsvoering van en werkzaamheden aan, met of nabij elektrische installaties met een spanningsniveau groter dan 1 000 V wisselspanning of 1 500 V gelijkspanning.

Omdat op alle objecten van Rijkswaterstaat elektrische installaties en (elektrische) arbeidsmiddelen ruimschoots aanwezig zijn is dit veiligheidshandboek van belang voor alle medewerkers. Het maakt daarbij niet uit of de medewerkers in dienst zijn van de eigen organisatie, zijn ingeleend of een arbeidsrelatie hebben met een contractpartij.

De elektrische installaties zijn ontworpen voor de opwekking, het transport, de omzetting, de distributie en het gebruik van elektrische energie. De meeste van deze elektrische installaties zijn permanent en vast aangebracht, zoals een installatie voor de distributie van elektrische energie in een tunnel of een sluis. Andere installaties zijn tijdelijk, zoals op bouwplaatsen en kunnen worden verplaatst wanneer zij onder spanning staan of in bedrijf zijn.

De norm NEN 3840:2019 geeft de eisen weer voor de veilige bedrijfsvoering van en de werkzaamheden aan, met of nabij elektrische hoogspanningsinstallaties. Onder bedrijfsvoering wordt verstaan alle handelingen en werkzaamheden die noodzakelijk zijn om de elektrische installatie te kunnen laten werken zoals schakelen, regelen, bewaken en onderhoudswerkzaamheden.

De norm geldt voor alle elektrotechnische en niet-elektrotechnische werkzaamheden, zoals bouwwerkzaamheden en graafwerkzaamheden als in de omgeving elektrische leidingen aanwezig zijn die onder spanning staan.

De norm is ook van toepassing op het gebruik, het onderhoud, de inspectie en het beheer van (elektrische) arbeidsmiddelen.

Onder een (elektrisch) arbeidsmiddel wordt verstaan: elke op de arbeidsplaats gebruikte machine, gereedschap, apparaat, hulpmiddel en persoonlijk beschermingsmiddel dat door de aard van hun gebruik of de omgevingsomstandigheden een elektrisch veiligheidsrisico kan opleveren.

De norm NEN 3840:2019 heeft betrekking op elektrische installaties en (elektrische) arbeidsmiddelen, met een spanningsniveau van hoogspanning.

De bepalingen leggen een taak bij de T-IV. Hij/zij moet bij voortduring controleren of de elektrotechnische voorzieningen aan de vereiste normen blijven voldoen en of die voorzieningen op de juiste wijze en in de juiste omgeving worden gebruikt.

Normen veranderen doordat producten veranderen. Hierdoor ontstaan steeds weer nieuwe normen zodat de producten kunnen innoveren. Welke norm relevant is hangt onder andere af van de normen die gebruikt zijn bij het vervaardigen van de installatie of het product. Naast de verschillende normen zijn ook tal van Europese regels en richtlijnen van toepassing op de verschillende elektrische installaties en elektrische arbeidsmiddelen, zoals de laagspanningsrichtlijn, de machinerichtlijn en de EMC-richtlijn.

5 Functies volgens NEN 3840

5.1 De installatieverantwoordelijke (IV)

De installatieverantwoordelijke is een persoon die is aangewezen, door of namens de hoogste verantwoordelijke voor de naleving van de ARBO-wet, als direct verantwoordelijke voor de veilige bedrijfsvoering van de elektrische installatie en de veiligheid van de elektrische arbeidsmiddelen *(Bron: NEN 3840, par. 3.2.2, par 4.2.202).*

Verantwoordelijkheden

De installatieverantwoordelijke is verantwoordelijk voor:

1. De elektrische installaties en elektrische arbeidsmiddelen *(Bron: NEN 3840, par. 3.2.2);*
   NB: De IV kan eigen personeel zijn of tot een andere organisatie behoren *(Bron: NEN 3840, par. 4.2.202)*. Bij uitbesteding of aanneming moet er worden getoetst of de persoon aan de juiste criteria 's voldoet *(Bron: NEN 3840, Bijlage D.)*;
2. Het in stand houden van de veiligheid van elektrische installaties en elektrische arbeidsmiddelen, door regelmatige inspecties en tijdig herstel van gevonden gebreken *(Bron: NEN 3840, 5.3.3);*
   NB: Het inspectie-interval wordt door de installatieverantwoordelijke in een onderhoudsconcept onderbouwd en vastgelegd. *(Bron: NEN 3840, par. 5.3.3.1.202);*
   NB: De eisen/uitvoering met betrekking tot de inspectie van nieuwe of gewijzigde hoogspanningsinstallaties zijn onder andere gegeven in NEN-EN-IEC 61936. De resultaten/gegevens van zo'n inspectie kunnen als referentie dienen voor navolgende inspecties *(Bron: NEN 3840, par 5.3.3.1.201)*;
3. Toegangsbeleid.
   De toegang tot alle ruimten waar leken aan een elektrische gevarenbron zijn blootgesteld, moet aan regels zijn gebonden.
   De wijze van toegangsregeling en -controle behoort tot de verantwoordelijkheid van de installatieverantwoordelijke. *(Bron: NEN 3840, par 4.3)*;
4. De bedieningshandelingen moeten worden uitgevoerd volgens de bedrijfsinstructies, die goedgekeurd zijn door de installatieverantwoordelijke. *(Bron: NEN 3840, par 5.2.1.203)*;
5. Het goedkeuren van plannen voor de uitvoering van werkzaamheden, de werkverantwoordelijke is verantwoordelijk voor de werkrisico's *(Bron: NEN 3840, par 4.3)*;
6. Het toestemming geven voor de aanvang van werkzaamheden *(Bron: NEN 3840, par 4.3, par 4.4)*;
   De werkverantwoordelijke en de installatieverantwoordelijke moeten beide instemmen met zowel de configuratie van de elektrische installatie on de werkzaamheden te kunnen laten beginnen als met een beschrijving van de werkzaamheden aan, met of nabij de elektrische installatie voordat wijzigingen aan de configuratie van de elektrische installatie worden doorgevoerd of werkzaamheden worden uitgevoerd. Voordat met werkzaamheden wordt begonnen, moet de installatieverantwoordelijke over de voorgenomen werkzaamheden worden geïnformeerd.
7. Het goedkeuren van bedieningshandelingen *(Bron: 3840, par 5.1);*
   Aan de installatieverantwoordelijke moet worden gemeld wanneer de standaard bedrijfsvoeringsprocedures zijn voltooid.

8. Afspraken met andere installatieverantwoordelijke wanneer installaties of elektrische arbeidsmiddelen zich in elkaars nabijheid bevinden *(Bron: NEN 3840, par. 4.3)*;
   Op het scheidsvalk tussen twee beheersgebieden moet duidelijk en ondubbelzinnig worden vastgesteld waar de scheidlijn tussen de installatieverantwoordelijkheid van de ene partij en van de andere partij. Deze afspraken moeten schriftelijk worden vastgesteld.
9. Het goedkeuren van de onderhoudsprocedure *(Bron: NEN 3840, par 7.2.1);*

NB: Delen van de taken van de installatieverantwoordelijke kunnen worden gedelegeerd *(bron: NEN 3840 par. 3.2.2).*

Binnen RWS heeft ervoor gekozen de taken van de installatieverantwoordelijke te belegd bij (in het algemeen) 2 functionarissen: de functioneel beheerder (F-IB) en de technische installatieverantwoordelijke (T-IV). Dit geldt voor zowel de laagspanning als de hoogspanning. Er is echter een uitzondering mogelijk dat de T-IV wordt belegd bij een opdrachtnemer. Dit wordt geregeld in het contract met deze opdrachtnemer.

De punten 1 en 8 zijn zaken die een sterke relatie hebben met beleid en worden daarom belegd bij de F-IB. In praktijk zullen deze punten worden uitgewerkt door de T-IV en geaccepteerd worden door de F-IB. Hierna kan de T-IV zorg dragen voor de uitvoering hiervan.

De eindverantwoordelijkheid van de BEI van een object ligt bij de F-IB.

Opleiding

Afhankelijk van een contract, kunnen taken van de T-IV bij een marktpartij worden neergelegd. Dit is verwoord in de projecteigen vraagspecificatie.

De installatieverantwoordelijke heeft ten minste een middelbaar elektrotechnisch niveau verkregen door opleiding en/of ervaring. De IV is verantwoordelijk voor de uitvoering van het eigen takenpakket en moeten zich daarvoor kunnen verantwoorden. *Tot de verantwoordelijkheid kunnen planning, administratie, beheer en/of ontwikkeling horen*. De werkzaamheden worden meestal zelfstandig en zonder toezicht verricht *(Bron: NEN 3840 par. 4.2.204).*

5.2 Werkverantwoordelijke [WV]

Definitie

De werkverantwoordelijke is een persoon die is aangewezen als direct verantwoordelijke voor de veiligheid van de werkzaamheden en het gebruik van elektrische arbeidsmiddelen. *(Bron: NEN 3840, par. 3.2.1).*

Verantwoordelijkheden

De werkverantwoordelijke is verantwoordelijk voor:

- Waar de werkzaamheden langdurig of gecompliceerd zijn, moeten de instructies tijdens de voortgang van de werkzaamheden worden herhaald dit ter beoordeling van de werkverantwoordelijke. (bron NEN 3840, par 4.2)
- Elektrische veiligheid bij alle werkzaamheden *(Bron: NEN 3840, par. 3.2.1)*;
  NB: De WV kan eigen personeel zijn of tot een andere organisatie behoren;
  NB: De WV toetst of aan alle regels en instructies is voldaan;
- Het vaststellen van de risico's verbonden aan werkzaamheden *(Bron: NEN 3840, par. 6.1)*;
- Het opstellen van plannen voor werkzaamheden *(Bron: NEN 3840, par. 4.2.204)*;
- Het kiezen van de juiste uitvoerenden voor werkzaamheden *(Bron: NEN 3840, par. 5.3.2.1.201)*;
- Alle werkzaamheden moeten worden voorbereid door de werkverantwoordelijke *(Bron: NEN 3840 par. 6.1)*;
- Het instrueren van de uitvoerenden bij werkzaamheden *NEN 3840 par. 4.2)*;

- De werkverantwoordelijke stelt bij de voorbereiding van de werkzaamheden de frequentie en de aard van het toezicht vast. *(Bron: NEN 3840, Bijlage C.3)*;
- Informeren van de installatieverantwoordelijke over aard, plaats, veiligheidsmaatregelen en gevolgen werkzaamheden *(Bron: NEN 3840 par. 6.1);*
- Bij spanningsloos werken:
  - veiligheid op de werkplek *(Bron: NEN 3840, par. 6.2.2 – 6.2.6);*
  - inspectie van installatie voor ingebruikname, ook als deel van de installatie hiervoor van spanning moet zijn voorzien *(Bron: NEN 3840, par. 6.2.7);*

NB: Delen van de taken van de werkverantwoordelijke kunnen worden gedelegeerd *(Bron: NEN 3840 par. 3.2.1).*

Opleiding

De Werkverantwoordelijken heeft ten minste een middelbaar elektrotechnisch niveau verkregen door opleiding en/of ervaring. De WV is verantwoordelijk voor de uitvoering van het eigen takenpakket en moeten zich daarvoor kunnen verantwoorden. *Tot de verantwoordelijkheid kunnen planning, administratie, beheer en/of ontwikkeling horen.* De werkzaamheden worden meestal zelfstandig en zonder toezicht verricht *(Bron: NEN 3840 par. 4.2.204).*

5.3 Vakbekwaam Persoon [VP]

Definitie

Een Vakbekwaam Persoon is een persoon die is aangewezen en met een relevante opleiding en ervaring waardoor hij in staat is gevaren die door elektriciteit kunnen worden veroorzaakt te onderkennen en te voorkomen *(Bron: NEN 3840, par. 3.2.3).*

Opleiding

Vakbekwame personen hebben ten minste een lager elektrotechnisch niveau verkregen door opleiding en/of ervaring. Ze zijn verantwoordelijk voor de uitvoering van het eigen takenpakket en moeten zich daarvoor kunnen verantwoorden. Ze werken meestal zelfstandig onder indirect toezicht en soms onder direct toezicht *(Bron: NEN 3840 par. 4.2.205).*

5.4 Voldoende Onderricht Persoon [VOP]

(zie ook hoofdstuk 6)

Definitie

Een Voldoende Onderricht Persoon is een persoon die is aangewezen en die voldoende is geïnstrueerd voor specifieke taken, werkzaamheden en het gebruik van elektrische arbeidsmiddelen waardoor hij in staat is gevaren die door elektriciteit kunnen worden veroorzaakt te onderkennen en te voorkomen *(Bron: NEN 3840, par. 3.2.4).*

Werkzaamheden

Voorbeelden van werkzaamheden die voldoende onderrichte personen, na instructie, kunnen uitvoeren zijn:

- Het bedienen van elektrische installaties;
- Het gebruiken van elektrische arbeidsmiddelen;
- Het uitvoeren van eenvoudige elektrotechnische werkzaamheden;

Opleiding/ervaring

Voldoende onderrichte personen zijn, door instructie, in staat om bij hun werkzaamheden elektrische gevaren te vermijden. Ze kunnen, na instructie, bedrijfsspecifieke werkzaamheden uitvoeren waarvan de elektrische risico's beperkt zijn *(Bron: NEN 3840 par. 4.2.206).*

5.5 Ploegleider [PL]

Een ploegleider is een vakbekwaam persoon die ter plaatse met de leiding van werkzaamheden is belast *(Bron: NEN 3840 par. 3.2.202).*

Een ploegleider heeft de leiding over de uitvoering van werkzaamheden wanneer de Werkverantwoordelijke deze bij afwezigheid heeft gedelegeerd aan de ploegleider *(Bron: NEN 3840 par. 6.2.0.201).*

Noot: Rijkswaterstaat kent geen "Ploegleider" en personeel van Rijkswaterstaat zal ook niet voor deze rol worden aangewezen.

5.6 Bedieningsdeskundige [BD]

Een bedieningsdeskundige is een persoon die is aangewezen als direct verantwoordelijk persoon voor bedieningshandelingen, waarbij deze handelingen worden gecoördineerd vanuit één punt *(Bron: NEN 3840 par. 3.2.203).*

Bedieningshandelingen in complexe installaties, waarbij de bediening wordt gecoördineerd vanuit één punt, mogen worden uitgevoerd door een bedieningsdeskundige. Hierbij gaat het om het (op afstand) uitvoeren van bedieningshandelingen of het opdracht geven tot bedieningshandelingen om de continuïteit van het proces en de veiligheid van het personeel te waarborgen.

Deze bedieningshandelingen moeten worden uitgevoerd volgens bedrijfsinstructies, die zijn goedgekeurd door de T-IV.

Bedieningsdeskundigen mogen binnen het raamwerk van deze instructie ook opdrachten geven voor bedieningshandelingen die niet op afstand kunnen worden uitgevoerd *(Bron: NEN 3840 par. 5.2.1.203).*

5.7 Leek

Een leek is een persoon die geen installatieverantwoordelijke, werkverantwoordelijke, vakbekwaam persoon, voldoende onderricht persoon, ploegleider en bedieningsdeskundige is van de desbetreffende installatie *(Bron: NEN 3840, par. 3.2.5).*

Een leek mag slechts:

- een ruimte met elektrisch gevaar betreden, onder toezicht van ten minste VOP *(Bron: NEN 3840, par. 4.3.202)*;
- metingen uitvoeren aan een elektrische installatie, uitsluitend onder ononderbroken toezicht van ten minste VP (Bron: NEN 3840, par. 5.3.1.1);
- beproevingen uitvoeren aan een elektrische installatie, onder voortdurend toezicht van ten minste VP (Bron: NEN 3840, par. 5.3.2.1);
- Voor werkzaamheden door een leek geldt de specifieke afstand tot de actieve delen afgeleid uit D_v uit tabel A.1 (Bron: NEN 3840, par. 6.4.4);

De NEN 3840 is niet van toepassing op het gebruik van installaties, toebehoren en (hulp)middelen door leken, mits installaties, toebehoren en hulpmiddelen zijn ontworpen en geïnstalleerd voor gebruik door leken en voldoen aan de desbetreffende normen

6 Voorschriften van personen in dienst van Rijkswaterstaat

Binnen de organisatie van Rijkswaterstaat worden op in de hoogspanningsinstallatie ook, in zeer geringe mate, elektrotechnische werkzaamheden uitgevoerd door eigen medewerkers.

De hoogspanningsinstallatie zijn uitbesteed aan de onderhoudspartij waarbij de verantwoordelijkheid bij de aannemende partij ligt.

Binnen de Oosterschelde kering is de opdrachtnemer verantwoordelijk voor de hoogspanning. En heeft Rijkswaterstaat bedieningsdeskundige aangesteld die de bedieningshandelingen van uit de centrale bediening uitvoeren.

Bij een operationele fase van de Oosterscheldekering is er in elk bedienteam de volgende personen aangesteld:

- Operationeel installatie verantwoordelijke.
- Werkverantwoordelijke
- Voldoende onderricht persoon

Deze personen hebben instructie gehad voor de werkzaamheden die nodig kunnen zijn tijdens deze operationele fase (sluiten van de Kering bij een verwachte hoge waterstand).
Ook krijgen deze personen jaarlijks een herhalingsopleiding in de hoogspanningsinstallatie.

Deze personen zijn schriftelijk aangesteld door de T-IV en de F-IB

Nimmer mogen werkzaamheden met een elektrotechnisch gevaar worden uitgevoerd als de medewerkers niet zijn aangewezen door de T-IV of de werkverantwoordelijke.

Van het eigen personeel en van personeel van derden moet worden geëist dat het zich houdt aan de eisen, regels en instructies, zoals deze door Rijkswaterstaat zijn opgesteld. Er kunnen disciplinaire maatregelen worden genomen tegen eigen personeel dat zich niet aan de eisen, regels en instructies houdt. Voor personeel van contractpartijen kan een regeling worden vastgesteld in de aanneemovereenkomst.

Het is noodzakelijk dat schriftelijk wordt vastgelegd op welke wijze is beoordeeld dat bij de persoon voldoende kennis en ervaring aanwezig is om de werkzaamheden uit te voeren. Ten minste moet beoordeeld worden of de personen die de werkzaamheden uitvoeren, voldoende:

- Kennis van elektriciteit bezitten.
- Ervaring met de betreffende elektrotechnische werkzaamheden hebben.
- Inzicht hebben in mogelijke gevaren tijdens de werkzaamheden en de in acht te nemen voorzorgsmaatregelen.
- Vaardigheid bezitten om te allen tijde te onderkennen of het veilig is om de werkzaamheden voort te zetten.

Dit is van toepassing op al het personeel dat op enige wijze betrokken is bij alle soorten werkzaamheden aan elektrische installaties.

Ook worden deze eisen gesteld aan de personen die op enige wijze werken met elektrotechnische installaties of werken in de omgeving van elektrotechnische installaties. Dit geldt voor elektrotechnische werkzaamheden, voor bedieningswerkzaamheden

Het aanwijzingsdocument voor de persoon in dienst van Rijkswaterstaat moet ten minste de volgende punten bevatten:

- De naam en de geboortedatum of het personeelsnummer van de persoon.
- De functie van de persoon binnen het bedrijf en de afdeling.
- De ingangsdatum en eventueel de einddatum van de aanwijzing.
- De werkzaamheden die de persoon mag uitvoeren.
- De omstandigheden waaronder de persoon de werkzaamheden mag uitvoeren.
- De ruimte(n) waarin de persoon de werkzaamheden mag uitvoeren.
- De installatie(s) of delen van installatie(s) waaraan de persoon de werkzaamheden mag uitvoeren.
- De verantwoordelijkheden en bevoegdheden die de persoon krijgt.
- De gereedschappen, hulpmiddelen en (persoonlijke) beschermingsmiddelen waarover de persoon de beschikking krijgt.
- De plaats en datum van de aanwijzing.
- De naam en de functie van de persoon die aanwijst.
- De handtekening van de persoon die aanwijst en de handtekening van de persoon die wordt aangewezen.

7 Overdracht taken aan contractpartijen: aanvullende eisen

Het overgrote deel van de elektrotechnische werkzaamheden die bij Rijkswaterstaat uitgevoerd moeten worden, wordt uitbesteed aan externe contractpartijen. Werkverantwoordelijken, vakbekwame personen en voldoend onderrichte personen die deze werkzaamheden uitvoeren zijn in dienst van deze contractpartijen.

Rijkswaterstaat heeft geen werkverantwoordelijken en geen vakbekwame personen in dienst.

Uitzonderingen hierop zijn de T-IV die tevens als werkverantwoordelijken zijn aangewezen voor de bij Rijkswaterstaat in dienst zijnde voldoend onderrichte personen of personeel aan boord van RWS-schepen.

Ook voor de contractpartijen geldt dat conform de NEN 3180:2019 gewerkt moet worden.

Rijkswaterstaat vraagt inzage in de activiteiten die door een externe contractpartij worden verricht, door in het contract te vragen naar een door de opdrachtnemer op te stellen werkplan BEI.

Voor het opstellen van dit werkplan is een handreiking beschikbaar, die als bijlage B aan dit veiligheidshandboek toegevoegd.

7.101 Het aanwijzen van personeel van contractpartijen

Voor het uitvoeren van elektrotechnische werkzaamheden maakt Rijkswaterstaat uitsluitend gebruik van externe installateurs op basis van contracten. De aanwijzing van de werkverantwoordelijke, de vakbekwame personen en de voldoend onderrichte personen zoals die zijn beschreven in de NEN 3840:2019 is een taak van de contractpartij.

Besteedt Rijkswaterstaat werkzaamheden uit aan een contractpartij en is de overdracht van de verantwoordelijkheid niet schriftelijk vastgelegd, dan is de contractpartij toch verantwoordelijk voor het aanwijzen van zijn personeel voor het uitvoeren van de werkzaamheden.

De werkverantwoordelijken en de vakbekwame personen worden door de externe contractpartij aangewezen. Deze contractpartij is er verantwoordelijk voor dat de aangewezen personen aan de criteria voldoen.

Nadat alle criteria zijn getoetst, kan de persoon worden aangewezen. De aanwijzing moet schriftelijk geschieden.

Het is noodzakelijk de argumenten die bij een aanwijzing een rol hebben gespeeld, eveneens schriftelijk vast te leggen.
Het is de verantwoordelijkheid van de directie van de contractpartijen om ervoor te zorgen dat de aanwijzing van haar personeel geheel overeenkomstig dit veiligheidshandboek plaatsvindt.

Rijkswaterstaat vertrouwt erop dat de contractpartij uitsluitend personeel werkzaamheden laat verrichten dat de gevaren van het werken aan elektrische installaties en met elektrische energie kent en dat haar personeel op de juiste wijze is aangewezen en voldoende is geïnstrueerd.

Rijkswaterstaat heeft het recht op volledige inzage in het aanwijzingsbeleid van de contractpartij. Elke aanwijzing door de contractpartij kan door Rijkswaterstaat worden ingezien. Bovendien kan Rijkswaterstaat bezwaar tegen een aanwijzing maken.

Werkverantwoordelijken, vakbekwame personen en voldoend onderrichte personen die bij Rijkswaterstaat elektrotechnische werkzaamheden verrichten, worden door de contractpartij aangewezen voor die werkzaamheden. Personen kunnen ook

uitsluitend worden aangewezen voor werkzaamheden aan bepaalde installaties of installatiedelen.

De aanwijzing van deze personen kan voor verschillende installaties of installatieonderdelen verschillend zijn.

Een persoon kan voor een bepaalde installatie worden aangewezen als vakbekwaam persoon, terwijl hij voor een andere installatie slechts een voldoend onderrichte persoon is. Dit betekent dat de betreffende persoon gelijksoortige werkzaamheden aan de ene installatie wel en aan de andere installatie niet mag uitvoeren.

Indien elektrotechnische werkzaamheden met in- en/of uitleenkrachten plaatsvinden gelden de volgende voorwaarden:

Beide werkgevers moeten sluitende afspraken maken over de aanwijzing van de genoemde personen en hun onderlinge gezagsrelatie.

Werkverantwoordelijken, vakbekwame personen en voldoend onderrichte personen waarmee een gezagsverhouding bestaat en aan wie werkzaamheden zijn opgedragen, zoals bij inlenen en bij uitzendkrachten, door de contractpartij, moeten door de inlener schriftelijk zijn aangewezen.

Met deze twee voorwaarden wordt ingespeeld op de vergaande flexibilisering van de arbeidsovereenkomsten. De bedoeling hiervan is duidelijk. De kwaliteit van de arbeidsovereenkomst mag geen invloed hebben op het aanwijzingsbeleid. Daar waar werkzaamheden worden verricht, moet een eenduidig aanwijzingsbeleid worden gevoerd.

7.102 Het veilig uitvoeren van werkzaamheden

Externe contractpartijen die elektrotechnische werkzaamheden verrichten voor Rijkswaterstaat moeten niet alleen overeenkomstig de NEN 3840:2019 werken, maar moeten zich ook houden aan de huisregels en de veiligheidsvoorschriften die bij Rijkswaterstaat van toepassing zijn.

Ook van het personeel van derden ingezet door een contractpartij moet worden geëist dat het zich houdt aan de eisen, regels en instructies, zoals deze door Rijkswaterstaat zijn opgesteld. Er kunnen disciplinaire maatregelen worden genomen tegen personeel dat zich niet aan de eisen, regels en instructies houdt. Voor personeel van contractpartijen kan dit worden vastgelegd in de aanneemovereenkomst.

Bij de organisatie van het werk moet rekening worden gehouden met de samenstelling van de werkploeg. Op elke werkplek moet een voldoende aantal mensen aanwezig zijn dat nodig is om te werken aan, met of nabij een elektrische installatie.

De externe contractpartij moet controleren dat personeel dat zij naar een karwei stuurt, veilig kan werken in die omgeving waarin het karwei moet worden uitgevoerd. Deze bepaling is niet alleen van belang voor de elektrotechnische gevaren maar voor alle gevaren die bij werkzaamheden kunnen optreden.

In de NEN 3840:2019 staat dat iemand die om veiligheidsredenen bezwaar heeft om een opdracht op te volgen of werkzaamheden uit te voeren, de mogelijkheid moet worden geboden deze bezwaren meteen ter kennis te brengen van de werkverantwoordelijke.

De werkverantwoordelijke moet de situatie onderzoeken en, indien noodzakelijk, een hogere instantie raadplegen om tot een beslissing te komen. Ook in de Arbeidsomstandighedenwet vinden we een dergelijke bepaling.

Het is van belang dat de verantwoordelijkheid voor ieder die bij de werkzaamheden is betrokken vaststaat. Een collegiale gedachtewisseling of een aanvulling van een ter zake deskundig persoon blijft altijd mogelijk. De eindverantwoording blijft echter bij de werkverantwoordelijke liggen.

Voor ieder in de organisatie moet het duidelijk zijn door wie, welke werkzaamheden mogen worden verricht en hoe deze werkzaamheden moeten worden uitgevoerd.

7.103 Bevoegdheden en verantwoordelijkheden van extern personeel

Bij het uitvoeren van werkzaamheden op basis van een overeenkomst is eveneens de verantwoordelijkheid voor een veilige uitvoering van die werkzaamheden overgedragen.

Uitsluitend indien in een contract schriftelijk is vastgelegd dat de verantwoordelijkheid voor de veiligheid bij de werkzaamheden bij Rijkswaterstaat blijft, zal Rijkswaterstaat erop toezien dat de ingehuurde medewerkers capabel zijn.

Rijkswaterstaat is, zonder schriftelijke vastlegging van de verantwoordelijkheden, nimmer verantwoordelijk voor de elektrotechnische veiligheid bij werkzaamheden die worden uitgevoerd door personeel van derden.

De veiligheid van alle werkzaamheden behoort tot de verantwoordelijkheid van de werkverantwoordelijke. De werkverantwoordelijke kan een natuurlijke of een rechtspersoon zijn doch is nagenoeg altijd een persoon die verbonden is met een externe contractpartij.

Voor alle elektrotechnische werkzaamheden wordt de taak van de werkverantwoordelijke opgedragen aan de contractpartij die de werkzaamheden uitvoert.

Bij verdeling van de werkzaamheden kan het noodzakelijk zijn iemand aan te wijzen die verantwoordelijk is voor de veiligheid van elk gedeelte, waarbij het geheel valt onder de verantwoordelijkheid van één coördinerende werkverantwoordelijke.

Doordat Rijkswaterstaat elektrotechnische werkzaamheden uitbesteedt aan externe installateurs zal de werkverantwoordelijke een medewerker van de externe installateur zijn, of van een andere derde, terwijl de installatieverantwoordelijkheid nagenoeg altijd bij een medewerker van Rijkswaterstaat is belegd.

In een dergelijke situatie moeten de verantwoordelijkheden goed vastgelegd worden. Ook moet aandacht besteed worden aan de beheer- en werkprocedures. Tegenstrijdigheden in handelingswijzen tussen beide personen moeten voorkomen worden, een goede samenwerking is noodzakelijk.

Indien een werkverantwoordelijke het noodzakelijk vindt om een elektrische installatie of een gedeelte van de elektrische installatie uit te schakelen om de werkzaamheden veilig uit te voeren, moet hij hiervoor de bevoegdheid hebben.

Deze beslissing mag nimmer door een medewerker van Rijkswaterstaat teniet gedaan worden.

Uiteraard moet overleg plaatsvinden tussen de externe werkverantwoordelijke en de F-IB en/of T-IV van Rijkswaterstaat die de betreffende installatie onder zijn / haar beheer heeft.

Deze verantwoordelijken moeten afstemmen welke werkzaamheden, wanneer moeten worden uitgevoerd en welke veiligheidsmaatregelen noodzakelijk zijn.

Zo kunnen werkzaamheden op een gunstig tijdstip gepland worden, echter steeds gaat de veiligheid boven de continuïteit.

Het is zaak de werkafspraken goed te bespreken en in een register van de contractpartij vast te leggen.

8 Algemene werkvoorschriften en werkprocedures

Om de veiligheid van iedereen die aan of nabij elektrische installaties of aan en met elektrische arbeidsmiddelen werkt te waarborgen, moeten een aantal algemene eisen aan het beheer en de werkzaamheden gesteld worden.

In dit hoofdstuk worden deze eisen besproken. Aan bod komen:

- de algemene veiligheidsmaatregelen
- de werkprocedures
- de werkzaamheden bij risicoverhogende omstandigheden
- het sleutelplan
- de vastlegging of rapportage

8.101 Algemene Veiligheidsmaatregelen

Voor bepaalde handelingen die regelmatig voorkomen is het niet noodzakelijk om elke keer dat ze uitgevoerd worden een risico-inventarisatie en –evaluatie uit te voeren. De NEN 3840:2019 stelt dat voor dergelijke processen standaard bedrijfsvoeringprocedures ontwikkeld mogen worden.

Bedrijfsvoeringprocedures kunnen bijvoorbeeld worden opgesteld bij standaard bedieningshandelingen en bij functionele controles.

Bedieningshandelingen zijn bedoeld om de elektrische toestand van een elektrische installatie te wijzigen. Er bestaan twee soorten bedieningshandelingen:

- Bedieningshandelingen bedoeld om de elektrische toestand van een elektrische installatie te wijzigen, om (elektrisch) materieel te gebruiken, om materieel, dat is ontworpen om zonder risico te worden gebruikt, aan te sluiten of los te nemen, aan of uit te zetten, voor zover dit in de praktijk redelijkerwijs mogelijk is.

- Uitschakeling of inschakelen van installaties in samenhang met de uitvoering van werkzaamheden.

Bedieningshandelingen kunnen ter plaatse of op afstand worden uitgevoerd.

In de bedrijfsvoeringprocedures kan bijvoorbeeld staan dat geschikte gereedschappen moeten worden gebruikt om elektrisch gevaar voor personen te voorkomen.
Het gebruik van de juiste gereedschappen lijkt vanzelfsprekend. In de praktijk wordt regelmatig geïmproviseerd met verkeerd gereedschap. Door dit verkeerde gereedschap kan direct gevaar ontstaan.

Geïmproviseerd elektrisch handgereedschap mag bij Rijkswaterstaat niet toegepast worden, tenzij dit gereedschap goedgekeurd is door de T-IV of de werkverantwoordelijke. Dit geldt ook voor de externe contractpartijen die voor Rijkswaterstaat werkzaamheden uitvoeren.

De elektrische veiligheidsmaatregelen, zoals getroffen voor de oorspronkelijke installatie, moeten ten minste in stand worden gehouden.

De elektrische veiligheidsmaatregelen zoals die getroffen zijn voor de oorspronkelijke installatie, vinden we in de normen, voorschriften, richtlijnen en aansluitvoorwaarden waaraan het ontwerp van de installatie ten grondslag lag.

Dit betekent dat de veiligheidsbepalingen van een elektrische installatie moet voldoen aan de laatste druk van de NEN-EN-IEC 61936,
die van kracht was bij de aanleg van de installatie.

Uiteraard kan de T-IV altijd beslissen dat een hoger veiligheidsniveau nodig is dan strikt noodzakelijk.

Voor installaties of delen van installaties die niet mogen worden gebruikt, omdat ze niet veilig zijn, moet worden voorkomen dat ze onbedoeld in bedrijf kunnen worden genomen.

Aanbevolen wordt ten minste zodanige maatregelen te nemen dat minimaal twee bewuste handelingen moeten worden uitgevoerd alvorens de installatie ingeschakeld kan worden. Daarnaast is altijd een waarschuwingsbord noodzakelijk.

In een ruimte die hoofdzakelijk is bestemd voor het bedrijf van de elektrische installatie mogen alleen voorwerpen aanwezig zijn die dienen voor bedieningswerkzaamheden en elektrotechnische werkzaamheden aan de daar aanwezige elektrische installatie.

8.102 Werkprocedures

Voor alle werkzaamheden moet een plan worden opgesteld. Volgens de uitgangspunten van de NEN 3840:2019 moet de T-IV of de werkverantwoordelijke ervoor zorgen dat vóór de aanvang en bij de voltooiing van de werkzaamheden specifieke en uitvoerige aanwijzingen worden gegeven aan het personeel dat de werkzaamheden uitvoert.

Veel werkzaamheden zullen worden uitgevoerd op grond van een algemeen plan van aanpak dat bij alle betrokkenen bekend is, zonder dat daar specifiek over wordt gesproken of zonder dat een en ander schriftelijk is vastgelegd. Het is uiteraard niet noodzakelijk dat voor deze algemene werkzaamheden steeds een plan van aanpak moet worden opgesteld.

De F-IB en T-IV van Rijkswaterstaat moeten erop kunnen vertrouwen dat de algemene werkzaamheden door voldoende geïnstrueerde personen volgens de gebruikelijke regelen der techniek worden uitgevoerd.

Zowel de F-IB en T-IV van Rijkswaterstaat als de werkverantwoordelijke moeten er steeds van overtuigd zijn dat er altijd veilig zal worden gewerkt. Bij de geringste twijfel zal ten minste mondelinge instructie moeten worden gegeven. Bij gecompliceerde werkzaamheden is een schriftelijke werkinstructie verplicht.

Voor veelvoorkomende werkzaamheden dienen standaardinstructies te worden opgesteld door de opdrachtnemer van bijv. een onderhoudscontract.

Bij Rijkswaterstaat zullen de instructies bij gecompliceerde werkzaamheden verzorgd worden door de werkverantwoordelijke, die in dienst is van de externe contractpartij.

Vóór de aanvang van de werkzaamheden moet de werkverantwoordelijke de T-IV (of F-IB) van Rijkswaterstaat informeren over de aard, de plaats en de gevolgen van de voorgenomen werkzaamheden voor de elektrische installatie. Deze informatie wordt bij voorkeur schriftelijk verstrekt, vooral als de werkzaamheden gecompliceerd zijn.

Alleen de T-IV (of F-IB) van Rijkswaterstaat mag toestemming geven om met de werkzaamheden te beginnen.

Naast procedures die de aanvang van werkzaamheden vastleggen, moeten gelijksoortige procedures worden opgesteld voor het onderbreken en beëindigen van werkzaamheden.

Een korte onderbreking als gevolg van rustpauzes, weersinvloeden e.d., waarbij de werkplek niet wordt verlaten, wordt niet als onderbreking beschouwd.

Bij werkzaamheden wordt onderscheid gemaakt in drie werkmethoden:

- spanningsloos werken
- onder spanning werken (bij Rijkswaterstaat niet toegestaan)
- werken in de nabijheid van actieve delen. (bij Rijkswaterstaat niet toegestaan)

Al deze procedures zijn gebaseerd op het nemen van beschermende maatregelen tegen directe aanraking en/of de gevolgen van kortsluiting en vlambogen.

8.102.1 Spanningsloos werken [Bron NEN 3840 hoofdstuk 6.2]

Deze paragraaf behandelt de essentiële eisen die ervoor moeten zorgen dat de elektrische installatie op de werkplek spanningsloos en veilig is tijdens de duur van de werkzaamheden. Daartoe moet de werkplek duidelijk worden bepaald.

Het garanderen van de veiligheid van de werkplek is een taak van de werkverantwoordelijke. Ze worden in deze paragraaf kort aangehaald, omdat de T-IV van Rijkswaterstaat ook aangewezen kan worden als werkverantwoordelijke voor de eventueel aanwezige VOP-ers in dienst van Rijkswaterstaat.

Nadat de betrokken elektrische installaties zijn bepaald, moeten de volgende vijf essentiële eisen worden aangehouden in de aangegeven volgorde, tenzij er doorslaggevende redenen zijn om daarvan af te wijken:

1) scheiden;
2) beveiligen tegen opnieuw inschakelen;
3) controleren op afwezigheid van bedrijfsspanning;
4) zorgen voor aarding en kortsluiting;
5) zorgen voor bescherming ten opzichte van naastgelegen actieve delen.

De T-IV (of F-IB) van Rijkswaterstaat moet aan de werkverantwoordelijke toestemming geven om met de werkzaamheden te beginnen. Ieder die aan deze werkzaamheden deelneemt, moet voldoende opgeleid zijn of onder toezicht staan conform [NEN 3840]

Uitschakeling vóór of wederinschakeling na spanningsloos werken moet worden uitgevoerd door vakbekwame of voldoend onderrichte personen die op de hoogte zijn van alle mogelijk optredende gevaren.

Bij Rijkswaterstaat mag uitsluitend worden ingeschakeld en uitgeschakeld na goedkeuring door de werkverantwoordelijke, zie ook de werkafspraken die zijn gemaakt door Rijkswaterstaat met een contractpartij in bijv. een onderhoudscontract, prestatiecontracten, DBFM-contracten, etc..

8.102.2 Volledig scheiden [Bron NEN 3840 hoofdstuk 6.2.1]

Het uitgangspunt is dat spanningsloos gewerkt wordt. Om werkzaamheden te kunnen doen moet volledige scheiding worden toegepast, waarbij rekening moet worden gehouden dat er kans is op overslag. (par 6.2 [NEN 3840])

Alle ongeïsoleerde geleiders moeten worden geaard. (par 6.2.4 [NEN 3840])

Het scheiden en aarden van installatiedelen is beschreven in de specificaties van de leveranciers (of van de installateur)

Bescherming tegen naastliggende actieve delen dient te zijn beschreven

8.102.3 Beveiligen tegen wederinschakeling [Bron NEN 3840 hoofdstuk 6.2.2]

Al het schakelmaterieel dat is gebruikt om de elektrische installatie tijdens de werkzaamheden te scheiden, moet zijn beveiligd tegen wederinschakeling, bij voorkeur door vergrendeling van het bedieningsmechanisme. Bij afwezigheid van vergrendelingsmogelijkheden moeten gelijkwaardige, in de praktijk beproefde, maatregelen tegen wederinschakeling worden genomen.

Wanneer voor de bediening van het schakelmaterieel een hulpvoedingsbron is vereist, moet deze voedingsbron buiten bedrijf zijn gesteld.

Onbevoegd ingrijpen hierin moet door middel van opschriften worden verboden. Ook kunnen afsluitbare werkschakelaars worden toegepast.

Een beproefde methode is het aanbrengen van waarschuwingsborden nadat de volledige scheiding tot stand is gebracht. Er zal gezorgd moeten worden dat deze waarschuwingsborden niet onbedoeld worden verwijderd, bijvoorbeeld door een

goede toegangsregeling voor de elektrische bedrijfsruimte waarin met waarschuwingsborden wordt gewerkt en door goede instructies.

Wanneer toestellen voor afstandsbediening worden gebruikt om wederinschakeling te voorkomen, moet worden verhinderd dat deze ter plaatse met de hand worden bediend. Alle voor dit doel gebruikte toestellen voor signalering en vergrendeling moeten betrouwbaar zijn.

8.102.4 **Controleren of de installatie spanningsloos is [Bron NEN 3840 hoofdstuk 6.2.3]**

De spanningsloze toestand moet worden gecontroleerd aan alle polen en fasen van de elektrische installatie op of zo dicht mogelijk bij de werkplek.

8.102.5 **Aarding en kortsluiting [Bron NEN 3840 hoofdstuk 6.2.4]**

Hoogspanningsinstallaties waaraan gewerkt zal gaan worden, moeten altijd geaard en kortgesloten worden wanneer het risico bestaat dat de installatie spanning gaat voeren, bijvoorbeeld:

- bij bovengrondse leidingen die worden gekruist door andere lijnen of die elektrisch worden beïnvloed
- door een noodstroomgenerator.

8.102.6 **Toestemming om met de werkzaamheden te beginnen [Bron NEN 3840 hoofdstuk 6.2.6]**

De toestemming aan het uitvoerende personeel om met de werkzaamheden te beginnen, mag uitsluitend worden gegeven door de werkverantwoordelijke.

8.102.7 **Opnieuw inschakelen na de werkzaamheden [Bron NEN 3840 hoofdstuk 6.2.7]**

Na voltooiing en inspectie van de werkzaamheden moeten personen die niet langer nodig zijn, worden teruggetrokken. Alle bij de werkzaamheden gebruikte gereedschappen, hulpmiddelen en (persoonlijke) beschermingsmiddelen moeten worden verwijderd. Pas dan mag met de procedure worden begonnen om de installatie opnieuw in te schakelen.

Wanneer de werkverantwoordelijke ervan is overtuigd dat de elektrische installatie opnieuw kan worden ingeschakeld, moet aan de T-IV (of F-IB) van Rijkswaterstaat worden medegedeeld dat de werkzaamheden zijn voltooid en de elektrische installatie gereed is voor wederinschakeling.

De T-IV (of F-IB) van Rijkswaterstaat zal daarna de opdracht tot wederinschakeling geven. Zie hierbij ook de werkafspraken die zijn gemaakt door Rijkswaterstaat met een contractpartij in bijv. een onderhoudscontract, prestatiecontracten, DBFM-contracten, etc..

Als de werkzaamheden onderdeel zijn van een prestatiecontracten, DBFM-contracten, etc dan hoeft de opdracht niet specifiek door de T-IV van Rijkswaterstaat gegeven te worden.

In het algemeen zullen de werkverantwoordelijke en de T-IV deze taak overdragen aan de persoon die ter plaatse met de leiding is belast, mits deze in staat is te beoordelen of veilig kan worden ingeschakeld. Van elke vakbekwame persoon mag dit worden verwacht in eenvoudige omstandigheden.
In gecompliceerde situaties zal de werkverantwoordelijke altijd zelf de situatie moeten beoordelen.

Het verdient aanbeveling dat de overdracht schriftelijk wordt vastgelegd. Dat kan ook worden gedaan in algemene werkinstructies die gedurende een langere periode en voor meer werkzaamheden gelden in samenhang met de afspraken voor het uitschakelen.

8.102.8 **Onder spanning werken**

In Nederland is slechts onder zeer uitzonderlijke omstandigheden en na extra procedures en maatregelen onder spanning werken toegestaan.

Bij Rijkswaterstaat is het onder spanning werken niet toegestaan.

8.102.9 **Werken in de nabijheid van niet voldoende geïsoleerde actieve delen [Bron NEN 3840 hoofdstuk 6.2.5]**

Werkzaamheden in de nabijheid van niet voldoende geïsoleerde actieve delen die tijdens de werkzaamheden aangeraakt kunnen worden, worden beschouwd als werkzaamheden onder spanning. Zie hiervoor paragraaf 6.2.5.

8.103 Werkzaamheden bij risicoverhogende omstandigheden

Bij Rijkswaterstaat worden geen werkzaamheden in de hoogspanning aangevangen wanneer risicoverhogende omstandigheden optreden.

8.104 Sleutelplan

De toegang tot alle ruimten waar voor leken een elektrische gevarenbron aanwezig is, moet aan regels zijn gebonden. De wijze van toegangsregeling en -controle behoort tot de verantwoordelijkheid van de T-IV.

De lijst met sleutels (wie heeft welke sleutel wanneer ontvangen) ligt bij de beheerder.

Toegang tot deze ruimte wordt geregeld door de aanwijzing of contract.
Het mogen betreden buiten de aanwijzing of contract valt onder de huisregels van het object. Het beleid voor het betreden ligt bij de F-IB, die voor veel objecten dit heeft gedelegeerd aan de VWM. Hierbij is het aanmelden voor uitvoering van de werkzaamheden en planning een verplichting. De toestemming geven voor het betreden van het object is de verantwoordelijkheid van VWM of in sommige gevallen van de F-IB.

Deuren die toegang geven tot ruimten waarin een elektrische gevarenbron aanwezig is, moeten zijn afgesloten.

Ruimten, waarin een elektrische gevarenbron aanwezig is, zijn ruimten met niet-voldoende geïsoleerde actieve delen. Onder deze ruimten moeten niet alleen elektrotechnische bedrijfsruimten verstaan worden, maar ook schakel-, verdeel- en regelkasten en bijvoorbeeld opstellingsruimten voor accu's ten behoeve van de noodverlichting.

Ruimten waar een elektrische gevarenbron aanwezig is, mogen alleen worden betreden door:

De volgende personen hebben zelfstandig toegang tot elektrische bedrijfsruimten mits zij beschikken over een door of namens de werkgever verstrekte schriftelijke aanwijzing:

a) — T-IV en/of F-IB
b) — de werkverantwoordelijke;
c) — de vakbekwame persoon;
d) — de voldoende onderrichte persoon;
e) — de bedieningsdeskundige.

Elektrische bedrijfsruimten mogen niet worden betreden door leken, tenzij onder toezicht van ten minste een voldoende onderrichte persoon.

Directieleden, of daarmee gelijk te stellen functionarissen, zijn met betrekking tot hun elektrotechnische kennis gelijkgesteld aan leken. Het is raadzaam dat zij zich bij het betreden van ruimten met een elektrische gevarenbron laten vergezellen door een van de onder b) tot en met e) genoemde personen en dat hun aanwijzingen worden opgevolgd. Op grond van de wetgeving mogen werkgevers alle ruimten betreden.

8.105 Rapportage

Voor een goed beheer van de elektrische installaties en de elektrische arbeidsmiddelen is het noodzakelijk om allerlei informatie schriftelijk vast te leggen. Niet alleen de technische informatie van de installaties en arbeidsmiddelen zijn van belang, maar ook risicoanalyses, aanwijzingen, werk- en veiligheidsprocedures, verantwoordelijkheden en resultaten van inspecties.

8.106 Risicoanalyses

De vastlegging van de beoordeling van de elektrische risico's en van de bedrijfsvoering moet worden bewaard zolang deze van belang is voor de heersende veiligheid.

Het is noodzakelijk en verplicht dat de afwegingen van de risico's en de bronnen waarop deze afwegingen zijn gebaseerd (plan van aanpak, bestek, proces-verbaal van oplevering), schriftelijk worden vastgelegd.

Zolang een installatie of een arbeidsmiddel blijft bestaan en zolang er geen nieuwe risicoanalyse is gemaakt, zal de schriftelijke vastlegging bewaard moeten blijven. Nieuwe risicoanalyses zullen worden gemaakt als het gebruik van de installatie is veranderd of als de elektrische arbeidsmiddelen onder andere omstandigheden worden toegepast.

8.107 Verantwoordelijkheid

De overdracht van verantwoordelijkheid voor de veiligheid en het tijdstip waarop deze overdracht heeft plaatsgevonden moeten worden vastgelegd.

De overdracht kan bijvoorbeeld worden vastgelegd in een logboek of worden geregeld via de tijdregistratie.(par 4.4 [NEN 3840]) Alle mededelingen moeten zijn voorzien van de naam van de persoon die de informatie verschaft en de plaats waar deze zich bevindt. Informatie over de overdracht van de werkzaamheden worden schriftelijk gedaan (par 6.1)

8.108 Tekeningen en documenten

Bijgewerkte tekeningen en documenten van de elektrische installatie, die noodzakelijk zijn voor het veilig beheer van de installatie, moeten beschikbaar zijn.

In de norm NEN-EN 60204 wordt gesteld dat de informatie die noodzakelijk is voor installatie, bedrijf en onderhoud van de elektrische uitrusting van machines, moet worden verstrekt in de vorm van tekeningen, schema's, diagrammen, tabellen en gebruiksaanwijzingen. Deze informatie dient direct bij oplevering te worden verstrekt.

In zowel NEN-EN 61936 A1 en C13worden aanvullende eisen gesteld en wordt aangegeven wat in de betreffende documenten ten minste moet worden opgenomen.

De informatie mag ook digitaal beschikbaar zijn.
De informatie moet zijn:

A. Actueel
B. Betrouwbaar
C. Compleet

9 Bepalingen met betrekking tot inspecties, inspectiefrequenties en steekproeven

Binnen Rijkswaterstaat worden inspecties uitsluitend uitgevoerd door medewerkers van derden. De medewerkers die inspecties uitvoeren moeten zich aan de in dit hoofdstuk gestelde regels houden.

Het doel van inspectie is te controleren of een elektrische installatie voldoet aan de technische voorschriften en veiligheidsvoorschriften, zoals omschreven in de normen, die van toepassing zijn op de betreffende installatie.

De inspectie kan een controle van de normale toestand van de installatie inhouden.

Nieuwe elektrische installaties evenals wijzigingen en uitbreidingen van bestaande installaties moeten worden geïnspecteerd voordat deze in bedrijf worden genomen. Daarnaast moet een periodieke controle plaatsvinden om gebreken, die na de eerste ingebruikname zijn ontstaan, te detecteren en te verhelpen.

Het vaststellen van de inspectiefrequentie is een taak van de T-IV. Deze moet ook bepalen of bepaalde onderdelen van de periodieke inspectie met behulp van een steekproef uitgevoerd mogen worden. Is dit het geval dan moet hij/zij ook kiezen welk steekproefmethode toegepast moet worden.

Het inspectie-interval wordt door, afhankelijk van de verantwoordelijkheid of door de prestatie ON of door de T-IV in een onderhoudsconcept onderbouwd en vastgelegd.
Volgens par. 5.3.3.1.202 [NEN3840] moet het inspectie-interval worden bepaald aan de hand van:
— fabrikantgegevens;
— bevindingen van inspecties;
— het gebruik en de algemene toestand van de installatie;
— de gevolgen bij uitval (veiligheidsrisico en bedrijfsrisico).

Het inspecteren zelf wordt uitbesteed aan externe inspectiebureaus. Hiervoor is het wel noodzakelijk dat vaststaat volgens welke normen de installatie en/of de arbeidsmiddelen geïnspecteerd moeten worden.

9.101 Toe te passen normen

Het is de taak van de T-IV van Rijkswaterstaat te bepalen aan welke normen de installatie ten minste moet voldoen. In het algemeen geldt dat de installatie ten minste moet voldoen aan de veiligheidsvoorschriften en normen die van kracht waren op de datum van eerste aanleg van de installatie. De installatie is volgens deze normen ontworpen en geïnstalleerd.

De T-IV kan ook kiezen voor recentere normen die een hogere veiligheid bieden. Dit zal vooral van belang zijn als in de installatie wijzigingen of uitbreidingen zijn aangebracht.

Uitbreidingen of wijzigingen van betekenende omvang mogen niet worden gerealiseerd overeenkomstig de veiligheidsvoorschriften en normen die van kracht waren op de datum van eerste aanleg, maar moeten voldoen aan de veiligheidsvoorschriften en normen die tijdens de uitbreiding of de wijziging van kracht waren.

Soms worden ook recentere normen geëist op grond van gebruiksvergunningen of omdat Rijkswaterstaat en een externe installateur dit zijn overeengekomen.

Huurt Rijkswaterstaat roerend en/of onroerend goed met elektrische voorzieningen dan moeten in de huurovereenkomst afspraken opgenomen worden met betrekking tot het veilig beheer van die elektrische voorzieningen.

In de praktijk zal men ook worden geconfronteerd met een aantal punten die niet binnen het kader van de NEN 3840:2019, en NEN-EN 61936 A1 en C13met betrekking tot het veilig omgaan met de elektrische installatie of een elektrisch arbeidsmiddel vallen, zoals:

- wettelijke voorschriften
- eisen, voorschriften en aanbevelingen van leveranciers

Daarnaast is het mogelijk dat een of meer punten, genoemd in het kader van de veiligheid, ook nog vanuit een ander kader, bijvoorbeeld een economisch of verzekeringstechnisch kader, moeten worden meegewogen.

9.102 De inspectiefrequentie

Elektrische installaties moeten met een passende regelmaat worden geïnspecteerd. Het doel van regelmatige inspecties is gebreken te ontdekken die zich na ingebruikstelling kunnen voordoen en de werking kunnen belemmeren of een mogelijke gevarenbron kunnen veroorzaken.

De inspectie-interval wordt conform par 5.3.3.1.202 [NEN 3840]

bepaald aan de hand van:
— fabrikantgegevens;
— bevindingen van inspecties;
— het gebruik en de algemene toestand van de installatie;
— de gevolgen bij uitval (veiligheidsrisico en bedrijfsrisico).

Verder speelt mee hoe het onderhoud en de instandhouding van de installatie is belegd; of de werkafspraken die zijn gemaakt door Rijkswaterstaat met een contractpartij in bijv. een onderhoudscontract, prestatiecontracten, DBFM-contracten, etc. of door de T-IV in een onderhoudsconcept onderbouwd en vastgelegd.

9.103 De inspectie

De inspectie van een elektrische installatie kan inhouden:

- een visuele controle
- een meting en/of beproeving

Het inspecteren vindt volgens een vaststaande procedure plaats.

Eerst wordt een pre-inspectie geheel volgens NEN 3840:2019 uitgevoerd. Hieruit kan een lijst met gebreken voortkomen.

Naar aanleiding van deze lijst met gebreken worden reparaties uitgevoerd, waarvoor separaat opdrachten moeten worden gegeven.

Daarna volgt een eindinspectie, gevolgd door een verslag en een ondertekende verklaring dat de installatie veilig is.

Deze verklaring wordt pas verstrekt nadat de gebreken zijn verholpen.

Ten behoeve van een gestructureerde en reproduceerbare uitvoering van de visuele controle en de inspectie door meting en/of beproeving wordt aanbevolen gebruik te maken van controlelijsten of meetprotocollen, in welke vorm dan ook.

Inspecties moeten worden uitgevoerd aan de hand van vereiste elektrotechnische tekeningen en specificaties.

Bij geconstateerde gebreken moeten passende herstelmaatregelen getroffen worden.

Gebreken die een onmiddellijk gevaar vormen, moeten zonder uitstel worden hersteld of defecte delen moeten worden uitgeschakeld en beveiligd tegen opnieuw aansluiten.

Rijkswaterstaat zal met de externe inspecteur afspraken maken over de wijze waarop moet worden gehandeld als tijdens het uitvoeren van inspecties defecten

worden geconstateerd die direct gevaarlijk zijn. In geen geval mogen direct gevaarlijke situaties ongewijzigd blijven. Gevaar moet direct worden weggenomen.

Inspecties moeten worden uitgevoerd door vakbekwame personen die ervaring hebben met het inspecteren van gelijksoortige installaties.

Of vakbekwame personen voldoende ervaring hebben om op verantwoorde wijze inspecties uit te voeren moet steeds per situatie beoordeeld worden. Het is daarbij zeker niet voldoende om alleen te letten op opleiding die eventueel wordt bevestigd door een persoonlijk certificaat. Voldoende ervaring moet in de praktijk zijn opgedaan.

Inspecties moeten zodanig worden uitgevoerd dat gevaren worden voorkomen, waarbij, indien nodig, rekening wordt gehouden met beperkingen door de aanwezigheid van ongeïsoleerde onder bedrijfsspanning staande delen van de installatie. De inspectie moet worden uitgevoerd door gebruikmaking van de juiste hulpmiddelen.

Het resultaat van elke inspectie moet schriftelijk of digitaal vastgelegd worden in een inspectierapport.

Het inspectierapport beoogt de registratie van de resultaten van de veiligheidsinspectie van een bestaande hoogspanningsinstallatie, meetstokken en aardgarnituren .

De Meetstokken en aardgarnituren worden door Rijkswaterstaat ter beschikking gesteld, maar de opdrachtnemer dient zich door middel van de benodigde inspecties en metingen te vergewissen van de technische staat van deze hulpmiddelen.

Het inspectierapport is bedoeld voor diegene die verantwoordelijk is voor de veiligheid binnen de gebouwen of terreinen van Rijkswaterstaat waar de installatie zich bevindt of waar de elektrische arbeidsmiddelen worden gebruikt.

Gebruikers en eigenaren van de elektrische installatie of de elektrische arbeidsmiddelen kunnen ook rechten ontlenen aan het rapport.

Het rapport moet worden ondertekend door diegene die de inspectie feitelijk heeft uitgevoerd of onder wiens leiding de inspectie is uitgevoerd.

Bijlagen

A. Hulplijst voor vragen in een RIE bij Rijkswaterstaat

B. Handreiking voor het door de ON op te stellen Werkplan BEI voor een object of regio

Bijlage A Hulplijst voor vragen in een RIE bij Rijkswaterstaat

Met behulp van deze (niet uitputtelijke) vragenlijst kan een RIE worden opgesteld van de opzet en uitvoering van de Bedrijfsvoering Elektrische Installatie

1. Weten alle werknemers op welke wijze ze veilig met de elektrische installaties en de elektrische arbeidsmiddelen moeten werken?
2. Is er voor alle medewerkers een scholingsplan en komt daarbij de elektrotechnische veiligheid ook aan de orde?
3. Worden nieuwe medewerkers systematisch op de hoogte gebracht van de geschreven en ongeschreven regels?
4. Is er een introductieboekje voor nieuwe werknemers?
5. Wordt bij Rijkswaterstaat gewerkt door personen van derden, zoals een installatiebedrijf, schoonmaakbedrijf, een cateraar, een hovenier of een beveiligingsbedrijf?
6. Worden nieuwe personen van derden op dezelfde wijze geïnformeerd als eigen personeel?
7. Zijn er medewerkers bij Rijkswaterstaat die extra aandacht vragen bij een goed veiligheidsbeleid? (Denk bijvoorbeeld aan medewerkers die de Nederlandse taal niet goed beheersen.)
8. Is er een procedure aanwezig voor het melden van gevaarlijke situaties bij Rijkswaterstaat en is deze procedure bij alle medewerkers bekend?
9. Zijn er procedures vastgelegd in geval van calamiteiten zoals brand, spanningsuitval en dergelijke?
10. Wordt direct actie ondernomen als gevaarlijke situaties worden gemeld?
11. Worden de gevaarlijke situaties geïnventariseerd en geëvalueerd?
12. Worden de resultaten van die evaluaties gebruikt bij het beleid in de toekomst?
13. Wordt bij de aanschaf van nieuwe materialen gedacht aan de elektrotechnische gevaren?
14. Wordt bij het verstrekken van een installatieopdracht voldoende nagedacht over de elektrotechnische veiligheid?
15. Weet de inkoopafdeling en weten de toeleveranciers welke materialen voor gebruik binnen Rijkswaterstaat geschikt zijn?
16. Worden apparaten of verlichting regelmatig gehuurd bij verhuurbedrijven en zijn deze dan veilig?
17. Zijn bij Rijkswaterstaat afspraken gemaakt over de wijze waarop storingen aan de elektrische voorzieningen moeten worden opgelost?
18. Worden de juiste elektrotechnische arbeidsmiddelen gebruikt?
19. Worden de elektrotechnische installaties en de arbeidsmiddelen periodiek gecontroleerd?
20. Worden niet goedgekeurde arbeidsmiddelen en defecte delen van elektrische installaties uit bedrijf genomen?

21. Zijn de taken, de verantwoordelijkheden en de bevoegdheden met betrekking tot de elektrotechnische installatie en de elektrische arbeidsmiddelen voor alle medewerkers geregeld?
22. Zijn de elektrotechnische medewerkers van Rijkswaterstaat en haar contractpartijen aangewezen?
23. Hebben de elektrotechnische medewerkers van Rijkswaterstaat en van de contractpartijen voldoende middelen, zoals geld en tijd, om de verantwoordelijkheid met betrekking tot de veiligheid voor elektrotechnische installaties te kunnen dragen?
24. Worden de elektrotechnische medewerkers van Rijkswaterstaat en van de contractpartijen, voldoende in de gelegenheid gesteld hun kennis en vaardigheid op peil te houden en te ontwikkelen?
25. Worden de elektrotechnische medewerkers van Rijkswaterstaat en haar contractpartijen regelmatig beoordeeld over de wijze waarop ze hun verantwoordelijkheid dragen met betrekking tot het veilig werken?

Bijlage B Handreiking voor het door de ON op te stellen Werkplan BEI voor een object of regio

B.1 Doel

Het doel van het **ON-werkplan BEI** is Rijkswaterstaat inzage te geven in de activiteiten die de ON zal uitvoeren ten einde een veilige bedrijfsvoering van de elektrische installatie in te vullen. Bij steeds herhalende werkzaamheden kan met een algemeen plan worden gewerkt. Voor de overige bijzonder werkzaamheden (hoog risico, groot impact op doorstroming, werken onderspanning) kan niet worden volstaan met een algemeen werkplan.

B.2 Voor welk object of regio?

Korte beschrijving van het object of de regio, de functie ervan en van welk netwerk (vaarweg, snelweg of watersysteem) het een onderdeel is en welke installaties er binnen het object of de regio zijn.

Met welke aspecten zal er rekening mee worden gehouden, denk hierbij onder andere aan:

- Beschikbaarheideisen van de functies van een object/regio;
- Doorstroming;
- Veiligheid (ARBO), aanwezige RI&E, TRA, etc;
- Veiligheid (bij bijvoorbeeld een waterkering);
- Beschikbare tijd voor planbaar onderhoud om werkzaamheden te kunnen verrichten;
- Specifieke normen (anders dan de NEN 3840) die gebruikt worden voor de uitvoering van deze werkzaamheden.

Verder dienen er beschrijvingen van bijzondere ruimtes (vochtige ruimte, explosiegevaar, nauwgeleidende ruimtes, etc.) opgenomen te zijn als deze aanwezig zijn. Eventueel kunnen de beschrijvingen vanuit DISK worden overgenomen.

B.3 Algemene normen, richtlijnen en overige documenten

De volgende normen en documenten kunnen worden geraadpleegd voor opzetten van dit werkplan BEI:

- De NEN 3140:2019 (laagspanning);
- De NEN 3840:2019 (hoogspanning);
- Het NEN 3140 Veiligheidshandboek RWS;
- Het NEN 3840 Veiligheidshandboek RWS;
- Overige documenten specifiek in het contract genoemd.

B.4 Inzet van personeel en gereedschappen

Voor de diverse rollen, zoals beschreven in NEN 3840, worden eisen gesteld aan opleiding en/of ervaring.

In dit werkplan BEI moet worden opgenomen:

- de eisen die een ON stelt aan zijn personeel voor invulling van een bepaalde rol. Dit kan een eventueel worden overgenomen uit het kwaliteitshandboek van de eigen organisatie;
- Aangegeven hoe overdracht van werkzaamheden en (geven van veiligheids)instructie is geregeld met eigen personeel, personeel van derden;

- Hoe personeel van derden wordt ingezet (bijvoorbeeld van onder-ON) en welke criteria hiervoor zijn;
- Gebruik van gereedschappen en hulpmiddelen van zowel van ON als van OG die bij een kunstwerkhoren. Denk bij het laatst aan aardgarnituren, meetstokken, etc.

B.5 Invulling van de bedrijfsvoering

Hierin dienen te worden opgenomen:

- Bedieningshandelingen:
  Wie moet er geïnformeerd worden als er geschakeld gaat worden en/of wie beslist of er geschakeld mag worden;
- Meten:
  Volgens welke normen, richtlijnen, aangevuld met fabrikantgegevens van de te gebruiken meetapparatuur;
- Beproeven:
  Volgens welke normen, richtlijnen, aangevuld met fabrikantgegevens van de te gebruiken beproevingsapparatuur;
- Inspectie:
  Herhalingstijd Conform par 5.3.3.1.202 [NEN 3840]
- Opleiding:
  Welke mensen worden waarvoor opgeleid, getraind en wat is de herhaling hierbij.

B.6 Procedures

In de procedures moeten zijn opgenomen hoe spanning wordt afgeschakeld en heringeschakeld, dit geschiedt onder meer met:

- Schakelbrieven:
  Voor het afschakelen en spanningsloos maken van delen van een installatie moet bekend zijn hoe dit moet gebeuren. Dit geldt voor zowel hoog- als laagspanning
- Spanningsloos maken;
- Relatie met NEN 3140 en NEN 3840.

B.7 Rapportages

Van de operationele activiteiten moeten er rapportages worden gemaakt. In deze (ON-werkplan)BEI moet onder andere worden beschreven:

- Wordt er gebruik gemaakt van een onderhoudsmanagement systeem?
- Hoe is er geïnspecteerd?
- Welke meetgereedschappen zijn er gebruikt.

B.8 Escalatiemodel

Hiervoor moet een beschrijving worden gemaakt waarin staat wat er moet gebeuren bij een gevaarlijke (elektrische) situatie (denk daarbij in het bijzonder wie moet er geïnformeerd worden, bijvoorbeeld: telefoonlijst).

B.9 Overzicht van tekeningen en documenten

Er moet een overzicht worden gemaakt welke tekeningen en documenten zijn van toepassing zijn en wat de status van deze documenten is.

Er is in principe een overzicht van tekeningen en documenten die bij de bedrijfsvoering van een object of regio horen beschikbaar. Als de status hiervan niet duidelijk is moet worden aangegeven wat er met de tekeningen en documenten moet gebeuren en/of dat er tekeningen of documenten ontbreken.

B.10 Calamiteiten

Zie B.8 Escalatiemodel.

B.11 Storingswerkzaamheden

Storingswerkzaamheden zijn in het algemeen een onderdeel van het (algemeen) werkplan. Voor de specifieke storingswerkzaamheden (hoog risico, groot impact op doorstroming, werken onderspanning) kan niet worden volstaan met het algemene werkplan en moet worden nagedacht welke maatregelen moeten worden getroffen ten einde deze storingswerkzaamheden veilig te kunnen uitvoeren. Bij gecompliceerde werkzaamheden is een werkplan verplicht….EN toestemming vooraf.

Handleiding Bedrijfsvoering Elektrische Installaties (BEI)

Nummer:	5905
Versienummer standaard:	1.0
Versienummer document:	
Status:	In beheer
Type:	Kader
Inhoudelijk beheerder:	Andre Smits
Verantwoordelijke afdeling:	District Midden
Netwerken:	
Rollen:	
Fase:	
Proceseigenaar:	Proceseigenaar Omgeving- en Assetmanagement
Link om te reageren:	*Link*

Bijlage S Bijlagen Cybersecurity

Bijlage S Cybersecurity Implementatierichtlijn Objecten v2.4.1

Bijlage S1 CMDB IA OT – Informatiebehoefte en presentatie Excel Format v2.0.1 (Deze Excel spreadsheet is toegevoegd bij “Informatie Opdrachtgever).

Rijkswaterstaat
Ministerie van Infrastructuur en Milieu

RWS INFORMATIE

Cybersecurity Implementatierichtlijn Objecten










Datum	17 april 2025
Versie	2.4.1
Status	Definitief

Colofon

Uitgegeven door	CIV/IRN/Security Centre/Security by Design
Auteurs	Turabi Yildirim Mark van Leeuwen Michael Theuerzeit Mieke van Nierop
Datum	17 april 2025
Versie	2.4.1
Status	Definitief

Versiebeheer en wijzigingshistorie

Het beheer van dit document berust bij Rijkswaterstaat CIV/IRN/Security Centre/Security by Design.

2.0	18-04-2021	RWS interne versie CSIR
2.4	23-04-2021	Gestripte versie t.b.v. aanbestedingen
2.4.1	17-04-2025	Verbeterde CSR 16 “Registratie assets in een configuratiemanagement database (CMDB)”

Over Rijkswaterstaat

Rijkswaterstaat is de uitvoeringsorganisatie van het ministerie van Infrastructuur en Waterstaat en werkt dagelijks aan een veilig, leefbaar en bereikbaar Nederland.
We willen leven in een land dat beschermd is tegen overstromingen. Een land waar voldoende groen is, en voldoende en schoon water. En waar we vlot en veilig van A naar B kunnen.
Daarvoor zetten de mensen van Rijkswaterstaat zich dagelijks in. Met ruim 200 jaar kennis van de inrichting van ons land weten ze dat dit meer is dan het technisch uitvoeren van projecten aan weg en water. Het gaat ook om de balans tussen al die belangen: economie, milieu, woongenot.

Rechten en vrijwaring

Rijkswaterstaat is zich bewust van haar verantwoordelijkheid een zo betrouwbaar mogelijke uitgave te verzorgen. Niettemin kan Rijkswaterstaat geen aansprakelijkheid aanvaarden voor eventueel in deze uitgave voorkomende onjuistheden, onvolledigheden of nalatigheden. Rijkswaterstaat aanvaardt ook geen aansprakelijkheid voor enig gebruik van voorliggende uitgave of schade ontstaan door de inhoud van de uitgave of door de toepassing ervan.

Inhoudsopgave

1 Inleiding 4
1.1 Baseline Informatiebeveiliging Overheid (BIO) en de IEC 62443 4
1.2 Cybersecurity Implementatierichtlijn Objecten (CSIR) 6
1.3 Instructie voor praktische toepassing 10
1.4 Inhoud 10
2 Verdiepende maatregelpakketten 12
2.1 Maatregelen fysieke toegangsbeveiliging IA-gerelateerde ruimten 12
2.2 Maatregelen logische toegang 16
2.3 Maatregelen beveiligingsincidenten en incident response plan 19
2.4 Maatregelen netwerkkoppelingen en cryptografie 21
2.4.1 Netwerkkoppelingen 21
2.4.2 Cryptografie 23
2.5 Maatregelen bescherming tegen kwetsbaarheden 24
2.5.1 Anti-malware 24
2.5.2 Hardening 25
2.5.3 Patching 26
2.6 Maatregelen logging en monitoring 28
2.7 Maatregelen bewustwording en training 32
2.7.1 Medewerkers 32
2.7.2 Managers 35
2.8 Maatregelen gecontroleerd wijzigen 37
2.9 Maatregelen beheer en onderhoud 39
2.10 Maatregelen back-ups 42

Bijlage CSR 1 Omgaan met vertrouwelijke informatie en documenten 44
Bijlage CSR 2 Personele toegang 47
Bijlage CSR 3 Architectuur objectnetwerk 48
Bijlage CSR 4 Het veilig koppelen van beheer- en onderhoudsapparatuur aan ICT- en IA-systemen 51
Bijlage CSR 5 Draadloze netwerken 53
Bijlage CSR 6 IoT 54
Bijlage CSR 7 Wachtwoorden 56
Bijlage CSR 8 Patch management 59
Bijlage CSR 9 Hardening 64
Bijlage CSR 10 Logging 66
Bijlage CSR 11 Malware scanning en opschoning middels een USB 68
Bijlage CSR 12 Continuïteitsplan voor energievoorziening 71
Bijlage CSR 13 Handelswijze bij SOC incident melding en verhoogde dreiging 72
Bijlage CSR 14 Incident response 77
Bijlage CSR 15 Recoveryplan 83
Bijlage CSR 16 Registratie assets in een configuratiemanagement database (CMDB) 89
Bijlage CSR 17 Beveiligingshuisregels 138
Bijlage CSR 18 Back-up en recovery 139
Bijlage CSR 19 Intellectueel eigendom 140
Bijlage CSR 20 Camera's en omgang met camerabeelden van de verkeersregistratiesystemen 147
Bijlage CSR 21 Uniform aanleveren van incidentrapportages 148
Bijlage CSR 22 Virtualisatie 150
Bijlage CSR 23 Verwijdering en vernietiging van informatie en apparatuur 151
Bijlage A Begrippenlijst 152
Bijlage B Cybersecurity Dossier / Cybersecurity Beveiligingsplan 154
Bijlage C Best practice voor risico inschatting bij CSIR afwijkingen 155

1 Inleiding

De samenleving verandert snel onder invloed van technologie en digitalisering. Digitalisering is de belangrijkste bron van groei, innovatie en nieuwe bedrijvigheid. In de informatiesamenleving ontstaan nieuwe kansen door de digitalisering. Tegenover de kansen van digitalisering staan bedreigingen op het gebied van cybersecurity. Cybercrime, cyberspionage en cybersabotage kunnen systemen en processen verstoren, met grote gevolgen voor de volksgezondheid, veiligheid en economie. Deze digitale bedreigingen vragen van de partners in vitale sectoren met bijbehorende vitale processen om een gezamenlijke aanpak en inspanning.

De komende jaren kan verdere digitalisering van de productieprocessen verwacht worden en daarmee ook de grotere afhankelijkheid van ICT en Industriële Automatisering (IA) in onze samenleving. Industriële Automatisering omvat de ICS/SCADA systemen en de ICT gerelateerde systemen en onderdelen (hardware en software), waarbij functioneel interactie plaatsvindt met de fysieke omgeving of gebruikers (bijvoorbeeld een brug, onderstation, DRIP, etc.). Industriële Automatisering draagt ook zorg voor het verkrijgen van informatie over de fysieke omgeving (inwinnen) en het beïnvloeden van de fysieke omgeving (bedienen en besturen). Productieprocessen waarvan sommige vitaal zijn stellen eisen aan de betrouwbaarheid en beschikbaarheid en zijn digitaal vaak verbonden met processen van ketenpartners waarmee samengewerkt wordt. Voor een effectieve en efficiënte samenwerking is de beveiliging van de Industriële Automatisering dan ook essentieel.

Industriële Automatisering zorgt er bijvoorbeeld voor dat sluizen en bruggen functioneren, energie en gas worden gedistribueerd, drinkwater wordt gereinigd, afvalwaterzuivering plaatsvindt, treinen op bestemming komen, containers worden vervoerd en liften en overige gebouwbeheersystemen functioneren. De vitale processen van organisaties worden vaak ondersteund door Industriële Automatisering en door de bescherming van Industriële Automatisering worden ook de te beschermen belangen gewaarborgd.

De doelstelling die met dit document wordt nagestreefd is de vitale infrastructuur met Industriële Automatisering cyberweerbaar te maken en te houden door het treffen en onderhouden van een passende set van beheersmaatregelen. De doelgroep voor dit document zijn objecteigenaren, objectbeheerders, assetmanagers, omgevingsmanagers, technisch managers, contractmanagers, architecten, netwerkspecialisten, staf medewerkers, IA adviseurs, IA cybersecurity adviseurs, opdrachtnemers en leveranciers.

1.1 Baseline Informatiebeveiliging Overheid (BIO) en de IEC 62443

De BIO schrijft het basisniveau voor informatiebeveiliging voor binnen de overheid. De BIO biedt één normenkader voor de beveiliging van de Informatievoorziening (IV) van de overheid.
De BIO richt zich vooral op de beveiliging van de Kantoorautomatisering (KA)
en minder op de Industriële Automatisering. Hierbij zijn Procesautomatisering (PA) en Operationele Technologie (OT) synoniemen voor Industriële Automatisering (IA).

Vergelijking Kantoorautomatisering en Industriële Automatisering

Voor de IA zijn aanvullende eisen en maatregelen nodig om de risico's in het IA domein te beheersen. Dit omdat er andere technologie en componenten worden ingezet, de dreigingen en kwetsbaarheden en de life-cycle processen verschillen. Een wezenlijk onderscheid en focuspunt tussen de kantoorautomatisering en procesautomatisering is dat binnen de BIO de focus ligt op de informatie en de vertrouwelijkheid ervan en dat binnen procesautomatisering de focus ligt op de functies van het object of systeem/proces en de betrouwbaarheid ervan. Hiernaast ligt binnen procesautomatisering ook meer focus op safety naast security. Dit verklaart ook de focus op betrouwbaarheid van Industriële Automatisering in termen van de RAMSSHEEP aspecten voor betrouwbaarheid en beschikbaarheid. Een beschikbare object- of systeemfunctie die niet veilig (safety) is, heeft weinig toegevoegde waarde binnen de Industriële Automatisering. Een ander

wezenlijk verschil is dat binnen de BIO betrouwbaarheid gedefinieerd wordt in termen van beschikbaarheid, integriteit en vertrouwelijkheid met focus op informatie (afgekort BIV) en dat binnen procesautomatisering betrouwbaarheid anders wordt gedefinieerd waarbij de focus ligt op de functies van het object en/of het systeem/proces. Zie voor de definities van betrouwbaarheid en beschikbaarheid en het onderscheid hiertussen de begrippenlijst in de bijlagen. Bij Industriële Automatisering hanteert men de begrippen uit de RAMSSHEEP[1] en worden betrouwbaarheid en beschikbaarheid afzonderlijk gedefinieerd. Dit betekent dat de lading en strekking van de BIO eisen en maatregelen niet zondermeer betekenis kunnen hebben in het werkveld van Industriële Automatisering. De binnen de BIO onderkende BBN niveaus met bijbehorende BIV waarden die bedoeld zijn voor een IT/Kantooromgeving bieden dan ook weinig houvast voor de beveiliging van Industriële Automatisering. Een vertaalslag en aanvulling op de eisen en maatregelen is dan ook nodig om de BIO eisen en maatregelen betekenis en toegevoegde waarde te laten hebben voor de Industriële Automatisering.

Vergelijking normenkader BIO en IEC 62443

Voor de beveiliging van Industriële Automatisering zijn standaarden beschikbaar. De Europese standaard hiervoor is de IEC 62443. De IEC 62443 is in feite een verzameling van normen, technische rapporten en gerelateerde informatie voor het beveiligen van Industriële Automatisering. Deze documenten zijn het resultaat van het IEC proces waarbij ANSI/ISA-62443 voorstellen (vanuit de ISA99 werkgroepen) en andere bijdragen (zoals van de WIB) worden ingediend bij landelijke commissies. Aanmerkingen op een indiening worden geëvalueerd door verschillende IEC 62443 normcommissies waarbij de commentaren worden besproken en, als het nodig is, veranderingen worden doorgevoerd. De IEC ontwikkelt wereldwijde normen onder de vlag van de World Standards Cooperation, waar de ISO en ITU lid van zijn.

De BIO is voor de overheid verplicht en is een baseline. De BIO bevat generieke controls/beheersdoelen voor de IT/Kantooromgeving die ook van toepassing kunnen zijn voor Industriële Automatisering. De BIO controls/beheersdoelen moeten echter wel vertaald worden voor toepassing en betekenis binnen de Industriële Automatisering en aangevuld worden met controls/beheersdoelen om de specifieke risico's van de Industriële Automatisering ook te kunnen mitigeren. De IEC 62443 is een standaard voor de beveiliging van Industriële Automatisering maar is niet verplicht en mist naast de BIO ook overige van toepassing zijnde controls/beheersdoelen uit andere wet en regelgeving.

In de praktijk worden vaak de datanetwerken van de Kantoorautomatisering (KA) met die van Industriële Automatisering vervlecht. Een zuivere scheidslijn is dan ook niet meer te trekken tussen de KA en die van de Industriële Automatisering. De Industriële Automatisering wordt ook nog eens vaak vanuit een KA omgeving aangestuurd en/of beheerd en onderhouden waar de BIO verplicht is en waarop aanvullende controls en maatregelen nodig zijn voor de Industriële Automatisering.

Synthese Cybersecurity Implementatierichtlijn Objecten

Gezien het verplichte karakter van de BIO, de vervlechting van de datanetwerken van KA en IA en de vereiste om zowel voor de BIO en de IEC 62443 een management systeem op te zetten en te onderhouden ligt het meer voor de hand om te komen tot een synthese product. De BIO schrijft een Information Security Management Systeem (ISMS) voor en de IEC 62443 heeft het over een Cyber Security Management Systeem (CSMS). De ontwikkeling is dat ook de IEC 62443 het begrip ISMS gaat hanteren in plaats van CSMS. Twee management systemen inrichten en erop nahouden voor een (overheid)organisatie is ondoenlijk en uitgaande van de overheidssituatie dat een overheidsorgaan altijd de kantooromgeving als thuisbasis heeft van waaruit andere activiteiten worden ontplooid, ligt het meer voor de hand om de BIO en het bijbehorende ISMS (eigenlijk het zuivere ISO 27001 framework) als basis te gebruiken voor het management systeem en deze te vullen met de relevante controls en maatregelen uit de IEC 62443 maar ook uit andere bronnen om de risico's binnen het werkveld van IA te kunnen mitigeren.

---

[1] RAMSSHEEP staat voor Reliability, Availability, Maintainability, Safety, Security, Health, Environment, Economics and Politics.

De eerste versie van de Cybersecurity Implementatierichtlijn Objecten van RWS was het product van deze synthese waarbij werd uitgegaan van de Baseline Informatiebeveiliging Rijkdienst 2012 (BIR 2012) als basis en de concept delen van de IEC 62443. Met de komst van de BIO en de definitief geworden delen van de IEC 62443 is de Cybersecurity Implementatie Richtlijn Objecten geactualiseerd en heeft als eerste basis de relevante BIO controls/beheersdoelen die aangevuld zijn met niet overlappende controls en requirements uit de IEC 62443 en overige bronnen. In de volgende paragraaf volgt een beschrijving hoe de synthese van Cybersecurity Implementatierichtlijn Objecten versie 2.0 tot stand is gekomen.

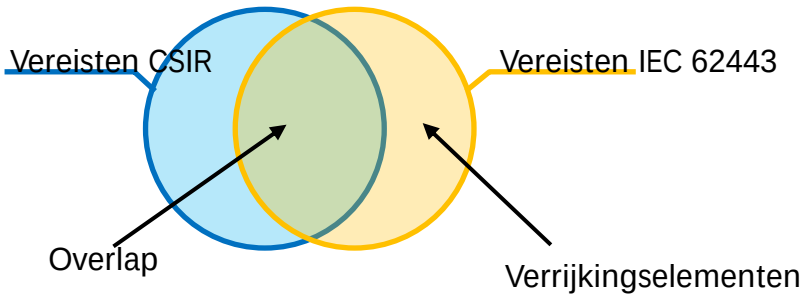
1.2 Cybersecurity Implementatierichtlijn Objecten (CSIR)

Beschrijving CSIR

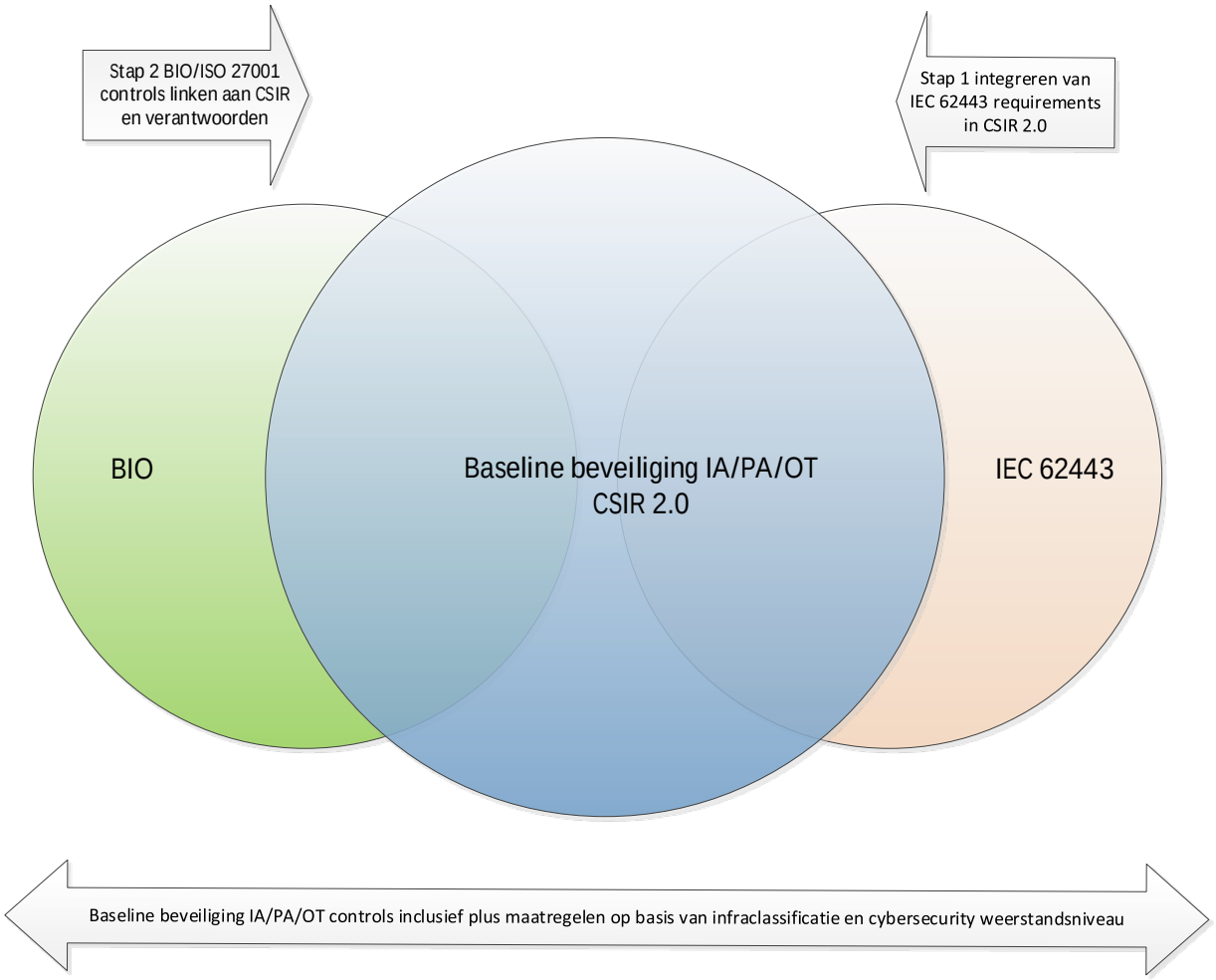
De eerste versie van de Cybersecurity Implementatierichtlijn Objecten is een vertaalslag van de relevante controls/beheersdoelen uit de BIO en de NCSC Checklist beveiliging ICS/SCADA systemen met controls en requirements aanvullingen uit de relevante delen van de IEC 62443 voor de beveiliging van Industriële Automatisering. Waar nodig zijn ook aanvullingen gedaan uit overige best practices voor de beveiliging van Industriële Automatisering. De formulering van de controls/beheersdoelen heeft een operationeel karakter en is daardoor meer geschikt voor toepassing door opdrachtgevers en opdrachtnemers binnen Grond Weg en Waterbouw (GWW) projecten. Ook worden de controls/beheersdoelen geoormerkt of ze een proces of systeemtechnische vereiste betreffen opdat aansluiting wordt gevonden bij het proces van Systems Engineering inclusief de fasering van het V-model voor GWW projecten. Voor het overzicht van de proces- en systeemtechnische controls wordt verwezen naar de vraagspecificatie/contract.

Ontwikkelproces CSIR

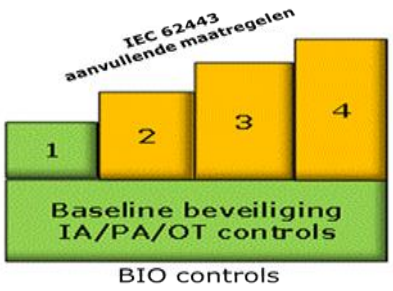
De Cybersecurity Implementatierichtlijn Objecten 2.0 is een doorontwikkeling van de eerste versie van de Cybersecurity Implementatie Richtlijn Objecten RWS. In versie 1.0 van de Cybersecurity Implementatie Richtlijn Objecten waren al de nodige en beschikbare requirements uit de voorlopers van de IEC 62443 delen overgenomen en geïntegreerd. Om naar meer volledigheid en integratie van de recente IEC 62443 requirements te werken is samengewerkt met de Subject Matter Expert (SME) ten aanzien van de IEC 62443 om te toetsen welke requirements nog toegevoegd moest worden ten behoeve van de integratie voor versie 2.0 van de Cybersecurity Implementatierichtlijn Objecten.



De Subject Matter Expert heeft aangegeven welke requirements uit de relevante delen van de IEC 62443 ontbraken in versie 1.0 van de Cybersecurity Implementatie Richtlijn Objecten RWS en dus voor verrijking in aanmerking kwamen inclusief een advies wat de logische plaats was voor integratie. Vervolgens heeft dezelfde Subject Matter Expert geholpen met de daadwerkelijke integratie van de ontbrekende requirements uit de IEC 62443 in versie 2.0 van de Cybersecurity Implementatierichtlijn Objecten (CSIR). Vervolgens zijn de CSIR maatregelen en achterliggende uitwerkingen weer verankerd en geïntegreerd met de relevante BIO controls binnen de structuur van de NEN-ISO-27001 bijlage A.



De BIO is een baseline en de hieruit voor Industriële Automatisering relevante en afgeleide basisset aan controls moet dan ook worden gezien als de baseline controlset voor Industriële Automatisering die altijd van toepassing is. Voor een overzicht van de proces- en systeemtechnische baseline controlset wordt verwezen naar de vraagspecificatie/contract. Deze uit de BIO afgeleide baseline controlset voor IA zal echter niet alle kwetsbaarden en risico's afvangen die zich voordoen binnen de Industriële Automatisering. De kwetsbaarheden en risico's binnen de Industriële Automatisering zijn van een andere aard en orde en vragen om andere en aanvullende controls en maatregelen zoals ook opgenomen in de IEC 62443. De uit de BIO afgeleide basisset aan controls dienen uitgebreid te worden met aanvullende controls binnen de structuur van de NEN-ISO-27001 bijlage A die meer specifiek zijn voor de beveiliging van IA en een minimale plus set met verdiepende maatregelen in relatie tot de baseline IA controls. De minimale plus set aan verdiepende maatregelen in relatie tot de baseline IA controls dient dan ook minstens van het Security Level 1 te zijn zoals voorgeschreven vanuit de IEC 62443. De Baseline beveiliging IA (groene vlak in volgende afbeelding) kan dan ook langs deze weg gedefinieerd worden als de samenvoeging van de baseline beveiliging IA controls die een plus set aan verdiepende maatregelen aanroept die behoort bij het cybersecurity weerstandsniveau 1 zoals beschreven in hoofdstuk 2 van de Cybersecurity Implementatierichtlijn Objecten. De maatregelen die behoren bij cybersecurity weerstandsniveau 1 komen grotendeels overeen met de maatregelen die worden voorgeschreven vanuit de IEC 62443 voor het security level 1.



Om te kunnen bepalen of de Baseline beveiliging IA toereikend is of dat er nog meer aanvullende maatregelen moeten worden getroffen bovenop de baseline beveiliging IA dient altijd een risicoanalyse en afweging gemaakt te worden voor het definiëren van de plus set aan maatregelen boven op de baseline beveiliging IA. Om uitgebreide en complexe risicoanalyses te voorkomen voor het bepalen of de Baseline beveiliging IA maatregelen toereikend zijn of dat er nog meer aanvullende maatregelen nodig zijn, kunnen objecten op een pragmatische manier geclassificeerd worden naar de (ondersteunende) functies die ze vervullen in relatie tot het vitale primaire proces of Infrastructuur van de betreffende organisatie. Hiervoor dient een gangbare Business Impact Analyse (BIA) uitgevoerd te worden.

Bij het classificeren wordt pragmatisch gekeken naar de impact bij het uitvallen van de functie die het object vervult in relatie tot het primaire vitale proces van de organisatie en niet naar de oorzaken van uitval. Aan elke functiebox is een cybersecurity weerstandsniveau gekoppeld. Cybersecurity weerstandsniveau wordt hierbij gedefinieerd als het vermogen om weerstand te bieden tegen aanvallen die bedoeld zijn om zich met geweld of manipulatie toegang fysiek dan wel digitaal te verschaffen tot ruimten en of Industriële Automatiseringssystemen. De maatregelen uit de cybersecurity weerstandsniveaus corresponderen met de maatregelen voor de verschillende security levels zoals beschreven in de IEC 62443. In de functiebox indeling is Box A de hoogste functiebox indeling. Hoe hoger de functiebox indeling hoe weerbaarder een object voor cyberaanvallen moet zijn en dus meer maatregelen nodig zijn.

Toepasselijkheid CSIR

Elk beheerobject moet minimaal uitgevoerd worden met de Baseline beveiliging IA controls en de verdiepende aanvullingen (de plus maatregelen) uit hoofdstuk 2 waarbij cybersecurity weerstandsniveau 1 aangehouden moet worden. De richtlijnen in de bijlagen van de CSIR die ook vanuit de controls uit de vraagspecificatie/contract worden aangeroepen maken tevens onderdeel uit van de Baseline Beveiliging IA. De Baseline beveiliging IA is eigenlijk niet meer dan een bundeling en opstapeling van de controls en maatregelen uit de vraagspecificatie/contract die verdiepende uitwerkingen aanroepen uit hoofdstuk 2 van de CSIR waarbij het aangegeven cybersecurity weerstandsniveau aangehouden moet worden en de aangeroepen richtlijnen in de bijlagen van de CSIR.

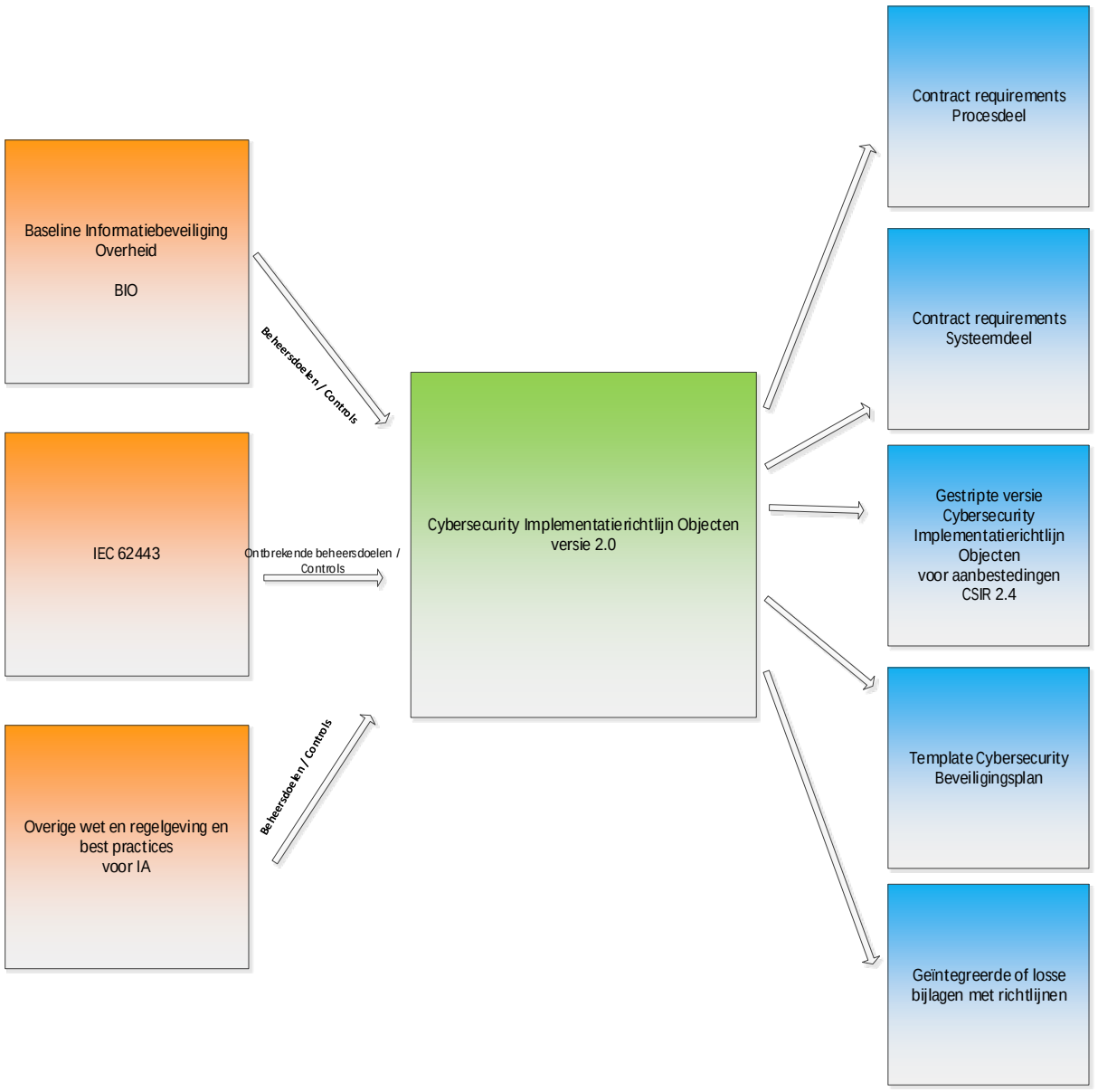
De door de controls aangeroepen verdiepende uitwerkingen uit hoofdstuk 2 van de CSIR zijn maatregel pakketten om de meest voorkomende kwetsbaarheden en risico's binnen de Industriële Automatiseringsomgeving te mitigeren. Bij de keuze voor deze verdiepende set van maatregelen is gebruik gemaakt van internationale onderzoeken naar de meest voorkomende kwetsbaarheden en risico's binnen de Industriële Automatiseringsomgeving en de resultaten van interne onderzoeken. De door de controls aangeroepen verdiepende maatregelen pakketten staan ook in relatie tot de maatregelen van de security levels uit de IEC 62443. De toets door de Subject Matter Expert van de IEC 62443 heeft aangetoond dat de 10 paragrafen uit hoofdstuk 2 van de Cybersecurity Implementatierichtlijn Objecten samen met de controls uit de vraagspecificatie/contract en de richtlijnen in de bijlagen van de CSIR vergelijkbaar zijn met de security requirements uit de IEC 62443 voor de beveiliging van Industriële Automatisering.

Voor het bepalen van de verdiepende set van plus maatregelen uit hoofdstuk 2 is de functiebox indeling van het object nodig waaraan het cybersecurity weerstandsniveau is gekoppeld. Als het object geen functiebox indeling kent omdat er sprake is van losse IA componenten of oplossingen in het veld, dient altijd het cybersecurity weerstandsniveau 1 aangehouden te worden voor de verdiepende plus set aan maatregel uitwerkingen uit hoofdstuk 2 van de CSIR. De maatregelen moeten altijd in relatie staan tot de scope, toepassing en de risico's hierbinnen. Afwijkingen op de controls en maatregel implementatie dienen op basis van een risicoanalyse en afweging conform de uitgangspunten zoals die

ook voor de BIO controls en maatregelen gelden verantwoord en via de explain procedure van de opdrachtgever behandeld te worden. In bijlage C is een best practice opgenomen voor het kunnen maken van risico afwegingen bij (tijdelijke) afwijkingen op de Baseline beveiliging IA controls en maatregelen.

Gebruik CSIR bij aanbestedingen

In geval van aanbestedingen wordt een gestripte versie van de RWS interne versie van de CSIR meegegeven bij aanbestedingen. De controls zoals opgenomen in de RWS interne versie van de CSIR worden vertaald naar proces en systeemtechnische eisen en opgenomen in de vraagspecificatie en of contract. Uit de RWS interne versie van de CSIR wordt het hoofdstuk met proces- en systeemtechnische controls verwijderd waardoor de gestripte versie CSIR 2.4 ontstaat voor aanbestedingen. De verschillende paragrafen uit hoofdstuk 2 en bijlagen van de CSIR 2.4 worden dan vanuit de vraagspecificatie of contract eisen aangeroepen. Zie de schematische weergave hieronder..



1.3 Instructie voor praktische toepassing

Gestreefd moet worden naar een passend niveau van beveiliging voor de objecten en de infrastructuur waar de objecten onderdeel van uitmaken. Daarbij wordt aan een object een specifieke functiebox indeling toegekend. De functiebox indeling correspondeert met een zgn. cybersecurity-weerstandsniveau, conform onderstaande tabel.

Classificatie object in functiebox

Functiebox indeling	Cybersecurity weerstandsniveau
A	4
B	3
C	2
D	1
E	

Voor een object met een weerstandsniveau 4 wordt een zwaarder maatregelenpakket geïmplementeerd dan voor een object met een weerstandsniveau 3. In dit document worden in de 10 paragrafen van hoofdstuk 2 de maatregelen beschreven per cybersecurity weerstandsniveau.

Cybersecurity weerstandsvermogen in ketens: Elke keten is zo sterk als de zwakste schakel. Indien de bediening of het beheer van object A wordt gedaan vanuit een initieel lager geclassificeerd object B, wordt de classificatie van dat object B verhoogd tot het cybersecurity weerstandsniveau van object A.

Als een object nog niet voorzien is van een cyber-classificatie dient er contact gezocht te worden met de beheerder/eigenaar van het object voor het (alsnog) classificeren en indelen van het object in een functiebox.

In het geval dat er helemaal geen sprake is van een echt object in de zin van een civiel technisch werk dan dient voor de beveiliging van de ICT en Industriële Automatisering en datanetwerkcomponenten binnen de eigen infrastructuur het cybersecurity weerstandniveau van 1 te worden aangehouden. Voorbeelden zijn pompkelders of kast ruimten in het areaal met ICT en IA componenten hierbinnen.

Ook kan het voorkomen dat de volledige set van de controls niet altijd van toepassing zijn omdat gewoonweg de risico's zich niet in de scope van de overeengekomen opdracht voordoen. In dat geval dient men risico gestuurd te werken. De opdrachtgever maakt een selectie van de relevante controls en geeft dat in de vraagspecificatie mee. De opdrachtnemer dient altijd uit te gaan van de vraagspecificatie (controls) die bepaalde delen uit hoofdstuk 2 met verdiepingen en overige bijlagen met richtlijnen uit de Cybersecurity Implementatierichtlijn Objecten aanroept waarbij minimaal de maatregelen behorende bij cybersecurity weerstandsniveau 1 aangehouden moet worden voor de invulling. De bijlagen met richtlijnen moeten worden gezien als een best practice uitwerking en hierbinnen is geen onderscheid naar cybersecurity weerstandsniveau.

1.4 Inhoud

Hoofdstuk 1 bevat een inleiding, afleiding en toelichting op de werking van de Cybersecurity Implementatie Richtlijn Objecten.

Hoofstuk 2 met de 10 paragrafen bevat voor elk cybersecurity weerstandsniveau de verdiepende set met maatregelen voor de baseline beveiliging IA controls die onder andere uit de BIO zijn afgeleid. In de maatregelen set van hoofdstuk 2 van de CSIR zijn ook de maatregelen en of requirements uit de IEC 62443 delen als aanvulling en verdieping van de baseline beveiliging IA controls opgenomen. De tien paragrafen met de geclusterde thema's zijn afgeleid uit internationale onderzoeken naar de meest voorkomende kwetsbaarheden en risico's binnen de Industriële Automatiseringsomgeving en in relatie tot de maatregelen voor de security levels zoals voorgeschreven in de IEC 62443. De toets door de Subject Matter Expert met de IEC 62443 heeft aangetoond dat deze 10 paragrafen en thema's van de Cybersecurity Implementatierichtlijn Objecten dekkend zijn voor de IEC 62443 reguirements samen met de ruime uit de BIO afgeleide en vertaalde controls en ondersteunende richtlijnen in de bijlagen van de Cybersecurity Implementatierichtlijn Objecten die aangeroepen worden door de proces of systeem eisen zoals opgenomen in de vraagspecificatie of het contract voor de beveiliging van Industriële Automatisering. Opgemerkt moet worden dat de controls in de vraagspecificatie of contract ruimer kunnen zijn dan de controls die uit de BIO volgen en ook kunnen komen uit andere bronnen die meer specifiek zijn voor de beveiliging van vitale Infrastructuur en processen.

De bijlagen bevatten een aantal verdiepende richtlijnen en of templates/sjablonen waar gevraagde uitwerkingen in moeten worden vastgelegd en onderhouden. Met de templates/sjablonen wordt uniformering en uitwisselbaarheid van de cybersecurity maatregel uitwerking voor de objecten nagestreefd. Dit draagt bij aan uniforme beoordeling en sturing door object (risico) eigenaar, beoordelingen vanuit toezichthouders en de uitwisselbaarheid van cybersecurity uitwerkingen bij overgang van beheer en onderhoud werkzaamheden door andere marktpartijen.

2 Verdiepende maatregelpakketten

In de volgende paragrafen volgen de 10 aanvullende en verdiepende maatregelpakketten voor de controls die naar thema geclusterd zijn en gerelateerd aan de meest voorkomende kwetsbaarheden en risico's uit onder andere internationale onderzoeken binnen het werkveld van de Industriële Automatisering. De proces- en systeemtechnische controls uit de vraagspecificatie/contract roepen verschillende paragrafen uit hoofdstuk 2 van de CSIR aan. De opdrachtgever dient altijd de aan te houden proces- en systeemtechnische controls aan te geven die gevolgd moeten worden bij de uitvoering van het werk. Naast proces- en systeemtechnische controls uit de vraagspecificatie/contract dient ook het cybersecurity weerstandsniveau meegegeven te worden voor de beheerobjecten. Hierbij kan gebruikt gemaakt worden van de volgende vertaaltabel om te bepalen welk cybersecurity weerstandsniveau van toepassing is bij de functieboxen.

Object classificatie in functiebox	Cybersecurity weerstandsniveau
A	4
B	3
C	2
D	1
E	1

2.1 Maatregelen fysieke toegangsbeveiliging IA-gerelateerde ruimten

VRKI-referentie No.	Vereiste	Weerstandsniveau 1	2	3	4
F1	VRKI-referentie: 1	X			
F2	VRKI-referentie: 2		X		
F3	VRKI-referentie: 3			X	
F4	VRKI-referentie: 4				X

Toegangsbeheer No.	Vereiste	Weerstandsniveau 1	2	3	4
F5	Sleutel: Toegang middels een fysieke sleutel (voor normering zie Bouwkundige maatregelen/sluitwerk)	X			
F6	Sleutel: Toegang middels een fysieke sleutel (voor normering zie Bouwkundige maatregelen/sluitwerk)		X		
F7	Rijkspas kantoor: Toegang middels Rijkspas Kantoor installatienormen			X	X

Toegangsproces No.	Vereiste	Weerstandsniveau 1	2	3	4
F8	Lokaal geldende regels en processen zijn van toepassing.	X	X	X	X

Organisatorisch		Weerstandsniveau			
No.	Vereiste	1	2	3	4
F9	O1: Standaard organisatorische maatregelen.	X	X		
F10	O2: Als O1 met daarbij een omschrijving van de specifieke organisatorische maatregelen die zijn toegespitst op het risico-object.			X	X

Bouwkundig		Weerstandsniveau			
No.	Vereiste	1	2	3	4
F11	BK2: Bouwkundige maatregelen met prestatie-eis van 3 minuten inbraakwerendheid.	X	X		
F12	BK3: Bouwkundige maatregelen met prestatie-eis van 5 minuten inbraakwerendheid.			X	
F13	BK4: Bouwkundige maatregelen met prestatie-eis van 10 minuten inbraakwerendheid.				X

Compartimentering		Weerstandsniveau			
No.	Vereiste	1	2	3	4
F14	CO2: Compartimentering met prestatie-eis van 3 minuten inbraakwerendheid.	X	X		
F15	CO3: Compartimentering met prestatie-eis van 5 minuten inbraakwerendheid.			X	
F16	CO4: Compartimentering met prestatie-eis van 10 minuten inbraakwerendheid.				X
F17	ME2: Meeneem beperkende maatregel met prestatie-eis van 3 minuten diefstalvertraging.	X	X		
F18	ME3: Meeneem beperkende maatregel met prestatie-eis van 5 minuten diefstalvertraging.			X	
F19	ME4: Meeneem beperkende maatregel met prestatie-eis van 10 minuten diefstalvertraging.				X

Elektronische maatregelen		Weerstandsniveau			
No.	Vereiste	1	2	3	4
F20	EL2: Grade 2	X	X		
F21	EL3: Grade 2 / Grade 3			X	
F22	EL4: Grade 3 + maatwerk				X

F23	SD1: De schildetectie bestaat uit openstand detectie op nooduitgangen.	X	X		
F24	SD2: Schildetectie bestaat uit detectie, met als doel inbraaksignalering bij de eerste aanval op vaste en beweegbare gevelelementen van of voor, de periferie van ruimten waar de attractieve goederen zich bevinden.			X	
F25	SD3: Schildetectie als bij SD2 met als aanvulling dat (bereikbare) wanden, vloeren en daken zijn voorzien van geschikte detectie.				X

Alarmtransmissie		Weerstandsniveau			
No.	Vereiste	1	2	3	4
F26	AT2: ATS: SP2/DP1; security grade: 2; ontvangst PAC: T2	X	X		
F27	AT3: ATS: DP3; security grade: 3; ontvangst PAC: T4			X	
F28	AT4: ATS: DP4; security grade 3; ontvangst PAC: T5				X

Reactie		Weerstandsniveau			
No.	Vereiste	1	2	3	4
F29	RE1: In deze situatie kan de alarmering door het inbraaksignaleringssysteem gemeld worden naar een (mobiele) telefoon (spraak, tekstbericht) die bereikbaar is. Bij bedrijven is dit een eis. De alarmopvolging kan geschieden door persoonlijke verificatie door de eigenaar of sleutelhouder(s).	X			
F30	RE2: Reactie alarmopvolging: alarmopvolging door sleutelhouder(s) die door de PAC worden gebeld. Bij de PAC moeten minimaal 3 sleutelhouders zijn opgegeven.		X		
F31	RE3: Reactie alarmopvolging: procedure als bij RE2 met de aanvulling dat voor de alarmopvolging een contract moet zijn gesloten met een door het Ministerie van Justitie en Veiligheid toegelaten particuliere beveiligingsorganisatie (geregistreerd middels ND nummer), die onder meer als sleutelhouder kan fungeren. Bij RE3 kan ook worden gekozen voor RE2 + technische alarmverificatie waarmee in plaats van alarmopvolging door een particuliere beveiligingsorganisatie alarmopvolging door een sleutelhouder samen met prioriteit 1 door de politie kan worden bereikt.			X	
F32	RE4: Reactie alarmopvolging: procedure als bij RE3 (dus opvolging door een particuliere beveiligingsorganisatie). Uitgangspunt is opvolgingstijd van maximaal 15 minuten door de particuliere beveiligingsorganisatie en een prioriteit 1 van de politie (15 minuten, na technisch alarmverificatie).				X

N.B.:

1. De in deze paragraaf beschreven fysieke beveiligingsmaatregelen hebben als scope de beveiliging van IA-gerelateerde ruimten. Hieronder wordt verstaan de bedienruimte en technische ruimten binnen de objectpanden. Voor de fysieke beveiliging van het complex/terrein en de hierbinnen gepositioneerde objectpanden dienen de maatregelen aangehouden te worden die volgen uit het locatiebeveiligingsplan. De fysieke beveiligingsmaatregelen uit het locatiebeveiligingsplan omvatten de samenvoeging en dus de opstapeling en integratie van de set van fysieke beveiligingsmaatregelen die volgen uit het Handboek Security RWS en de Cybersecurity Implementatierichtlijn Objecten. Bij constatering van overlap in de samenbundeling en integratie van maatregelen in het locatiebeveiligingsplan wordt de regel aangehouden dat de zwaarste maatregel uit één van de kaders wordt overgenomen. De fysieke beveiligingsmaatregelen uit het locatiebeveiligingsplan dienen vervolgens door het RWS projectteam vertaald te worden naar proces en systeemtechnische vereisten en integraal onderdeel uitmaken van de vraagspecificaties bij aanbestedingen.
2. Gemotiveerd afwijken van de hier genoemde maatregelen kan, bijv. als dat efficiënter is in de integrale aanpak vanuit het locatiebeveiligingsplan, als maar wel aan de bovenliggende weerstandseisen wordt voldaan door de stapeling en integratie van de set van fysieke beveiligingsmaatregelen in het locatiebeveiligingsplan.
3. Bij voorgaande maatregelen m.b.t. de fysieke toegangsbeveiliging van de IA-gerelateerde ruimten is aansluiting gezocht bij VRKI 2020.

2.2 Maatregelen logische toegang

Mens No.	Vereiste	Weerstandsniveau 1	2	3	4
LM11	Voor bewustwording, gedragsregels en training van bedienaars, beheerders en overig ondersteunend personeel (zowel van RWS als die van Opdrachtnemer) wordt verwezen naar paragraaf 2.7 de maatregelen-set “bewustwording en training” van de Cybersecurity Implementatierichtlijn Objecten.	X	X	X	X

Procedures en Organisatie No.	Vereiste	Weerstandsniveau 1	2	3	4
LP1	De Opdrachtgever heeft het recht om controles uit te voeren op de naleving van het logische toegangsproces door de Opdrachtnemer.	X	X	X	X
LP2	Er dient erop toe te worden gezien dat: a. de toegang voor de bedienaars en beheerders tot ICS/SCADA en overige ondersteunende ICT-systemen uitsluitend plaatsvindt, rol gebaseerd en op basis van het ‘need to have’ en 'segregation of duties' principe; b. de toewijzing en het gebruik van privileges van administrators en systeembeheerders beperkt dienen te blijven tot het strikt noodzakelijke; c. fysieke toegang tot objecten en ruimten waar zich informatie, software en andere bedrijfsmiddelen (o.a. apparatuur) bevinden, alsmede de logische toegang tot systemen, uitsluitend wordt toegestaan voor personen die hiertoe geautoriseerd zijn; d. disciplinaire maatregelen worden genomen bij misbruik van accounts en autorisaties.	X	X	X	X
LP3	Er dient erop toe te worden gezien dat: a. de toewijzing en het gebruik van privileges van software en apparatuur beperkt dienen te blijven tot het noodzakelijke, zodat alleen geauthentiseerde apparatuur toegang kan krijgen tot een vertrouwde zone; b. het voor een geautoriseerde gebruiker mogelijk is om privileges te koppelen aan rollen voor alle menselijke gebruikers; c. gebruikersaccounts door een procuratiehouder tijdelijk kunnen worden opgeschort.	X	X	X	X
LP4	De toegangsrechten van alle medewerkers (bedienaars, beheerders en overig ondersteunend personeel) dienen minimaal eenmaal per halfjaar te worden beoordeeld en geactualiseerd in een formeel proces. Opvolging van de bevindingen is gedocumenteerd en wordt behandeld als een beveiligingsincident.	X	X	X	X
LP5	De lokale logische toegang voor medewerkers (op basis van functieprofiel) tot de RWS infrastructuur, ICT, ICS/SCADA systemen en de centrale en lokale objectnetwerken dient bij de hiertoe verantwoordelijk gestelde en gemandateerde lijnmanager te worden aangevraagd en goedgekeurd. Hierbij dient ten minste het volgende te worden gedocumenteerd: details van de accounthouder,	X	X	X	X

	autoriserend manager, permissies behorende bij het account, geautoriseerde apparatuur.				
LP6	Bij remote toegang om beheeractiviteiten uit te voeren dient gebruik te worden gemaakt van de diensten die RWS hiervoor beschikbaar stelt.	X	X	X	X
LP7	Het gebruik van systeemhulpmiddelen die in staat zijn om beheersmaatregelen voor systemen en toepassingen te omzeilen behoort te worden beperkt en nauwkeurig te worden gecontroleerd.	X	X	X	X
LP8	Beheerders, bedienaars en overig ondersteunend personeel wordt ondersteund in het beheren van hun wachtwoorden en krijgen hiertoe de beschikking over een wachtwoordkluis.	X	X	X	X
LP9	Toepassingen, functionaliteit of apparatuur om de toegangseisen te passeren mogen niet worden gebruikt.	X	X	X	X
LP10	Er dient een geborgde procedure te bestaan die de toewijzing en verspreiding van authenticatiemiddelen aan bedienaars, beheerders en overig ondersteunend personeel regelt alsmede het innemen daarvan bij functiewisseling of vertrek (in-, door- en uitstroming). In deze procedure dienen ook de voorgeschreven handelingen bij verlies, diefstal dan wel beschadiging te worden opgenomen.	X	X	X	X
LP11	Accounts dienen op uniforme wijze te worden beheerd.	X	X	X	X
LP12	De toegang voor beheer en onderhoud op afstand door een leverancier wordt alleen voor de geschatte duur van het beheer en onderhoud opengesteld op basis van een wijzigingsverzoek of storingsmelding. De toegang wordt bewaakt en afgesloten bij afmelding van het onderhoud, dan wel automatisch beëindigd na de vooraf ingestelde periode van openstelling.	X	X	X	X
LP13	Systeemhulpmiddelen waarmee beheersmaatregelen kunnen worden omzeild dienen nauwkeurig te worden gecontroleerd en geminimaliseerd, waarbij uitsluitend bevoegd personeel toegang heeft tot deze hulpmiddelen en gebruik wordt gelogd en bewaard voor tenminste 6 maanden.	X	X	X	X
LP14	Het overnemen van sessies op remote werkplekken op een andere werkplek is alleen mogelijk via dezelfde beveiligde loginprocedure als waarmee de sessie is gecreëerd. Uitsluitend mag hiervan worden afgeweken na een expliciete risicoafweging op dit punt.	X	X	X	X

Techniek		Weerstandsniveau			
No.	Vereiste	1	2	3	4
LT1	De logische toegang tot informatiesystemen en netwerk dient plaats te vinden na het succesvol doorlopen van het identificatie, authenticatie en autorisatieproces (IAA), waarbij de IAA-gegevens voor zover haalbaar in versleutelde vorm worden uitgewisseld en opgeslagen.	X	X	X	X

LT2	De toegang tot ICS/SCADA en overige ondersteunende ICT-systemen is geblokkeerd, tenzij het expliciet is toegestaan.	X	X	X	X
LT3	Voor bedienaars, beheerders en systemen worden unieke ID's gehanteerd zodat uitgevoerde handelingen terug te leiden zijn tot een persoon of systeem.	X	X	X	X
LT4	Voor bedienaars, beheerders, software processen en systemen worden unieke ID's gehanteerd zodat uitgevoerde handelingen terug te leiden zijn tot een persoon, software proces of systeem.			X	X
LT5	Het aantal gelijktijdige sessies dat kan worden opgezet door enige gebruiker (mens, software-proces of apparaat) dient te worden beperkt en instelbaar te zijn.	X	X	X	X
LT6	Toegang tot de programmabroncode behoort te worden beperkt.	X	X	X	X
LT7	(Standaard) wachtwoorden moeten door gebruikers bij het in gebruik nemen van de systemen gewijzigd kunnen worden .	X	X	X	X
LT8	Wanneer systemen alleen met generieke accounts kunnen werken, moet dit worden gemotiveerd, vastgelegd en de risico's in beeld gebracht en voorgelegd worden aan Opdrachtgever voor acceptatie van de afwijking om met generieke accounts te mogen werken.	X	X	X	X
LT9	Gedurende het gehele authenticatieproces dient er geen feedback te worden geven over de authenticatie-informatie.	X	X	X	X
LT10	Alvorens aan te melden dient een systeemnotificatie op het scherm te worden weergegeven. Hierin worden restricties omtrent (on)geautoriseerd systeemgebruik aangegeven, evenals logging en monitoring van het systeemgebruik.	X	X	X	X
LT11	Broncode van ontwikkelde programma's dient te worden beschermd en toegang tot de code beperkt.	X	X	X	X
LT12	De logische toegang dient als volgt te worden ingevuld: a. Lokaal bediening – minimaal een user-ID en wachtwoord combinatie; b. Lokaal beheer en administrator accounts – 'two-factor' authenticatie ('bezit' plus 'kennis'); c. Remote toegang voor beheer en onderhoud - 'two-factor' authenticatie en uitsluitend via de centrale beveiligde voorzieningen van RWS-CIV.	X	X		
LT13	De logische toegang dient als volgt te worden ingevuld: a. Lokaal bediening, beheer en administrator accounts – Rijkspas Kantoor/vergelijkbaar elektronisch toegangsbeheersysteem ('bezit' plus 'kennis'); b. Remote toegang voor beheer en onderhoud - 'two-factor' authenticatie en uitsluitend via de centrale beveiligde voorzieningen van RWS/CIV. c. Apparatuur en applicaties dienen bij onderlinge task-to-task communicatie uniek geauthentiseerd te worden middels Mac-adres, en/of IP-adres, device naam, elektronische sleutel, etc.			X	X

LT14	Het gebruik van sterke wachtwoorden dient mogelijk te zijn en net als de vervangingsfrequentie te worden afgedwongen.	X	X	X	X
LT15	Indien 10 keer achter elkaar een foutieve inlogpoging plaatsvindt, dient het account voor een minimale periode van 24 uur te worden geblokkeerd.	X	X	X	X
LT16	Bij het gebruik van een chipcardtoken voor toegang tot systemen wordt bij het verwijderen van het token de toegangsbeveiligingslock automatisch geactiveerd.	X	X	X	X

2.3 Maatregelen beveiligingsincidenten en incident response plan

Mens No.	Vereiste	Weerstandsniveau 1	2	3	4
IM1	Voor bewustwording, gedragsregels en training van bedienaars, beheerders en overig ondersteunend personeel (zowel van RWS als die van Opdrachtnemer) wordt verwezen naar paragraaf 2.7 de maatregelen-set “bewustwording en training” van de Cybersecurity Implementatierichtlijn Objecten.	X	X	X	X

Procedures en Organisatie No.	Vereiste	Weerstandsniveau 1	2	3	4
IP1	Er dient een geborgde procedure te bestaan die regelt dat bedienaars, beheerders en overig ondersteunend personeel (zowel van RWS als die van externe partijen) beveiligingsincidenten en zwakke plekken in de beveiliging zo snel mogelijk melden bij de daartoe ingerichte meldpunten. Van bedienaars, beheerders en overig ondersteunend personeel (zowel van RWS als die van externe partijen) wordt geëist dat zij alle beveiligingsincidenten, verdachte of zwakke plekken in systemen of diensten registreren en rapporteren aan de Objectverantwoordelijke/-beheerder.	X	X	X	X
IP2	Er is een Incident Manager benoemd en bijbehorende verantwoordelijkheden voor Cybersecurity zijn vastgesteld.	X	X	X	X
IP3	Er bestaat een geborgde procedure voor de reactie op en eventuele escalatie van security incidenten. De security incidenten worden vastgelegd, gerapporteerd, gerouteerd, geanalyseerd, gekwantificeerd en afgewikkeld in relatie tot het betrouwbaarheidsniveau en de ernst van het incident. Bepaald wordt welke rolhouders aanspreekbaar zijn inzake storingen, security incidenten en zwakke plekken. De verantwoordelijkheden en incidentenprocedure moeten worden gecommuniceerd naar en worden besproken met de bedienaars, beheerders en overig ondersteunend personeel (zowel van RWS als die van externe partijen).	X	X	X	X
IP4	De Opdrachtnemer draagt zorg voor aansluiting en borging van het eigen incidentmanagementproces op dat van RWS-CIV.	X	X	X	X
IP5	Voor het afhandelen van urgente en niet-standaard security incidenten (bijv. bij computervirusinfecties en aanvallen via	X	X	X	X

	publieke netwerken zoals internet) wordt de Incident Manager van RWS-CIV ingeschakeld.				
IP6	Er dient een operationeel incident response plan te bestaan voor reactie op en afhandeling van incidenten en calamiteiten.	X	X	X	X
IP7	Er dient een operationeel recovery plan te bestaan voor recovery na incidenten of calamiteiten.	X	X	X	X
IP8	Jaarlijks dienen de incident response en recovery te worden beproefd aan de hand van een actueel oefenplan om te bewerkstelligen dat ze doeltreffend blijven. Onderdeel van de jaarlijkse oefening is het testen van de noodbediening.	X	X	X	X
IP9	Tijdens een calamiteit kan het noodzakelijk zijn om het object te evacueren of deuren die toegang bieden tot IA-systemen, te openen voor hulpdiensten. Hierdoor hebben ook kwaadwillenden op dat moment toegang tot de IA-systemen. De bescherming van de vitale delen van het IA-systeem dient gedurende calamiteiten te zijn geborgd middels een procedure.			X	X

Techniek		Weerstandsniveau			
No.	Vereiste	1	2	3	4
IT1	De ingebouwde beveiligingsfuncties, controlemechanismen en waarschuwingen die systemen genereren dienen te worden geactiveerd en benut voor registratie en rapportage van beveiligingsincidenten.	X	X	X	X
IT2	Indien het control systeem niet meer normaal kan functioneren als gevolg van een aanval, dient het control system naar een vooraf gedefinieerde veilige situatie te schakelen (bijvoorbeeld: unpowered, hold of fixed).	X	X	X	X
IT3	Het ICS/SCADA systeem dient na onderbreking of falen terug te kunnen keren naar een bekende veilige staat.	X	X	X	X
IT4	Het ICS/SCADA systeem en de bediening dienen te kunnen schakelen naar en van een noodstroomvoorziening zonder dat dit invloed heeft op de beveiligingsstatus van het object.	X	X	X	X
IT5	In geval van een DOS-aanval dient het ICS/SCADA systeem in een beperkte modus te kunnen functioneren om ten minste de toegang tot de safety systemen te waarborgen.			X	X

2.4 Maatregelen netwerkkoppelingen en cryptografie

2.4.1 Netwerkkoppelingen

Mens No.	Vereiste	Weerstandsniveau 1	2	3	4
NM1	Voor bewustwording, gedragsregels en training van bedienaars, beheerders en overig ondersteunend personeel (zowel van RWS als die van Opdrachtnemer) wordt verwezen naar paragraaf 2.7 de maatregelen-set “bewustwording en training” van de Cybersecurity Implementatierichtlijn Objecten.	X	X	X	X

Procedures en Organisatie No.	Vereiste	Weerstandsniveau 1	2	3	4
NP1	Opdrachtnemer draagt zorg voor en ziet erop toe dat alle datanetwerkverbindingen van het lokale objectnetwerk met het RWS netwerk strikt en uitsluitend plaatsvinden via de beveiligde centrale netwerkvoorzieningen en koppelpunten conform de “Nieuwe Netwerkvoorzieningen Verkeer en Waterstaat - Aansluitvoorwaarden” van Rijkswaterstaat (zal na gunning op verzoek van de Opdrachtnemer beschikbaar worden gesteld). Rechtstreekse (vaste of draadloze) toegang tot het Systeem vanuit andere netwerken dan die van RWS, of vice versa, is strikt verboden.	X	X	X	X
NP2	Opdrachtnemer draagt zorg voor en ziet erop toe dat bij netwerkkoppelingen tussen het object en de centrale netwerken van RWS (NNV/VicNet) de aansluitvoorwaarden van NNV/VicNet in acht worden genomen. Voor remote logische toegang van personeel tot de aan het object gekoppelde systemen moet de procedure “Toegang Derden” van RWS-CIV worden gevolgd waarbij de Objectverantwoordelijke/-beheer de aanvraag verzorgt.	X	X	X	X
NP3	Opdrachtnemer draagt zorg voor en ziet erop toe dat bij renovatie en nieuwbouw van lokale objectdatanetwerken afstemming plaatsvindt met RWS-CIV voor beoordeling en aansluiting van de lokale objectdatanetwerken aan de centrale netwerken, netwerkvoorzieningen, de RWS Netwerkarchitectuur inclusief security.	X	X	X	X
NP4	Opdrachtnemer dient zorg te dragen dat het aantal data netwerkkoppelingen tussen ICS/SCADA systemen en andere datanetwerken beperkt blijft tot alleen de functioneel noodzakelijke, waarbij de koppeling een passende vorm van beveiliging kent en geen onacceptabele risico’s oplevert voor het object en de centrale netwerkdienstverlening. Voor elke koppeling is een risicoanalyse en afweging gemaakt. Streef naar maximale beveiliging en continue monitoring van deze netwerkkoppelingen.	X	X	X	X
NP5	Opdrachtnemer draagt zorg voor en ziet erop toe dat het lokale objectdatanetwerk gehardend is door niet noodzakelijke	X	X	X	X

	netwerkservices uit te zetten (voor hardening zie 'Maatregelen bescherming tegen kwetsbaarheden).				
NP6	Bij afname van netwerkdiensten via providers, of in het geval van samenwerkingsverbanden, dient geëist te worden dat maximale hardening is doorgevoerd op de ingezette netwerk componenten en of apparatuur.	X	X	X	X
NP7	Het koppelen van mobiele apparatuur van derden of removable media aan lokale ICS/SCADA systemen, lokale objectdatanetwerken of het RWS datanetwerk dient uitsluitend plaats te vinden na autorisatie van de hiertoe aangewezen en gemandateerde functionaris aan de kant van Opdrachtnemer.	X	X	X	X
NP8	Gestreefd moet worden naar maximale inzichtelijkheid van de datanetwerkkoppelingen van de objecten. Alle datanetwerkkoppelingen dienen in kaart te worden gebracht, zodat altijd duidelijk is via welk datanetwerkpad een actor (uiteindelijk) een object zou kunnen binnendringen, beginnend vanuit het internet.	X	X	X	X
NP9	Opdrachtnemer draagt zorg voor de beschikbaarheid van de actuele configuratiegegevens van de lokale objectdatanetwerken door middel van een Configuration Management Database (CMDB).	X	X	X	X
NP10	Opdrachtnemer draagt zorg voor een geborgde procedure die aanhaakt op en opvolging geeft aan geregistreerde datanetwerk incidentmeldingen vanuit RWS-CIV.	X	X	X	X

Techniek		Weerstandsniveau			
No.	Vereiste	1	2	3	4
NT1	ICS/SCADA en safety systemen, de ondersteunende systemen en besloten lokale objectnetwerken mogen alleen verbindingen hebben met kantoornetwerken indien deze verlopen via de beveiligde centrale voorzieningen van RWS.	X	X	X	X
NT2	Communicatie en functies van safety systemen zijn afgeschermd van overige communicatie.	X	X	X	X
NT3	De gebruikte communicatiemethoden dienen de integriteit van de gegevensoverdracht te borgen, inclusief fysieke en omgevingsinvloeden op de integriteit van de gegevensoverdracht.	X	X	X	X
NT4	De klokken van alle relevante informatie verwerkende systemen binnen een object behoren te worden gesynchroniseerd met één hiertoe aangewezen centrale referentietijdbron binnen het netwerk van Opdrachtgever.	X	X	X	X
NT5	Een back-up voor de referentietijdbron lokaal dient te zijn ingericht, opdat tijdsynchronisatie kan plaatsvinden in geval dat de centrale referentietijdbron van Opdrachtgever niet beschikbaar is.	X	X	X	X

2.4.2 Cryptografie

Mens No.	Vereiste	Weerstandsniveau 1	2	3	4
CM1	Voor bewustwording, gedragsregels en training van bedienaars, beheerders en overig ondersteunend personeel (zowel van RWS als die van Opdrachtnemer) wordt verwezen naar paragraaf 2.7 de maatregelen-set “bewustwording en training” van de Cybersecurity Implementatierichtlijn Objecten.	X	X	X	X

Procedures en organisatie No.	Vereiste	Weerstandsniveau 1	2	3	4
CP1	De Opdrachtnemer dient bij gebruik van cryptografie uitsluitend PKI-Overheid certificaten in te zetten voor communicatie met (externe) netwerken buiten de RWS infrastructuur. Deze kunnen via Opdrachtgever worden aangevraagd.	X	X	X	X
CP2	De Opdrachtnemer dient bij gebruik van cryptografie uitsluitend PKI-RWS certificaten in te zetten voor communicatie binnen de interne RWS infrastructuur. Deze kunnen via Opdrachtgever worden aangevraagd.	X	X	X	X
CP3	De Opdrachtnemer heeft ten minste de volgende onderwerpen uitgewerkt in het cryptografiebeleid: a. Wanneer wordt cryptografie ingezet; b. Wie is verantwoordelijk voor de implementatie; c. Wie is verantwoordelijk voor het sleutelbeheer; d. Welke normen dienen als basis voor cryptografie en de op welke wijze worden de normen van het Forum Standaardisatie toegepast; e. Op welke wijze wordt het beschermingsniveau vastgesteld; f. Welke procedures gevolg worden voor de communicatie tussen organisaties onderling; g. Het gebruik, bescherming en levensduur van de cryptografische sleutels.	X	X	X	X
CP4	De Opdrachtnemer kiest bij gebruik van cryptografie voor cryptografische toepassingen die voldoen aan passende standaarden en heeft dit gedocumenteerd.	X	X	X	X

Techniek No.	Vereiste	Weerstandsniveau 1	2	3	4
CT1	Bij inzet van versleuteling (cryptografie) dient de gekozen versleuteling en de onderliggende algoritmes en instellingen uitsluitend de duiding “goed” te hebben zoals aangegeven in de meest actuele versie van het NCSC document “Richtlijnen voor Transport Layer Security”.	X	X	X	X
CT2	Indien het configureren van de IA/PA/OT systemen op afstand plaatsvindt, dan dient dit over beveiligde verbindingen plaats te vinden. Inzet van onveilige communicatieprotocollen (FTP, Telnet, VNC en RDP) dient vermeden te worden. Indien het Systeem geen veilig communicatieprotocol ondersteunt dan mag enkel gemotiveerd en na goedkeuring door de Opdrachtgever het	X	X	X	X

	onveilige communicatieprotocol worden ingezet, mits er een additioneel versleuteld kanaal wordt toegepast (SSL, TLS, IPSEC etc.). De gekozen versleuteling en de onderliggende algoritmes en instellingen dienen dan uitsluitend de duiding “goed” te hebben zoals aangegeven in de meest actuele versie van het NCSC document “Richtlijnen voor Transport Layer Security”.				

2.5 Maatregelen bescherming tegen kwetsbaarheden

2.5.1 Anti-malware

Mens		Weerstandsniveau			
No.	Vereiste	1	2	3	4
AM1	Voor bewustwording, gedragsregels en training van bedienaars, beheerders en overig ondersteunend personeel (zowel van RWS als die van Opdrachtnemer) wordt verwezen naar paragraaf 2.7 de maatregelen-set “bewustwording en training” van de Cybersecurity Implementatierichtlijn Objecten.	X	X	X	X

Procedures en Organisatie		Weerstandsniveau			
No.	Vereiste	1	2	3	4
AP1	Opdrachtnemer dient over een geborgde procedure en voorzieningen te beschikken voor detectie van en preventie tegen malware.	X	X	X	X
AP2	Bij anti-virusupdates die vanaf Internet worden gedownload, wordt gecontroleerd dat met de juiste Internetsite contact is gelegd en/of wordt het gebruik van digitale handtekeningen geverifieerd met gebruik van een betrouwbare certificate authority.			X	X
AP3	Opdrachtnemer dient te beschikken over een recoveryplan, waarin zijn opgenomen: alle nodige voorzieningen voor back-up en herstel, kopieën van gegevens en programmatuur, evenals benodigde herstelmaatregelen na een incident zoals b.v. een besmetting met malware.	X	X	X	X
AP4	Voor zover technisch te scannen dienen zowel intern ontworpen, als ingekochte systemen en applicaties, jaarlijks te worden gescand op fouten in code, malware en generieke beveiligingskwetsbaarheden.			X	X
AP5	Opdrachtnemer draagt er aantoonbaar zorg voor (en ziet er op toe) dat gegevensdragers, beheer- en onderhoudsapparatuur gecontroleerd is op en vrij is van malware voordat deze worden gekoppeld aan ICS/SCADA of overige ICT-systemen en lokale objectdatanetwerken.	X	X	X	X

Techniek		Weerstandsniveau			
No.	Vereiste	1	2	3	4
AT1	Antimalware voorzieningen moeten worden ingezet in overeenstemming met RWS-CIV, waarbij de opdrachtnemer,	X	X	X	X

	beheerder dient aan te kunnen tonen dat de antimalware software correct is geïnstalleerd en geconfigureerd. De juiste werking dient hierbij te kunnen worden aangetoond.				
AT2	Antimalware voorzieningen moeten worden ingezet in afstemming met RWS-CIV voor de in- en uitgangen tot de systeemzones. Zoals removable media, firewalls, unidirectional gateways, web servers, proxy servers en remote-access servers.			X	X
AT3	Updates van de signatures, anti-malwaresoftware en bijbehorende herstelsoftware dienen dagelijks plaats te vinden.	X	X	X	X
AT4	De anti-malware voorzieningen mogen geen invloed hebben op de werking en functionaliteit van in gebruik zijnde ICS/SCADA en ICT-systemen.	X	X	X	X

2.5.2 Hardening

Mens		Weerstandsniveau			
No.	Vereiste	1	2	3	4
HM1	Voor bewustwording, gedragsregels en training van bedienaars, beheerders en overig ondersteunend personeel (zowel van RWS als die van Opdrachtnemer) wordt verwezen naar paragraaf 2.7 de maatregelen-set “bewustwording en training” van de Cybersecurity Implementatierichtlijn Objecten.	X	X	X	X

Procedures en Organisatie		Weerstandsniveau			
No.	Vereiste	1	2	3	4
HP1	Opdrachtnemer dient over een geborgde procedure te beschikken voor het (laten) hardenen van ICS/SCADA en overige ondersteunde ICT-systemen en datanetwerkelementen.	X	X	X	X
HP2	Hardware, software en netwerkapparatuur dienen op basis van een analyse veilig geconfigureerd te worden waarbij gebruik wordt gemaakt “good practice security baselines”.	X	X	X	X
HP3	Opdrachtnemer dient aan te tonen welke hardening-methoden zijn gebruikt en hoe deze zijn toegepast.	X	X	X	X
HP4	Het weer inschakelen van uitgezette services en/of protocollen mag alleen door geautoriseerd personeel worden uitgevoerd.	X	X	X	X

Techniek		Weerstandsniveau			
No.	Vereiste	1	2	3	4
HT1	Indien mogelijk dienen ICS/SCADA-systemen zodanig te worden (her)geconfigureerd dat auto-run van USB-tokens, USB harde schijven, mounted network shares of andere removable media niet is toegestaan. Ook dient het gebruik van mobiele code beperkt te	X	X		

	worden, waarbij het uitvoeren van mobiele code niet is toegestaan, tenzij: a. de afkomst van de mobiele code op voldoende wijze is geauthentiseerd en geautoriseerd; b. het versturen van mobiele code naar/van de ICS/SCADA systemen is geblokkeerd.				
HT2	Indien mogelijk dienen ICS/SCADA-systemen zodanig (her)geconfigureerd te worden dat auto-run van USB-tokens, USB harde schijven, mounted network shares of andere removable media niet wordt toegestaan. Ook dient het gebruik van mobiele code beperkt te worden, waarbij het uitvoeren van mobiele code niet is toegestaan, tenzij: a. de afkomst van de mobiele code op voldoende wijze is geauthentiseerd en geautoriseerd; b. het versturen van mobiele code naar/van de ICS/SCADA systemen is geblokkeerd; c. het gebruik van mobiele code wordt gemonitord; d. voor gebruik een integriteitscheck op de mobiele code wordt uitgevoerd.			X	X
HT3	Gedeeld geheugen (b.v. RAM) dient te worden leeggemaakt voordat het gedeeld geheugen wordt vrijgegeven voor andere gebruikers.			X	X
HT4	Minimale hardening maatregelen zijn: a. niet noodzakelijke datanetwerkservices uit te zetten; b. het verwijderen (patchen) van bekende kwetsbaarheden; c. alle poorten die niet nodig zijn te deactiveren/blokkeren; d. alle default “access points” te verwijderen; e. de default accounts uit te schakelen conform het wachtwoord policy; f. indien beschikbaar gebruik te maken van de security opties van leveranciers.	X	X	X	X
HT5	Het weer functioneel kunnen aanzetten van uitgeschakelde services en/of protocollen moet mogelijk blijven.	X	X	X	X

2.5.3 Patching

Mens No.	Vereiste	Weerstandsniveau 1	2	3	4
PM1	Voor bewustwording, gedragsregels en training van bedienaars, beheerders en overig ondersteunend personeel (zowel van RWS als die van Opdrachtnemer) wordt verwezen naar paragraaf 2.7 de maatregelen-set “bewustwording en training” van de Cybersecurity Implementatierichtlijn Objecten.	X	X	X	X

Procedures en Organisatie No.	Vereiste	Weerstandsniveau 1	2	3	4
PP1	Opdrachtnemer dient zorg te dragen dat zijn ICT-systemen (die gekoppeld worden aan de ICT en IA van Opdrachtgever) voorzien	X	X	X	X

	zijn van alle recente beveiligingsupdates en patches. Patches mogen het niveau van systeem hardening niet aantasten.				
PP2	Bij patches die vanaf Internet worden gedownload, wordt gecontroleerd dat met de juiste Internetsite contact is gelegd en/of wordt het gebruik van digitale handtekeningen geverifieerd met gebruik van een betrouwbare certificate authority.	X	X	X	X
PP3	Indien patches om bepaalde redenen bewust niet worden uitgevoerd, dient de afweging hiertoe schriftelijk te worden vastgelegd voorzien van een risicoafweging, inclusief een mitigatievoorstel.	X	X	X	X
PP4	Opdrachtnemer dient over een geborgde procedure te beschikken waarmee tijdig gereageerd kan worden op technische kwetsbaarheden van de in gebruik zijnde ICS/SCADA en ondersteunende ICT-systemen en netwerken.	X	X	X	X
PP5	Opdrachtnemer dient over een geborgde procedure voor patching te beschikken waarin taken, bevoegdheden en verantwoordelijkheden van de betrokken rolhouders zijn beschreven inclusief de van toepassing zijn doorlooptijden en procuratiehouders.	X	X	X	X
PP6	Indien zowel de kans op misbruik als de verwachte schade hoog zijn (volgens de NCSC-classificatie voor kwetsbaarheidswaarschuwingen), wordt de betreffende patch in overleg met Opdrachtgever ingepland voor implementatie. In de tussentijd worden op basis van een expliciete risicoafweging tijdelijke mitigerende maatregelen getroffen.	X	X	X	X

Techniek		Weerstandsniveau			
No.	Vereiste	1	2	3	4
PT1	Het uitvoeren van securityfuncties (b.v. netwerkscans, patching) mag de beschikbare systeemresources niet zodanig beperken dat de normale softwareprocessen op de ICS/SCADA systemen hiervan zichtbaar hinder ondervinden.			X	X

2.6 Maatregelen logging en monitoring

Mens No.	Vereiste	Weerstandsniveau 1	2	3	4
MM1	Voor bewustwording, gedragsregels en training van bedienaars, beheerders en overig ondersteunend personeel (zowel van RWS als die van Opdrachtnemer) wordt verwezen naar paragraaf 2.7 de maatregelen-set “bewustwording en training” van de Cybersecurity Implementatierichtlijn Objecten.	X	X	X	X

Procedures en Organisatie No.	Vereiste	Weerstandsniveau 1	2	3	4
MP1	Opdrachtnemer draagt zorg voor en ziet er op toe dat: a. de loggegevens worden weggeschreven en opgeslagen in een apart bestand, dat alleen toegankelijk is voor speciaal hiertoe geautoriseerd personeel; b. de logbestanden van ICS/SCADA, beveiliging en ondersteunende ICT-systemen en –netwerkelementen worden beschermd tegen verlies of wijziging; c. op basis van een expliciete risicoafweging de bewaarperiode van de logbestanden (van alle systemen met logvoorziening) wordt bepaald. Deze bewaartermijn is altijd tenminste drie maanden; d. loggegevens die zijn gebruikt voor incidentonderzoeken, langer worden bewaard conform de bewaartermijnen die de (feiten)onderzoekers aangeven; e. er een overzicht is van alle logbestanden die worden gegenereerd; f. een (onafhankelijke) interne audit procedure ten minste elke 6 maanden toetst op het ongewijzigd bestaan van de logbestanden g. het oneigenlijk wijzigen, verwijderen of pogingen daartoe van loggegevens, zo snel mogelijk wordt gemeld als beveiligingsincident via de procedure voor beveiligingsincidenten.	X	X	X	X
MP2	De RWS Objectverantwoordelijke/-beheerder dient expliciet toestemming te verlenen voor de levering van logbestanden aan derden.	X	X	X	X
MP3	Opdrachtnemer heeft de afhankelijkheid van de geautomatiseerde gegevensoverdrachten tussen het ICS/SCADA en de gekoppelde ICT-componenten in kaart gebracht. Een geborgde procedure is aanwezig om te bewaken dat alle benodigde gegevens op tijd worden overgedragen en dat hierin geen fouten ontstaan.			X	X
MP4	Camerabeelden van verkeersregistratiesystemen dienen gelogd en gemonitord te worden.	X	X	X	X
MP5	De Opdrachtnemer dient zijn medewerking te verlenen voor het kunnen analyseren van het netwerkverkeer van en naar het object	X	X	X	X

	en binnen het lokale object netwerk door het Security Operations Centre (SOC) van Opdrachtgever.				
MP6	De Opdrachtnemer dient een analyse poort binnen de netwerkinfrastructuur van het object in te richten en beschikbaar te houden voor sensoren die door Opdrachtgever gekoppeld moeten kunnen worden aan deze analyse poort.	X	X	X	X
MP7	De Opdrachtnemer dient het ontwerp voor de inrichting van de analyse poort en de fysieke plaatsing van de sensor voor afstemming en acceptatie voor te leggen aan het RWS CIV IRN Netwerkteam/SOC van Opdrachtgever.	X	X	X	X
MP8	De opdrachtnemer dient voor de goede werking van de analyse poort (beheer-)documentatie op te stellen en te onderhouden.	X	X	X	X
MP9	De Opdrachtnemer dient indien het object niet permanent op het Security Operations Centre is aangesloten zijn medewerking te verlenen voor het incidenteel kunnen uitlezen van het lokale object netwerkverkeer of een specifiek deelnetwerk van het object middels de analyse poorten.	X	X	X	X
MP10	De Opdrachtnemer dient over een operationeel proces te beschikken als onderdeel van het incidentmanagementproces voor het melden van incidenten aan, en de response op meldingen van, het SOC van Opdrachtgever.	X	X	X	X
MP11	De Opdrachtnemer dient over een operationeel proces te beschikken voor de registratie en rapportage van netwerk storingen binnen het lokale objectnetwerk aan de Opdrachtgever.	X	X	X	X
MP12	De opdrachtnemer dient voor het ontwerp en inrichting van de analysepoort en de fysieke plaatsing van de sensor binnen (bestaande) lokale objectnetwerken gebruik te maken van de door Opdrachtgever voorgeschreven netwerkproducten en -diensten.	X	X	X	X
MP13	De Opdrachtnemer dient ontdekte nieuwe dreigingen te delen met Opdrachtgever.	X	X	X	X

Techniek		Weerstandsniveau			
No.	Vereiste	1	2	3	4
MT1	De handelingen van medewerkers, beheerders, operators, meldingen vanuit systemen en eventlogs dienen te worden vastgelegd in audit-logbestanden.	X	X	X	X
MT2	Ongeautoriseerde pogingen tot wijzigingen in software en opgeslagen gegevens dienen te worden gedetecteerd, gerapporteerd en voorkomen.	X	X		
MT3	Ongeautoriseerde pogingen tot wijzigingen in software en opgeslagen gegevens dienen automatisch te worden gedetecteerd, gerapporteerd en voorkomen.			X	X

MT4	Logregels bevatten minimaal de volgende gegevens: a. de gebeurtenis zelf; b. Benodigde informatie om de actie te kunnen herleiden tot een natuurlijk persoon, b.v. gebruikersnaam of een (systeem)-ID; c. component waarop de handeling werd uitgevoerd; d. het resultaat van de handeling; e. de datum en het tijdstip van de gebeurtenis; f. een doorlopende en unieke nummering per logregel.	X	X	X	X
MT5	Logfiles van ICS/SCADA, beveiliging en ondersteunende ICT-systemen en ICT-netwerkelementen dienen in CSV-formaat opgeleverd te worden.	X	X	X	X
MT6	In een logregel worden in geen geval gevoelige gegevens opgenomen. Dit betreft onder meer gegevens waarmee de beveiliging doorbroken kan worden zoals wachtwoorden, inbelnummers, e.d.	X	X	X	X
MT7	Het overschrijven of verwijderen van logregels en logbestanden wordt gelogd in een nieuw aangelegde log.	X	X	X	X
MT8	De loginstellingen en logbestanden worden zodanig beschermd dat deze niet benaderd, gewijzigd of gewist kunnen worden door ongeautoriseerden.	X	X	X	X
MT9	Voor kritieke ICS/SCADA en overige ondersteunende ICT-systemen moeten beveiligingsspecifieke logsystemen worden ingezet, in afstemming met (en op verzoek van) Opdrachtgever.			X	X
MT10	Indien er fouten optreden tijdens het verwerken van de loggegevens, dient er een waarschuwing te worden gegeven.	X	X	X	X
MT11	Werking van de logging van security-gerelateerde events dient door Opdrachtnemer aantoonbaar te worden gemaakt door middel van een door RWS goedgekeurd gesimuleerd security-gerelateerd event.			X	X
MT12	De robuustheid van de logging (bij grote aantallen gelijktijdig optredende gebeurtenissen) dient te worden aangetoond en beschreven door Opdrachtnemer.			X	X
MT13	Er dient voldoende ruimte te zijn voor audit opslag (logging), en maatregelen zijn genomen die de kans beperken dat de beschikbare ruimte overschreden wordt. Er dient tijdig een waarschuwing te worden gegeven indien de opslagcapaciteit op dreigt te raken.			X	X
MT14	Het object datanetwerk dient uitgevoerd te zijn met analysepoorten waarbij datanetwerk ontwerp van het object met eventuele onderkende deeldatanetwerken leidend is voor het aantal in te richten analysepoorten op de datanetwerken. Eén poort op het datanetwerk dient dan geconfigureerd te zijn als analysepoort.	X	X	X	X
MT15	Het object datanetwerk dient uitgevoerd te zijn met een datanetwerk ontwerp en inrichting, zodanig dat een volledige kopie via de analysepoorten van al het bedien en besturingslaag netwerkverkeer (bijvoorbeeld de SCADA en PLC systemen)	X	X	X	X

	uitgelezen en opgebouwd kan worden, dat over het objectdatanetwerk met eventuele onderkende deeldatanetwerken gaat en kan worden aangeleverd voor analyse doeleinden.				
MT16	Het object dient zodanig uitgevoerd te zijn dat de sensor van Opdrachtgever fysiek geplaatst kan worden binnen het lokale datanetwerk en de hiertoe voorziene technische ruimte en of kast. Voor de specificaties van de sensor dient Opdrachtnemer contact en afstemming te zoeken met Opdrachtgever.	X	X	X	X
MT17	Het object dient zodanig ingericht en beschikbaar te zijn dat de permanente of incidentele analyse van het lokale datanetwerk verkeer of een specifiek deeldatanetwerk van het object door Opdrachtgever via de analyse poorten moet kunnen plaatsvinden.	X	X	X	X
MT18	De inrichting van de analyse poort en de fysieke plaatsing van de sensor binnen bestaande lokale objectdatanetwerken dient uitgevoerd te worden met de door Opdrachtgever voorgeschreven datanetwerkproducten en -diensten.	X	X	X	X
MT19	Alle relevante informatie-verwerkende systemen en de daarbij behorende logging systemen dienen te worden gesynchroniseerd met één referentietijdbron, waarvan de integriteit is gevalideerd.	X	X	X	X

2.7 Maatregelen bewustwording en training

2.7.1 Medewerkers

Medewerker No.	Vereiste	Weerstandsniveau 1	2	3	4
TMe1	Bedienaars, beheerders en overig ondersteunend personeel zijn verplicht om de door het management aangegeven en beschikbaar gestelde periodieke Cybersecurity bewustwording en awareness cursussen, trainingen, E-Learning modulen te volgen en hiernaar te handelen. De bewustwording en awareness trainingen besteden ook aandacht aan Sociaal Engineering.	X	X	X	X
TMe2	Iedere opdrachtnemer, bedienaar, beheerder en overig ondersteunend personeel is zich bewust van de voor hem/haar van toepassing zijnde taken, bevoegdheden en verantwoordelijkheden voor beveiliging en weet dat gebruikers- en systeemactiviteiten worden gelogd.	X	X	X	X
TMe3	Opdrachtnemer, bedienaars, beheerders en overig ondersteunend personeel nemen de Cybersecurity beveiligingsinstructies strikt in acht en zijn verantwoordelijk voor hun aandeel in de beveiliging van het object.	X	X	X	X
TMe4	Opdrachtnemer, bedienaars, beheerders en overig ondersteunend personeel doen aan sociale controle, spreken elkaar aan op ontoelaatbaar en risicovol gedrag en bespreken geconstateerde onregelmatigheden in het periodieke werkoverleg met het eigen management/Objectbeheerder.	X	X	X	X
TMe5	Bij het constateren van een security incident dienen Opdrachtnemer, bedienaar, beheerder en overig ondersteunend personeel dit direct als een security incident te melden bij de verantwoordelijke objecteigenaar/ -beheerder. Er is sprake van een security incident bij het manifest worden van een (dreigend of reeds opgetreden) security risico als gevolg van een (mogelijke) overtreding van het Cybersecurity beleid of onregelmatigheid. Voorbeelden van security incidenten zijn: a. Uitval van diensten, apparatuur of voorzieningen, systeemstoringen of overbelasting als gevolg van cybersecurity inbreuken; b. menselijke fouten die leiden tot functionele verstoring of uitval van systemen; c. inbreuk op fysieke en logische beveiligingsvoorzieningen van het object; d. hack pogingen via de infrastructuur van opdrachtnemer en/of zijn netwerkproviders tot het netwerkdomein van opdrachtgever; e. inbreuk op de bediening en beheer; f. ongeautoriseerde systeemwijzingen; g. niet-naleving van beleid of gedragsregels; h. detectie van malware bij ad hoc controles/scans; i. virusmeldingen vanuit operationele antimalwarevoorzieningen; j. verlies of diefstal van ICT en IA bedrijfsmiddelen; k. oneigenlijk gebruik van bevoegdheden;	X	X	X	X

	l. vandalisme, moedwillige beschadiging.				
TMe6	Afwijkend systeemgedrag kan een aanwijzing zijn voor een aanval op de beveiliging of voor een daadwerkelijk beveiligingslek en behoort daarom altijd direct te worden gerapporteerd als een beveiligingsincident en gemeld aan de Objectverantwoordelijke/-beheerder.	X	X	X	X
TMe7	Opdrachtnemer, Bedienaars, beheerders en overig ondersteunend personeel moeten bij het constateren van eventuele onregelmatigheden of onveilige situaties als gevolg van cybersecurity inbreuken, die handelingen verrichten of maatregelen treffen die verdere uitbreiding van het incident kunnen voorkomen, dan wel de schade beperken.	X	X	X	X
TMe8	Bedienaars, beheerders en overig ondersteunend personeel gaan zorgvuldig om met de verstrekte persoonsgebonden fysieke toegangsmiddelen voor het object en de (systeem, bedien, technische) ruimten hierbinnen en delen deze niet met collega's.	X	X	X	X
TMe9	Opdrachtnemer, bedienaars, beheerders en overig ondersteunend personeel creëren geen eigen netwerkkoppelingen op het object en melden dit als een beveiligingsincident als er een zelf aangelegde netwerkkoppeling wordt geconstateerd.	X	X	X	X
TMe10	Opdrachtnemer, bedienaars, beheerders en overig ondersteunend personeel nemen de regels in acht voor de logische toegang tot ICS/SCADA en overige ondersteunende ICT-systemen.	X	X	X	X
TMe11	Opdrachtnemer, bedienaars, beheerders en overig ondersteunend personeel koppelen geen mobiele apparatuur of removable media aan de ICS/SCADA omgeving, overige ondersteunende ICT-systemen en object netwerken. Uitgezonderd hiervan zijn de beheerders die dit alleen na autorisatie van de hiertoe gemandateerde functionaris en uitgevoerde actuele malwarecontrole van apparatuur/media mogen doen.	X	X	X	X
TMe12	Voor Opdrachtnemer, bedienaars, beheerders en overig ondersteunend personeel is toegang tot internet en het gebruik van email vanaf ICS/SCADA en overige daaraan ondersteunende ICT-systemen strikt verboden.	X	X	X	X
TMe13	Opdrachtnemer, bedienaars, beheerders en overig ondersteunend personeel mogen de beschikbaar gestelde toegangsmiddelen (tokens, pasjes) tot ICS/SCADA en ondersteunende systemen en netwerken alleen gebruiken voor het doel waarvoor ze ontworpen zijn. Hierbij mogen de getroffen beveiligingsmaatregelen niet omzeild worden.	X	X	X	X
TMe14	Bedienaars, beheerders en overig ondersteunend personeel houden hun accountgegevens strikt geheim; zij gebruiken hun account en toegekende autorisaties alleen zelf en staan niet toe dat anderen onder hun account kunnen inloggen of werken. Handelingen zijn altijd te herleiden naar de voor dat account geautoriseerde persoon.	X	X	X	X

TMe15	Opdrachtnemer, bedienaars, beheerders en overig ondersteunend personeel dienen op ICS/SCADA en de overige ondersteunende ICT-systemen en netwerken de standaard/default/fabrieks-accounts en/of wachtwoorden bij ingebruikname te verwijderen, uit te schakelen of ten minste te wijzigen.	X	X	X	X
TMe16	Bij het constateren van onregelmatigheden in de logische toegang tot ICS/SCADA en overige ondersteunende ICT-systemen dient iedere medewerker dit onverwijld als een beveiligingsincident te melden bij de Objectverantwoordelijke/-beheerder.	X	X	X	X
TMe17	Alleen geautoriseerde medewerkers/beheerders mogen systemen koppelen aan objectdatanetwerken of ICS/SCADA systemen. Deze systemen dienen voorzien te zijn van de laatste security updates, patches en actuele viruscontroleprogrammatuur koppelen	X	X	X	X
TMe18	Gegevensdragers worden altijd vooraf op malware gecontroleerd, voordat deze worden gekoppeld aan ICS/SCADA of overige ondersteunende ICT-systemen en netwerken.	X	X	X	X
TMe19	Mobiele apparatuur mag niet onbeheerd achtergelaten worden in openbare, vergader-, en conferentieruimten, in auto's of andere vervoermiddelen.	X	X	X	X
TMe20	Verlies of diefstal van mobiele apparatuur dient spoedig mogelijk te worden gemeld als een security incident.	X	X	X	X
TMe21	Incidenten die zich voordoen binnen het wijzigingsproces en afwijkingen van het wijzigingsproces moeten worden gemeld bij de Objectverantwoordelijke/ -beheerder.	X	X	X	X
TMe22	Onregelmatigheden, incidenten en storingen binnen het back-up en recovery proces moeten worden gemeld bij de Objectverantwoordelijke/ -beheerder.	X	X	X	X
Tme23	Beheerders en overig ondersteunend personeel zorgen ervoor dat onbeheerde ICS/SCADA-systemen en overige ICT-apparatuur wordt gelockt, ondersteund door een automatische lock na een vooraf in te stellen periode van inactiviteit.	X	X	X	X
TMe24	Opdrachtnemers, bedienaars, beheerders en overig personeel zijn zich bewust van de wijze waarop zij met vertrouwelijke informatie om te dienen te gaan, van het aanmaken en gebruiken van informatie tot vernietiging ervan.	X	X	X	X
TMe25	Medewerkers van de Opdrachtnemer die beheer- en onderhoudswerkzaamheden uitvoeren aan ICT en IA systemen van Rijkswaterstaat hebben een bewustwordingstraining voor cybersecurity gevolgd waarbinnen ook aandacht is besteed aan het vertrouwelijk omgaan met persoonsgegevens. Voor deze medewerkers geldt verder dat zij strikte geheimhouding in acht nemen en over een Verklaring Omtrent het Gedrag (VOG) beschikken zoals contractueel overeengekomen.	X	X	X	X
TMe26	Medewerkers mogen zonder voorafgaande goedkeuring geen apparatuur, informatie of software van de locatie meenemen.	X	X	X	X

TMe27	Het is voor gebruikers niet toegestaan zelf software te installeren.	X	X	X	X

2.7.2 Managers

Manager No.	Vereiste	Weerstandsniveau 1	2	3	4
TMa1	Er dient bewerkstelligd te worden dat een ieder continu (dus ook bij aanstelling en functiewisseling) bewust wordt gemaakt door Opdrachtnemer en (valideerbaar) geschikte training, regelmatige bijscholing krijgt (en ook begrijpt) en geïnformeerd wordt met betrekking tot het (cybersecurity) beveiligingsbeleid, procedures, en verantwoordelijkheden ten aanzien van cyber security, voor zover relevant voor hun functie. De voor hen geldende regelingen en instructies ten aanzien van informatiebeveiliging zijn eenvoudig toegankelijk. Een ieder die zich bezig houdt met risicomanagement dient hier kennis van te hebben, dan wel hiervoor specifieke aanvullende training te ontvangen.	X	X	X	X
TMa2	Opdrachtnemer draagt zorg voor en ziet erop toe dat bedienaars, beheerders en overig ondersteunend personeel: a. aantoonbaar kennis hebben van cybersecurity; b. de periodieke Cybersecurity cursussen, trainingen en E-Learningmodulen volgen en een actuele administratie hiervan aanwezig is. Daarbij dient bijgehouden te worden wanneer aanvullende training wenselijk dan wel noodzakelijk is; c. de beschikking hebben over actuele (technische) beheerdocumentatie, gebruikers- en/of installatiehandleidingen voor de ICS/SCADA en overige ondersteunende ICT-systemen en bedrijfsmiddelen; d. dat werkzaamheden door gescreend personeel uitgevoerd worden en dat geheimhouding is overeengekomen voor ingehuurd personeel; Objectverantwoordelijke/-beheerder bepaalt in welke situaties dit aan de orde is en de vorm waarin; e. ingehuurd personeel een geheimhoudingsverklaring heeft ondertekend; f. dat bedienaars, beheerders en overig ondersteunend personeel van zowel RWS als van externe partijen alle bedrijfsmiddelen, ICS/SCADA en overige ondersteunende ICT-systeemdocumentatie van RWS die ze in hun bezit hebben, retourneren bij beëindiging van hun dienstverband, contract of overeenkomst; g. dat de toegangsrechten van alle bedienaars, beheerders en overig ondersteunend personeel van zowel RWS als die van externe partijen de verstrekte toegangsmiddelen direct worden geblokkeerd bij beëindiging van het dienstverband, het contract of na wijziging van de overeenkomst worden aangepast. Opdrachtnemer dient veranderingen van personeel of subcontractors die toegang hebben tot de besturingssystemen van objecten ook direct kenbaar te maken aan opdrachtgever; h. dat calamiteitenplannen worden betrokken in de bewustwordingstrainingen, trainingen en testactiviteiten;	X	X	X	X

	i. gebruik van de centraal beschikbaar gestelde technische middelen voor fysieke en logische toegang op medewerkers niveau.				
TMa3	De Opdrachtnemer/objectverantwoordelijke/-beheerder/verantwoordelijk management bespreken en evalueren in de periodieke werkoverleggen de beveiligingsincidenten van de afgelopen periode, hoe op dergelijke incidenten is geacteerd, hoe het beter kan en hoe deze in de toekomst kunnen worden vermeden alsmede de feedback van de bewustwordingsactiviteiten en specifieke trainingen. Feedback van medewerkers dient actief te worden opgevolgd teneinde cybersecurity te verbeteren.		X	X	X
TMa4	Opdrachtnemer ziet erop toe (en heeft contractueel vastgelegd)_dat werknemers en ingehuurd personeel zich houden aan de gedragsregels voor beveiliging, zoals fysieke en logische toegang, melding van beveiligingsincidenten en gebruik van bedrijfsmiddelen. Voor zover controle op naleving van gedragsregels mogelijk is, wordt hiervoor een controleprogramma met steekproefsgewijze controles vastgesteld en uitgevoerd.			X	X
TMa5	Opdrachtnemer besteedt en bespreekt Cybersecurity in de functioneringsgesprekken met medewerkers en beheerders en maakt hiertoe opleidingsplannen waarbij wordt toegezien op uitvoering.	X	X	X	X
TMa6	Opdrachtnemer dient bij het constateren van onregelmatigheden in de logische toegang tot ICS/SCADA en overige ondersteunende ICT-systemen uit voorzorg altijd het betreffende account en wachtwoord te laten wijzigen.	X	X	X	X

2.8 Maatregelen gecontroleerd wijzigen

Mens No.	Vereiste	Weerstandsniveau 1	2	3	4
WM1	Voor bewustwording, gedragsregels en training van bedienaars, beheerders en overig ondersteunend personeel (zowel van RWS als die van Opdrachtnemer) wordt verwezen naar paragraaf 2.7 de maatregelen-set “bewustwording en training” van de Cybersecurity Implementatierichtlijn Objecten.	X	X	X	X

Procedures en Organisatie No.	Vereiste	Weerstandsniveau 1	2	3	4
WP1	Opdrachtnemer beschikt over een geborgde procedure voor het (laten) inventariseren en registreren van alle Configuration Items (CI’s) met bijbehorende settings/configuraties in een Configuration Management Database (CMDB). Deze CMDB dient actueel te worden gehouden.	X	X	X	X
WP2	Opdrachtnemer beschikt over een geborgde wijzigingsprocedure voor het doorvoeren van wijzigingen aan ICS/SCADA, ondersteunende ICT-systemen, beveiligings- en netwerkomgeving. Alle wijzigingen worden conform de wijzigingsprocedure geregistreerd. Updates en patches dienen via de reguliere wijzigingsprocedure te verlopen.	X	X	X	X
WP3	Wijzigingen mogen alleen worden aangevraagd en uitgevoerd door geautoriseerden.	X	X	X	X
WP4	Voor wijzigingen aan ICS/SCADA en overige ondersteunende ICT-systemen dient altijd een risicoafweging te worden gemaakt. De risicoafweging en de hieruit voortvloeiende maatregelen moeten zijn goedgekeurd door de Objectverantwoordelijke/-beheerder voordat uitvoering van werkzaamheden plaatsvindt.			X	X
WP5	De wijzigingen worden bijgewerkt in de CMDB en jaarlijks worden de settings/configuraties van ICS/SCADA en overige ondersteunende ICT-systemen in de CMDB vergeleken met de daadwerkelijke situatie en afwijkingen in de CMDB worden gecorrigeerd.	X	X	X	X
WP6	Wijzigingen in ICS/SCADA en overige ondersteunende ICT-systemen moeten vooraf aan de implementatie in productie worden getest in een testomgeving (inclusief verslaglegging) om te bewerkstelligen dat er geen nadelige gevolgen zijn voor de functionaliteit van het systeem of de beveiliging van de organisatie. Afwijken hiervan is uitsluitend mogelijk indien Opdrachtgever hiervoor toestemming geeft en dit schriftelijk wordt vastgelegd. Testen in de productieomgeving mag uitsluitend na voorafgaande goedkeuring door Opdrachtgever en na vastlegging hiervan. Alle testgegevens dienen zorgvuldig te worden gecontroleerd en beschermd.			X	X
WP7	Gegevensdragers en updates van software en firmware van technische systemen dienen eerst gescand te worden op malware	X	X	X	X

	voordat zij aan ICT of IA systemen worden gekoppeld en/of geïnstalleerd.				
WP8	De authenticiteit/integriteit van de software voor ICS/SCADA en overige ondersteunende ICT-systemen moet worden gecontroleerd voorafgaand aan de implementatie op operationele systemen.			X	X
WP9	Opdrachtnemer draagt zorg voor en ziet erop toe dat noodwijzigingen die buiten het reguliere wijzigingsproces om zijn doorgevoerd als gevolg van incidenten met een bijzonder (urgent) karakter achteraf alsnog de gebruikelijke procedures volgen en de CMDB administratie wordt bijgewerkt.	X	X	X	X
WP10	Voor elke wijziging is een terugval scenario opgesteld waarin is vastgelegd waaruit de terugval bestaat, onder welke condities tot een terugval wordt overgegaan en wie daartoe kan besluiten. Direct na de implementatie van een wijziging dient een test plaats te vinden om te verifiëren dat de wijziging is gelukt of dat op het terugval scenario moet worden overgegaan.			X	X
WP11	Opdrachtnemer ziet erop toe dat naar aanleiding van een wijziging uitgeschakelde beveiligingsmaatregelen weer zijn geactiveerd alvorens de wijziging te sluiten.	X	X	X	X
WP12	Er wordt gebruik gemaakt van testvoorzieningen, om de door te voeren wijzigingen en/of security patches vooraf te testen.	X	X	X	X

Techniek No.	Vereiste	Weerstandsniveau 1	2	3	4
WT1	Ontwikkel-, test-, acceptatie, productie en Leeromgeving (OTAPL) behoren te worden gescheiden om het risico van onbevoegde toegang tot of veranderingen aan de productieomgeving te verlagen door minimaal de volgende maatregelen: a. Functionele scheiding van de ontwikkel, test, acceptatie, productie en leeromgeving; b. De omgevingen zijn qua systemen en netwerk logisch of fysiek van elkaar gescheiden; c. Gebruikers dienen voor elke omgeving met andere gebruikersprofielen te kunnen werken; d. Voor de gebruikers is het helder in welke omgeving er wordt gewerkt; e. Elke omgeving dient conform de logrichtlijnen handelingen in logfiles vast te leggen die alleen toegankelijk is voor geautoriseerden; f. Er is een geborgd proces voor versiebeheer van de OTAPL.	X	X	X	X
WT2	Indien leverbaar dient het ICS/SCADA systeem en bijbehorende ICT-systemen de mogelijkheid te ondersteunen om de geïnstalleerde componenten en hun kenmerken te kunnen rapporteren.	X	X	X	X

2.9 Maatregelen beheer en onderhoud

Mens No.	Vereiste	Weerstandsniveau 1	2	3	4
OM1	Voor bewustwording, gedragsregels en training van bedienaars, beheerders en overig ondersteunend personeel (zowel van RWS als die van Opdrachtnemer) wordt verwezen naar paragraaf 2.7 de maatregelen-set “bewustwording en training” van de Cybersecurity Implementatierichtlijn Objecten.	X	X	X	X

Procedures en Organisatie No.	Vereiste	Weerstandsniveau 1	2	3	4
OP1	Opdrachtnemer draagt zorg voor het evalueren van risico’s en effectieve werking van de getroffen beheersmaatregelen voor beveiliging in het kader van life-cycle management.	X	X	X	X
OP2	Opdrachtnemer draagt zorg voor en ziet erop toe dat waar nodig in de beheer en onderhoudscontracten met onderaannemers: a. geheimhouding is opgenomen; b. training- en opleidingsvereisten alsmede overige benodigde certificeringen zijn beschreven; c. screening van personeel is geregeld (bijv. VOG); d. beschreven is dat de beveiligingshuisregels van Opdrachtgever strikt in acht moeten worden genomen; e. een concrete procedure is vastgelegd met betrekking tot incidentresponse en voor escalatieprocedures met de leverancier (7*24) en dat deze bij alle betrokkenen bekend is; f. de procedures voor fysieke toegang tot objecten en ruimten, alsook de logische toegang tot systemen zijn vastgelegd; g. de registratie en rapportage van beveiligingsincidenten is geregeld; h. beschreven is dat handelingen van medewerkers en systemen worden gelogd en gemonitord ; i. de procedure “Toegang Derden” van de CIV voor de logische toegang tot netwerken en systemen moet worden gevolgd. De tijdelijke toegang tot de systemen ten behoeve van ondersteuning dient geautoriseerd te zijn en handelingen dienen te worden gelogd. j. beschreven is dat onderhoud en wijzigingen op ICS/SCADA systemen alleen uitgevoerd mogen worden vanaf systemen die zijn voorzien van de laatste security updates, patches en actuele viruscontroleprogrammatuur; k. beschreven is dat netwerkkoppelingen op objectnetwerken altijd en strikt via de beveiligde centrale voorzieningen van RWS verlopen; l. beschreven is dat wijzigingen conform het wijzigingsproces van RWS mogen worden uitgevoerd; m. beschreven is dat patchen strikt conform de Patchrichtlijnen en doorlooptijden van RWS moeten worden uitgevoerd; n. beschreven is hoe omgegaan moet worden met alarmvoorzieningen van het object en de alarmopvolging; o. beschreven is dat het ongeautoriseerd koppelen van removable media en usb sticks aan het RWS- of objectnetwerken strikt verboden is.	X	X	X	X
OP4	Opdrachtnemer draagt zorg voor de beschikbaarheid, onderhoud en accuraat houden van (technische) beheerdocumentatie (waaronder fysieke en logische netwerktekeningen, verbindingen	X	X	X	X

	en configuratie documenten en een inventaris van alle apparatuur en software, inclusief versie- en serienummers), gebruikers- en/of installatiehandleidingen voor de ICT- en IA-systemen alsmede procedures voor het opnieuw opstarten en herstellen van het systeem in geval van systeemstoringen.				
OP5	Opdrachtnemer draagt zorg voor een geborgde procedure die de personele toegang van al het vaste onderhoudspersoneel regelt voorafgaand aan de uitvoering van werkzaamheden.			X	X
OP6	Opdrachtnemer houdt toezicht op de operationele uitvoering en naleving van: a. het doorvoeren van wijzigingen conform de wijzigingen procedure; b. de procedure voor fysieke toegang; c. de procedure voor logische toegang; d. patching, back-up procedure en bewaartermijnen; e. incidentmanagement, log- en incidentrapportages en de analyse daarvan.	X	X	X	X
OP7	Opdrachtnemer dient jaarlijks de opzet, het bestaan en de werking van de getroffen maatregelen te (laten) onderzoeken, evalueren en bij te stellen. De resultaten dienen te worden gerapporteerd aan Opdrachtgever en het Cybersecurity Beveiligingsplan bijgewerkt en voorgelegd te worden aan de Opdrachtgever.		X	X	X
OP8	RWS Bedrijfsvertrouwelijk is alleen op basis van het ‘need-to-know’ principe toegankelijk voor de medewerkers van Rijkswaterstaat en de Opdrachtnemer.	X	X	X	X
OP9	Rijkswaterstaat en Opdrachtnemer zijn vanaf het moment van ontvangst van informatie verantwoordelijk om binnen de eigen organisatie de ontsluiting en verwerking van de informatie op de afgesproken werkwijze van ‘need-to-know’ te verzorgen.	X	X	X	X
OP10	Geprinte exemplaren van documenten met classificatie RWS Bedrijfsinformatie dienen in afgesloten kasten bewaard te worden. Bij digitale opslag in de eigen kantooromgeving is versleuteling niet verplicht.	X	X	X	X
OP11	Opdrachtnemer dient zowel actieve als passieve apparaten te controleren op malware voordat deze worden verbonden met, of gebruikt in, de IA-omgeving.	X	X	X	X
OP12	Het koppelen van beheer- en onderhoudsapparatuur aan ICT- en IA-systemen bij een object, dient op veilige wijze te gebeuren.	X	X	X	X
OP13	Apparatuur dient correct te worden onderhouden om de continue beschikbaarheid en integriteit ervan te waarborgen	X	X	X	X

Techniek		Weerstandsniveau 1	2	3	4
OT1	Voor de fysieke toegang (ICT-deel) van bedienaars, beheerders en overig ondersteunend (RWS en extern) personeel tot objecten en	X	X	X	X

	de ruimten hierbinnen, wordt gebruikt gemaakt van de PDC producten en diensten van RWS-CIV en RWS-CD.				
OT2	Voor (remote) logische toegang van bedienaars en beheerders tot het netwerk en ICS/SCADA systemen wordt gebruikt gemaakt van de PDC producten en diensten van RWS-CIV.	X	X	X	X
OT3	Gedurende FAT, SAT en onderhoud dient de werking van de cybersecurityfuncties in de systemen te kunnen worden aangetoond.	X	X	X	X
OT4	Gedurende FAT, SAT en onderhoud dient de werking van de cybersecurityfuncties in de systemen geautomatiseerd te kunnen worden aangetoond middels tooling.			X	X
OT5	Het koppelen van beheer- en onderhoudsapparatuur aan ICT- en IA-systemen bij een object, dient op veilige wijze te gebeuren.	X	X	X	X

2.10 Maatregelen back-ups

Mens No.	Vereiste	Weerstandsniveau 1	2	3	4
BM1	Voor bewustwording, gedragsregels en training van bedienaars, beheerders en overig ondersteunend personeel (zowel van RWS als die van Opdrachtnemer) wordt verwezen naar paragraaf 2.7 de maatregelen-set “bewustwording en training” van de Cybersecurity Implementatierichtlijn Objecten.	X	X	X	X

Procedures en Organisatie No.	Vereiste	Weerstandsniveau 1	2	3	4
BP1	Systeemimages/back-ups worden gemaakt vooraf en na iedere (functionele) systeemwijziging. Wanneer wijzigingen uitblijven wordt de systeemimage/back-up van de laatste versie op jaarbasis vernieuwd. Met deze back-up moet men in staat zijn middels een volledige roll-back naar de werkende situatie terug te kunnen gaan. Indien back-ups gedurende de operationele fase van een object gemaakt moeten worden, dan mag dit het operationele proces niet verstoren.	X	X	X	X
BP2	De integriteit en beschikbaarheid van de laatste drie versies van de ICS/SCADA systemen, programmatuur en besturingssystemen dient gewaarborgd te worden door het maken en testen van systeemimages/back-ups, conform een geborgde procedure: a. Deze back-ups worden opgeslagen op een locatie die zich op zodanige afstand bevindt dat geen schade aan de back-up kan worden aangericht als een calamiteit zich voordoet op de locatie waar het systeem zich bevindt; b. Back-ups en de ruimte waarin ze zijn opgeslagen behoren fysiek goed te worden beschermd volgens dezelfde normen die gelden voor de hoofdlocatie en zijn alleen toegankelijk voor bevoegden; c. Back-ups worden bewaard tot het moment van uitdienstname van het betreffend systeem; d. In geval de back-up terug wordt gezet, dient eventueel ook rekening te worden gehouden met ook het terugzetten van de dynamische gegevens over de systeemstatus.	X	X	X	X
BP3	Opdrachtnemer heeft gedocumenteerde herstelprocedures en volledige en actuele registers van back-up kopieën.	X	X	X	X
BP4	Opdrachtnemer controleert en test jaarlijks de herstelprocedures om te waarborgen dat ze doeltreffend zijn, dat ze werken en dat ze kunnen worden uitgevoerd binnen de daarvoor overeengekomen tijd. Jaarlijks wordt een recovery test gedaan om te zien of de media nog leesbaar is.		X	X	X
BP5	Opdrachtnemer evalueert maandelijks de gemelde incidenten en storingsmeldingen inzake back-up en treft waar nodig maatregelen.		X	X	X

Techniek No.	Vereiste	Weerstandsniveau 1	2	3	4
BT1	Opdrachtnemer richt in overleg met Opdrachtgever de benodigde voorzieningen in voor het back-up en restoreproces.	X	X	X	X

Bijlage CSR 1 Omgaan met vertrouwelijke informatie en documenten

CSR 1.1 Doelstelling

Medewerkers van Rijkswaterstaat en haar Opdrachtnemers moeten op de juiste wijze omgaan met vertrouwelijke informatie (documenten en gegevens). Dit is mede van groot belang voor de beveiliging van de ICT infrastructuur en de primaire processen van Rijkswaterstaat tegen cybercriminaliteit. Beveiliging van de informatievoorziening en bedienketens in het primair proces, hangt direct samen met de beveiliging van de documentatie betreffende de ICT-infrastructuur. De vertrouwelijkheid van informatie wordt uitgedrukt in een classificatie. De classificatie geeft de aard van de documentatie weer en helpt de gebruiker bij het bepalen hoe een document verwerkt dient te worden.

Rijkswaterstaat houdt de volgende rubricering of informatieclassificatie aan:

a. Departementaal Vertrouwelijk;
b. RWS Bedrijfsvertrouwelijk;
c. RWS Bedrijfsinformatie.

Departementaal Vertrouwelijk

Deze informatie dient strikt vertrouwelijk te worden behandeld en mag uitsluitend op basis van need-to-know worden verstrekt. Informatie met deze classificatie mag niet worden uitgewisseld met Opdrachtnemers en valt derhalve buiten de scope van dit document.

RWS Bedrijfsvertrouwelijk

Deze informatie is uitsluitend toegankelijk voor diegenen die de informatie nodig hebben om hun werkzaamheden uit te kunnen voeren en wordt op basis van need-to-know verstrekt.

RWS Bedrijfsinformatie

Deze informatie is voor iedereen vrij toegankelijk.

CSR 1.2 Best practice

CSR 1.2.1 Uitwisselen van informatie

In de overeenkomst tussen Rijkswaterstaat en een Opdrachtnemer zijn eisen opgenomen voor geheimhouding en het vertrouwelijk omgaan met documenten.

Voorbeelden van RWS bedrijfsvertrouwelijke informatie (gerelateerd aan cybersecurity) zijn:

a. Ontwerpdocumenten, constructietekeningen en -berekeningen;
b. Bediening en beheer handleidingen, veiligheidsinstructies en documentatie;
c. Configuratiedocumentatie van ICT en ICS/SCADA-systemen;
d. Datanetwerkschema's en IP adressen;
e. Informatie over de ligging van kabels en leidingen;
f. Informatie over accounts en wachtwoorden.

Uitwisseling van informatie kan op meerdere manieren plaatsvinden. Voor elke wijze van uitwisseling zijn specifieke voorwaarden en regels van kracht:

Informatie uitwisseling via email

a. Informatie met de classificatie RWS Bedrijfsvertrouwelijk mag onversleuteld via email worden uitgewisseld tussen Rijkswaterstaat en Opdrachtnemer.
b. Informatie met de classificatie TLP AMBER mag onversleuteld via email worden uitgewisseld tussen Rijkswaterstaat en BAW partners.

Informatie uitwisseling via bestand-uitwisselingsservices

a. Informatie met de classificatie RWS Bedrijfsvertrouwelijk via Wetransfer (of vergelijkbare service) mag uitsluitend versleuteld worden uitgewisseld tussen Rijkswaterstaat en Opdrachtnemer, waarbij bestanden worden versleutel met AES 256 encryptie. Het gekozen wachtwoord is uniek voor elke bestandsuitwisseling en dient te voldoen aan de wachtwoordrichtlijn en via een ander communicatiekanaal (b.v. via SMS) aan de ontvangende partij te worden verzonden.

b. Informatie met de classificatie TLP AMBER via Wetransfer (of vergelijkbare service) mag uitsluitend versleuteld worden uitgewisseld tussen Rijkswaterstaat en BAW partners, waarbij bestanden worden versleutel met AES 256 encryptie. Het gekozen wachtwoord is uniek voor elke bestandsuitwisseling en dient te voldoen aan de wachtwoordrichtlijn en via een ander communicatiekanaal (b.v. via SMS) aan de ontvangende partij te worden verzonden.

Informatie uitwisseling via servers van opdrachtnemer of opdrachtgever

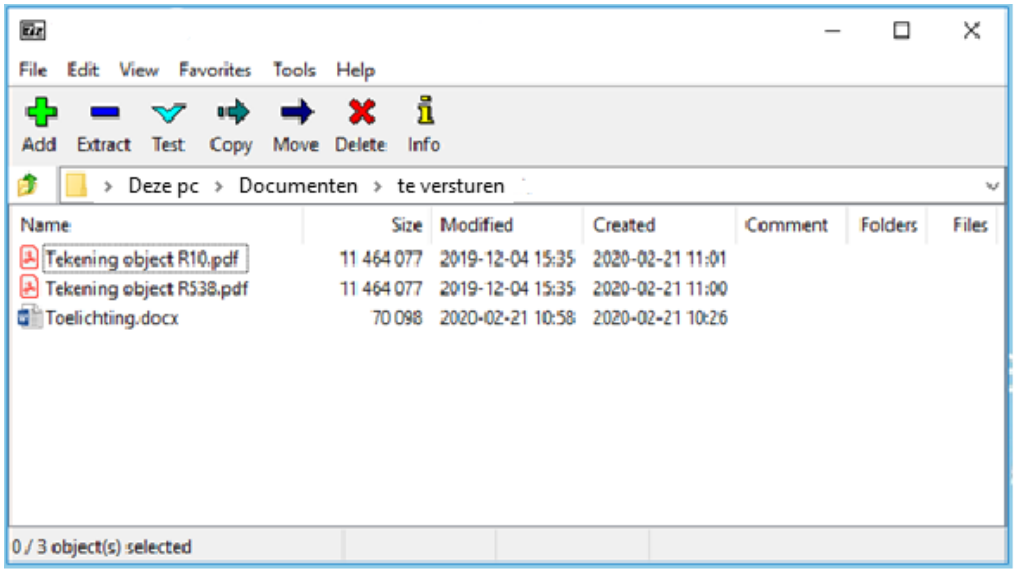
Informatie met de classificatie RWS Bedrijfsvertrouwelijk of TLP AMBER mag onversleuteld via servers van opdrachtgever, opdrachtnemer of BAW partner worden uitgewisseld, mits er een voldoende authenticatie van de gebruiker en zijn bevoegdheden plaatsvindt.

CSR 1.2.2 Versleutelen van gegevens

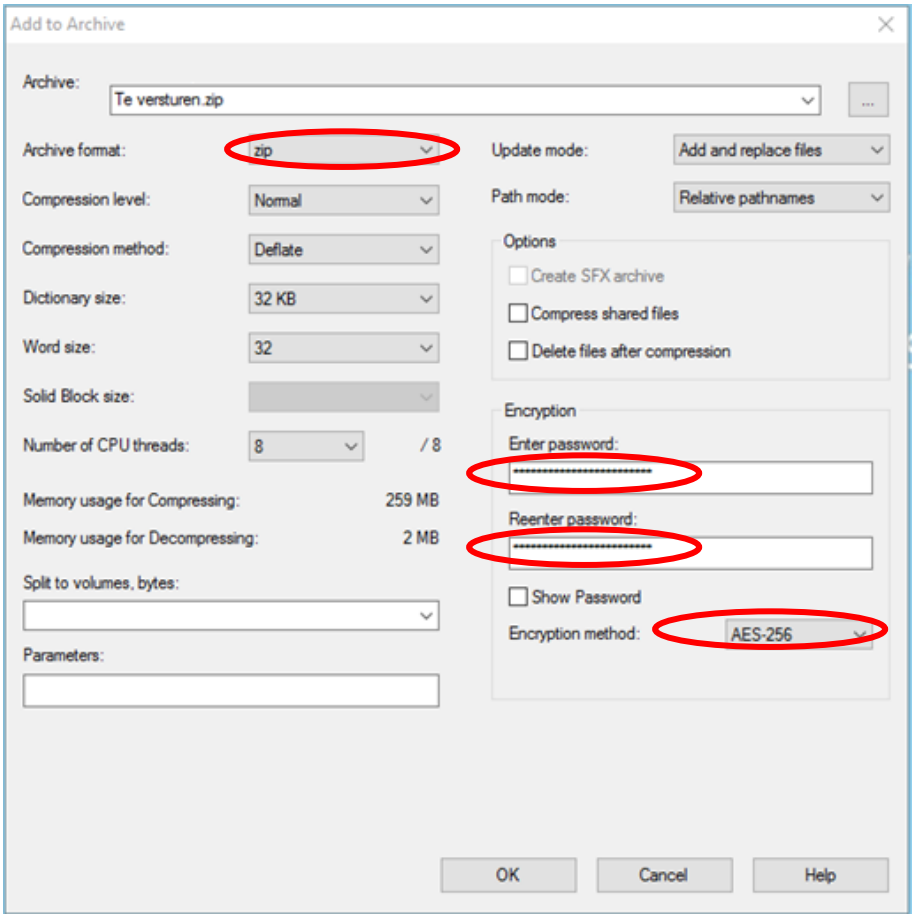
Wanneer versleuteling van informatie nodig is, dient dit te gebeuren met ten minste AES 256 encryptie en een sterk wachtwoord dat voldoet aan de vereisten voor wachtwoorden. Voor versleuteling maakt RWS gebruik van 7-Zip. Dit is een eenvoudig te gebruiken computerprogramma, waarmee bestanden versleuteld ingepakt kunnen worden.
7-Zip is standaard aanwezig op de RWS werkplek en is tevens gratis voor (thuis)gebruik (zie www.7-zip.org). Bij gebruik van AES-256 versleuteling en sterke wachtwoorden (zie hiervoor de wachtwoordrichtlijn) biedt 7-Zip een veilige manier voor gegevensversleuteling.

Documenten versleutelen met 7-Zip

a. Start 7-Zip via de Start toets links onderin Windows.
b. Ga naar de folder waar de te versleutelen bestanden staan.



c. Selecteer de bestanden en klik op de Add button (het groene + symbool).



d. Selecteer:
    i. Archive format: zip
    ii. Encryption method: AES-256
e. Kies een wachtwoord dat voldoet aan de wachtwoordrichtlijn en voer dit in.
f. Klik op de OK button en sluit 7-Zip af.
g. Het versleutelde bestand is klaar om te versturen.

Documenten ontsleutelen met 7-Zip

a. Open het bestand in 7-zip.
b. Selecteer de Extract button (het blauwe — symbool).
c. Selecteer de folder waar het bestand uitgepakt dient te worden.
d. Voer het wachtwoord in en klik de OK button.

CSR 1.2.3 Overdracht en vernietiging van vertrouwelijke data bij einde contract

Bij het aflopen en beëindiging van een contract draagt de Opdrachtnemer alle voor het onderhoud (en onderhoudshistorie) relevante objectinformatie -met de classificatie Bedrijfsvertrouwelijk- gestructureerd over aan Rijkswaterstaat.
Daarna vernietigt Opdrachtnemer de overgebleven Bedrijfsvertrouwelijke informatie en verwijdert deze alle Bedrijfsvertrouwelijke informatie van de eigen systemen.

Bijlage CSR 2 Personele toegang

CSR 2.1 Doelstelling

Het van belang inzicht te hebben in wie toegang heeft tot de IA systemen binnen de objecten. Van onderhoudspersoneel dient te worden vastgesteld dat verwacht kan worden dat zij op juiste wijze zullen omgaan met informatie waartoe men toegang heeft.

CSR 2.2 Best practice

Best practices voor personele toegang zijn als volgt (indachtig naleving van AVG regels):

a. De Opdrachtnemer dient te verzorgen dat al het vast onderhoudspersoneel voorafgaand aan zijn/haar operationele inzet:
   i. een persoonlijke geheimhoudingsverklaring heeft ondertekend;
   ii. zich daarbij kan legitimeren met een officieel geldig legitimatiemiddel met een goed gelijkende pasfoto;
   iii. een Verklaring Omtrent Gedrag (VOG) bezit welke is gerelateerd aan de beoogde Werkzaamheden;
b. Hangende de aanvraag voor een VOG kan volstaan worden met een eigen verklaring van de betreffende medewerker gedurende een periode van maximaal zes weken welke niet verlengd kan worden.

De Opdrachtnemer dient er op toe te zien dat al het onderhoudspersoneel dat niet structureel verschijnt:

a. Zich legitimeert;
b. In specifieke gevallen op eerste verzoek van de Opdrachtgever bereid is een eigen verklaring en een geheimhoudingsovereenkomst te ondertekenen.

De Opdrachtnemer dient al haar medewerkers nadrukkelijk te informeren over het feit dat het doorgeven van informatie over de werking, inrichting, organisatie rondom de objecten in welke vorm dan ook NIET zal geschieden dan na uitdrukkelijke toestemming van de Opdrachtgever.

Iedere geconstateerde afwijking van bovenstaande eisen dient door de Opdrachtnemer te worden behandeld als security incident.

Bijlage CSR 3 Architectuur objectnetwerk

CSR 3.1 Doelstelling

RWS streeft bij elk van de objecten naar een netwerkinfrastructuur die in lijn is met de te beschermen belangen en de geïdentificeerde risico's. Middels deze richtlijn wordt richting gegeven aan de cyberweerbaarheid van de objectnetwerken. Om de cyberweerbaarheid van de totale RWS ICT netwerk infrastructuur te waarborgen is het noodzakelijk dat elk te koppelen object dusdanig is ontworpen dat de cyberweerbaarheid gewaarborgd is. De hierbij gemaakte ontwerpkeuzes en bijbehorende maatregelen hebben als doel het object weerbaar te maken tegen cyberdreigingen, met een minimale impact bij een mogelijk cyberincident.

Het is van belang dat de gemaakte architectuurkeuzes van een objectnetwerk de gestelde maatregelen ondersteunen. Dat betreft enerzijds een veilige inrichting van het objectnetwerk zelf en anderzijds een zodanige inrichting dat data op een veilige en betrouwbare wijze ontsloten kan worden.

Deze richtlijn is bedoeld voor de medewerkers van de opdrachtnemer die tijdens nieuwbouw- of renovatieproject een netwerk voor het object specificeren en ontwerpen.

CSR 3.2 Best Practice

CSR 3.2.1 Inleiding

Binnen Rijkswaterstaat wordt onderscheid gemaakt in de netwerken voor de Informatie Voorziening (IV) en de netwerken voor de Industriële Automatisering (IA) ook wel Procesautomatisering (PA) of Operationele Technologie (TO) genoemd.
Binnen het IV netwerk wordt voor het waarborgen van de vertrouwelijkheid, integriteit en beschikbaarheid gewerkt volgens het RWS zoneringsmodel. Dit RWS zoneringmodel voor het IV netwerk is gebaseerd op het zoneringsmodel van de NORA[2].

Echter voor objectnetwerken wordt deze segmentering op basis van vertrouwelijkheidsniveaus niet toegepast. In plaats daarvan wordt een zonering toegepast op basis van een risicobeoordeling van het object.

Voor de segmentering van het objectnetwerk geldt het uitgangspunt: "een apart netwerksegment voor elke onderkende functie voor het functioneren van het object".

Voor de verschillende netwerksegmenten geldt het volgende:

a. Netwerksegmenten zijn fysiek of logisch van elkaar, gescheiden (er kan geen verkeer vrij tussen verschillende segmenten worden uitgewisseld);
b. Voor de netwerksegmenten is bepaald aan welke zones deze gekoppeld kunnen zijn;
c. Netwerk toegang door gebruikers is rol gebaseerd en per zone onder controle.

In een verzameling netwerksegmenten over verschillende objecten geldt een restrictie voor het onderlinge verkeer. Een object mag niet direct verkeer uitwisselen met een object op een andere locatie. Dit mag alleen via een gecontroleerd en gemonitord koppelvlak. Er mag wel verkeer plaatsvinden tussen het object en de centrale bedienlocatie.

CSR 3.2.2 Risicobeoordeling

Om tot een juiste netwerksegmentatie te komen wordt van opdrachtnemer verwacht dat er op basis van een risico beoordeling een zoneringsmodel van het objectnetwerk wordt gemaakt. In het zoneringsmodel worden (op basis van een abstracte weergave) afgebakende netwerken met IV en IA voorzieningen weergegeven. Binnen een zone kunnen gegevens vrij worden uitgewisseld. Gegevensuitwisseling met andere zones verloopt via gedefinieerde koppelvlakken. Het doel van zonering is het isoleren van risico's zodat bedreigingen en incidenten uit de ene zone niet kunnen doorwerken in de andere zone.

[2] https://www.noraonline.nl/wiki/Beschouwingsmodel_zonering

Op basis van een netwerkontwerp met netwerksegmentering wordt invulling gegeven aan het gedefinieerde zoneringsmodel.

Hiervoor dienen de volgende stappen te worden doorlopen:

a. Identificeer het totale systeem dat valt onder de opdracht;
b. Bepaal de cybersecurity risico's van het systeem en de deelsystemen;
c. Deel, op basis van de geïdentificeerde risico's, het systeem op in zones en de benodigde verbindingen tussen de zones;
d. Pas de maatregelen toe behorende bij het weerstandsniveau van het object;
e. Bepaal de overgebleven risico's voor elke zone;
f. Neem aanvullende cybersecurity maatregelen om de overgebleven risico's te mitigeren.

CSR 3.2.3 Uitgangspunten

Hierbij dienen de volgende uitgangspunten in acht te worden genomen:

a. Binnen een object worden op basis van de risico inventarisatie aparte netwerksegmenten ingericht.
b. Het zoneringsmodel dient te voldoen aan de maatregelen zoals vereist vanuit het weerstandsniveau van het object;
c. Het objectnetwerk bestaat uit een gelaagde opbouw die aansluit op het Purdue model;
d. Bedreigingen en incidenten uit de ene zone mogen niet doorwerken in de andere zone.
e. Zones kunnen logisch worden gescheiden door gebruikmaking van routering van datastromen, verificatie van de bron- en de bestemmingsadressen, door toepassing van verschillende protocollen, encryptietechnologie, partitionering of virtualisatie van servers, maar ook door fysieke scheiding;
f. Uitwisseling van gegevens tussen zones vindt uitsluitend plaats via een gedefinieerd koppelvlak. Deze koppelvlakken staan uitsluitend het noodzakelijke netwerkverkeer toe;
g. Voor de geïdentificeerd noodzakelijke communicatie tussen segmenten moet een risico beoordeling worden gemaakt en de juiste maatregelen zijn getroffen om de geïdentificeerde risico's te mitigeren;
h. Waar mogelijk wordt gebruik gemaakt van de beschikbare RWS bouwblokken;
i. Als er vereisten zijn vanuit safety dan worden die meegenomen in het netwerkontwerp.

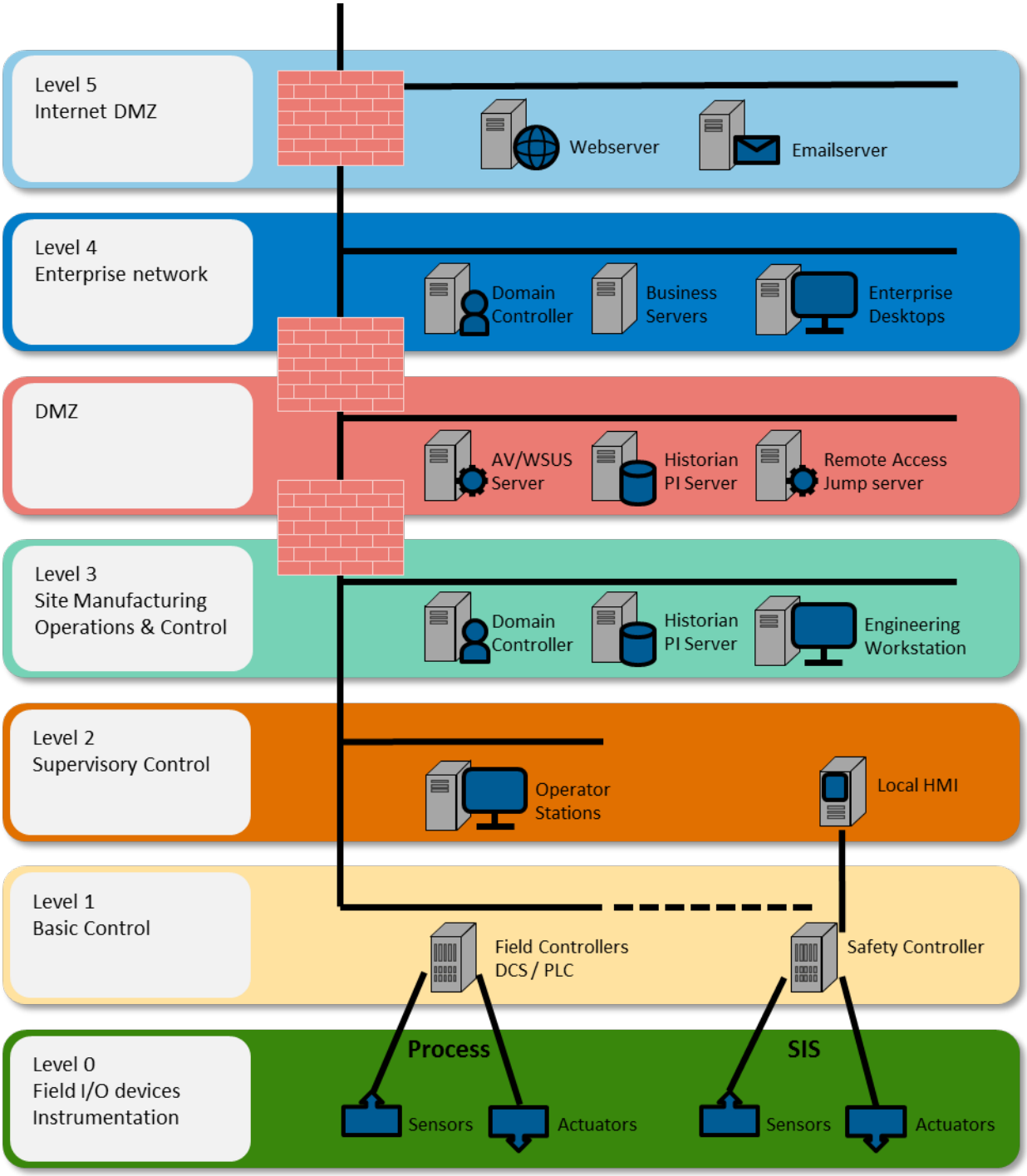
CSR 3.2.4 Gelaagde opbouw van het netwerk

In industriële omgevingen wordt voor de gelaagde opbouw van de netwerkinfrastructuur gerefereerd naar het Purdue model. Dit model gaat ervanuit dat er een aantal lagen zijn te onderscheiden, waarbij er tussen laag 3 en 4 een DMZ wordt ingericht om communicatie tussen IV en IA op digitaal veilige wijze te laten verlopen:

a. Laag 5 is de DMZ tussen het bedrijfsnetwerk en de externe netwerken;
b. Laag 4 is het bedrijfsnetwerk;
c. DMZ om IV en IA netwerken te scheiden (laag 3,5);
d. Laag 3 is gereserveerd voor Operations management;
e. Laag 2 bevat de lokale bediening;
f. Laag 1 bevat de veld controllers;
g. Laag 0 bevat de sensors en actuatoren, ofwel de interface tussen de elektronische wereld en de fysieke wereld.

CSR 3.2.5 Inrichting van het netwerk

Elke overgang tussen twee segmenten dient zodanig ingericht te zijn dat (in beide richtingen) geen verkeer wordt doorgelaten tenzij het noodzakelijk is ("deny by default") voor het veilig functioneren van het object. Daarnaast dient het objectnetwerk functioneel autonoom te zijn en derhalve zodanig te zijn ingericht en uitgerust dat het object ook op basis van lokale bediening kan functioneren. De werking van het object mag niet afhankelijk zijn van de beschikbaarheid van externe netwerken (island mode functie).



CSR 3.2.6 Koppelvlakken

Bijzondere aandacht dient besteed te worden aan de koppelvlakken tussen de verschillende segmenten. Daarbij zijn de volgende situaties te onderscheiden:

a. Koppelvlakken tussen segmenten binnen het object:
   De beveiliging van deze koppelvlakken wordt bepaald door een risicobeoordeling op de verschillende zones van het object.
b. Koppelvlakken met het DMZ:
   De beveiliging van deze koppelvlakken wordt bepaald door een risicobeoordeling met expliciet aandacht voor de koppeling met het DMZ en externe netwerken.

Bijlage CSR 4 Het veilig koppelen van beheer- en onderhoudsapparatuur aan ICT- en IA-systemen

CSR 4.1 Doelstelling

Tijdens het verrichten van beheer- onderhoudswerkzaamheden wordt door medewerkers van de Opdrachtnemer soms tijdelijk apparatuur (bijvoorbeeld draagbare media, waaronder USB-sticks, externe disks, laptop, tablet, CD's, DVD's, enz.)gekoppeld aan de ICT- en IA-omgeving (PLC's, servers, routers, switches, enz.) van Rijkswaterstaat. Hierdoor ontstaan cybersecurity risico's zoals b.v. malwarebesmetting of binnendringing van het netwerk. De Opdrachtnemer dient deze risico's te mitigeren.

CSR 4.2 Best practice

CSR 4.2.1 Soorten apparatuur

Met betrekking tot het koppelen van apparatuur wordt er onderscheid gemaakt tussen een tweetal soorten apparaten:

a. Actieve apparaten;
b. Passieve apparaten.

Actieve apparaten

Onder actieve apparaten wordt verstaan apparaten die zelfstandig kunnen opereren en over een Operating System beschikken, zoals b.v. een laptop of tablet.

Passieve apparaten

Onder passieve apparaten wordt verstaan apparaten die een actief apparaat nodig hebben voor informatie-uitwisseling. Dit zijn gegevensdragers en opslagmedia, zoals b.v. USB-sticks, externe disks, DVD's, CD-ROM's.

CSR 4.2.2 Instructies voor gebruik van actieve apparaten

Initieel

a. Zorg dat het apparaat gehardend is;
b. Versleutel de harde schijf van het apparaat;
c. Beveilig de toegang tot het apparaat met een sterk wachtwoord;
d. Installeer een malwarescanner;
e. Zet de interne firewall aan op het apparaat.

Vóór en tijdens elk gebruik

a. Gebruik het apparaat uitsluitend voor beheer en onderhoud van IA systemen van Rijkswaterstaat;
b. Alvorens verbinding te maken met het IA netwerk op de objecten, installeer de laatste updates en patches;
c. Alvorens verbinding te maken met het IA netwerk op de objecten, installeer de laatste updates van de malwarescanner en scan het apparaat;
d. Alvorens verbinding te maken met het IA netwerk op de objecten, download de benodigde updates en patches voor ICT en IA systemen;
e. Alvorens verbinding te maken met het IA netwerk op de objecten, download ICT of IA-software (updates en patches) uitsluitend vanaf een betrouwbare bron en via een beveiligde verbinding;
f. Alvorens verbinding te maken met het IA netwerk op de objecten, controleer de integriteit van downloads van ICT en IA software met de meegeleverde hashcode;
g. Alvorens verbinding te maken met het IA netwerk op de objecten, controleer de downloads op malware voordat deze worden geïnstalleerd binnen de ICT of IA omgeving;
h. Alvorens verbinding te maken met het IA netwerk op de objecten, zet 3G, 4G, 5G, WiFi, Bluetooth uit (koppelingen tussen IA en andere netwerken zijn niet toegestaan) en laat deze gedurende de koppeling met het IA netwerk uit staan;
i. Alvorens verbinding te maken met het IA netwerk op de objecten, dienen mobiele gegevensdragers door Opdrachtnemer ter controle gescand te worden op malware.

CSR 4.2.3 Instructies voor gebruik van passieve apparaten

Gebruik uitsluitend de voorgeschreven opslagmedia voor de koppeling met ICT- of IA-systemen;
Zorg dat alle gegevens op USB-sticks en externe harde schijven versleuteld zijn, volgens de richtlijn voor het omgaan met vertrouwelijke gegevens;
Scan gegevensdragers zoals b.v. USB-sticks, externe harde schijven, CD-ROM's, DVD's en diskettes elke keer vóór gebruik binnen de ICT- of IA-omgeving op malware;
Vervang een gegevensdrager waarop malware is ontdekt door een nieuwe gegevensdrager;
Alvorens verbinding te maken met het IA netwerk op de objecten, dienen gegevensdragers door Opdrachtnemer ter controle gescand te worden op malware.

CSR 4.2.4 Smartphones en Tablets

Smartphones en Tablets mogen niet worden ingezet voor bediening. Bij voorkeur ook niet voor beheer en onderhoudswerkzaamheden, aangezien deze niet kan voldoen aan de gestelde veiligheidseisen.

Bijlage CSR 5 Draadloze netwerken

CSR 5.1 Doelstelling

Middels draadloze communicatie is het mogelijk om op afstand te communiceren met een ander apparaat. WIFI, infrarood, Bluetooth, LoRa, 4G en 5G zijn enkele methoden voor draadloze communicatie. In tegenstelling tot bedrade communicatie hoeft een aanvaller geen fysieke toegang te hebben tot het netwerk of de apparatuur. Doelstelling is draadloze communicatie zo veel mogelijk te beperken en (waar gebruikt) te beveiligen tegen binnendringing en/of manipulatie.

CSR 5.2 Best practices

Basisuitgangspunt is dat de draadloze interfaces in apparaten en systemen zijn uitgeschakeld. Waar draadloze communicatie toch wordt ingezet, geldt het volgende:

a. Het gebruik van draadloze communicatie voor besturing en bediening van een object is niet toegestaan;
b. Het gebruik van draadloze communicatie voor het doorgeven van meetinformatie voor meten is uitsluitend toegestaan als het communicatiekanaal niet gebruikt kan worden voor configuratie, herstarten, uitschakelen of op enige andere wijze manipuleren van de meeteenheid;
c. Het gebruik van draadloze communicatie (o.a. WIFI, Bluetooth, IR, maar niet beperkt hiertoe) voor configuratie van apparatuur is uitsluitend toegestaan als de mogelijkheid tot draadloze communicatie na configuratie wordt uitgeschakeld;
d. Het draadloze netwerksegment is (bij voorkeur fysiek) gescheiden van het overige netwerk;
e. Communicatie tussen het draadloze netwerk en het vaste IA netwerk loopt via een beveiligd koppelvlak;
f. Bij draadloze verbindingen wordt gebruik gemaakt van encryptie middelen waarvoor het NBV een positief inzetadvies heeft afgegeven;
g. Voor de inzet van draadloze communicatie dient een risicoanalyse en afweging gemaakt te worden waarin ook de restrisico's en compenserende maatregelen zijn uitgewerkt;
h. Daar waar draadloze communicatie wordt toegepast dient dit te worden gedocumenteerd en onderhouden;
i. Telemetriesystemen o.b.v. GPRS, 4G, 5G enz. dienen koppelingen tussen SIM-kaart ID en Mac-adres van het bijbehorende apparaat vast te leggen;
j. De risicoanalyse en –afweging dient voorgelegd te worden aan het Security Centre van RWS/CIV voor goedkeuring;
k. Draag zorg voor passende fysieke beveiliging van de draadloze netwerkcomponenten om te voorkomen dat kwaadwillenden toegang hebben tot de infrastructuur;
l. Draadloze communicatie dient op een veilige wijze geconfigureerd te worden;
m. Draadloze communicatie dient te worden gelogd in overeenstemming met de logging richtlijn.

Bijlage CSR 6 IoT

CSR 6.1 Doelstelling

Internet of Things (IoT) apparatuur vindt ook binnen de IA steeds meer zijn weg. Het is van belang om deze apparatuur op een cyberveilige wijze te gebruiken.

CSR 6.2 Best practices

Voor gebruik van IoT apparatuur binnen de IA-omgeving dient tenminste te worden voldaan aan het volgende:

a. Voordat IoT wordt ingezet dient een risico en privacy assessment te zijn uitgevoerd en zijn waar relevant mitigerende maatregelen getroffen;
b. IoT toepassingen worden net als IA toepassingen beheerd en onderhouden en zijn derhalve opgenomen in het asset management CMDB, waarbij alle mogelijkheden om gegevens te verzamelen zijn gedocumenteerd;
c. IoT mag uitsluitend worden gebruikt voor het verzamelen van (meet)gegevens of telemetrie, niet voor het sturen of besturen van installaties;
d. IoT apparaten dienen in een apart netwerksegment te worden geplaatst dat is gescheiden middels een firewall die uitsluitend de noodzakelijke communicatie doorlaat;
e. Verschillende IoT systemen worden van elkaar geïsoleerd;
f. Principes van least privileges en hardening (uitschakelen debug interfaces, software services en andere niet gebruikte functionaliteit) worden toegepast;
g. Risico gestuurd dienen kwetsbaarhedenscans uitgevoerd te worden voor de gebruikte IoT apparatuur. Hierbij is aandacht voor kwetsbaarhedenscans, netwerk en penetratietesten;
h. IoT apparaten dienen gebruik te maken van wachtwoorden die voldoen aan de gestelde vereisten voor wachtwoord;
i. Elk IoT apparaat heeft een uniek, sterk wachtwoord dat niet af te leiden is uit andere wachtwoorden, device naam of gebruikersnaam. Hierbij dient de wachtwoordrichtlijn te worden gevolgd;
j. Pas waar mogelijk, en in overeenstemming met het weerstandsniveau van het object en de te beschermen functionaliteit, two-factor authenticatie toe;
k. Alle niet gebruikte protocollen dienen te worden uitgeschakeld;
l. Niet gebruikte (logische en fysieke) poorten dienen te worden uitgeschakeld of afgesloten;
m. IoT toepassingen worden risico gestuurd technisch gemonitord;
n. Foutieve inlogpogingen worden gelogd;
o. Het aantal foutieve inlogpogingen wordt beperkt;
p. IoT toepassingen worden voor ingebruikname afdoende getest.
q. IoT systemen vallen ook onder het regime van incident management, patchmanagement, configuratiemanagement en changemanagement;
r. De gebruikte IoT apparatuur dient voordat deze kan worden gebruikt, voldoende authenticatie te bieden, die in overeenstemming is met het weerstandsniveau van het object;
s. Security by design principes en secure development processes worden opgevolgd;
t. De life cycle van IoT apparatuur is vastgelegd en wordt nageleefd;
u. Vermijdt het gebruik van proprietary protocollen en versleutelingsalgoritmen, en pas uitsluitend bekende, gedocumenteerde en updatebare protocollen en versleutelingsalgoritmen toe;
v. IoT apparaten dienen te kunnen herstarten vanaf een vooraf gedefinieerde en beveiligde configuratie en daarbij de integriteit van de software te kunnen controleren;
w. Alle beschikbare beveiligingsmaatregelen op de IoT apparaten staan standaard aan;
x. Bij verwerking van persoonsgegevens dient te worden voldaan aan de AVG;
y. Inzet van IoT apparatuur dient zodanig te zijn ontworpen en geïmplementeerd dat grootschalige uitval ervan (door onbeschikbaarheid of compromittering) niet kan leiden tot uitval of onbeheersbaarheid van het object, of waardoor onacceptabele risico's ontstaan;
z. IoT apparaten kunnen zelfstandig herstellen van tijdelijke uitval van netwerkfunctionaliteit en/of stroomuitval en hun functie hervatten;
aa. Het is op eenvoudige en gedocumenteerde wijze mogelijk om (vertrouwelijke of persoonlijke) informatie van het IoT apparaat te verwijderen;

bb. Secure setup en validatie daarvan is gedocumenteerd;
cc. Er is een Coordinated Vulnerability Disclosure (CVD) policy voor de IoT apparatuur;
dd. Alle security parameters dienen op een veilige en versleutelde wijze te worden opgeslagen op het apparaat.

Bijlage CSR 7 Wachtwoorden

CSR 7.1 Doelstelling

Wachtwoorden zijn een essentiële authenticatiemethode om personen, assets of processen toegang te geven tot die functionaliteit en gegevens die noodzakelijk zijn voor het uitvoeren van de beoogde functie, alsook om deze te beschermen tegen oneigenlijk gebruik door anderen. In deze richtlijn zijn de minimale best practices opgenomen, die binnen Rijkswaterstaat gelden voor het gebruik, wijzigen en beschermen van wachtwoorden in IA systemen.

Met de steeds verder toenemende rekenkracht van computers is het van belang dat wachtwoorden complex genoeg zijn en blijven, om weerbaar te blijven tegen tools om wachtwoorden te kraken. Het gebruik van sterke wachtwoorden met een voldoende complexiteit maakt het economisch onrendabel en praktisch onhaalbaar om wachtwoorden binnen de IA-omgeving van objecten te achterhalen.

Het is van groot belang dat Opdrachtnemers in lijn werken met de minimale vereisten voor wachtwoordcomplexiteit en ervoor zorgen dat de complexiteit van alle gebruikte wachtwoorden met de tijd meegaat.

CSR 7.2 Best practice

CSR 7.2.1 Vereisten aan wachtwoorden

Aan wachtwoorden voor alle gebruikers (zowel personen als processen) worden eisen gesteld m.b.t. lengte, complexiteit, geldigheidsduur en hergebruik:

a. Wachtwoorden hebben een minimale lengte, passend bij het soort account;
b. Wachtwoorden hebben een minimale complexiteit (verplichte karakterset) waaruit het wachtwoord moet bestaan:
    i. Hoofdletters;
    ii. Kleine letters;
    iii. Cijfers;
    iv. Speciale karakters, bijvoorbeeld: “;’:<>,.?!@#$%&*()+=_-^/\;
c. Wachtwoorden hebben een maximale geldigheidsduur;
d. Wachtwoorden kunnen niet worden hergebruikt.

Deze eisen zijn afhankelijk van het soort gebruikersaccount en gebruik. In algemeenheid geldt: hoe meer rechten aan een account zijn toegekend, hoe zwaarder de eisen.

De volgende zaken dienen niet te worden opgenomen in, of onderdeel uit te maken van, wachtwoorden:

a. Namen van familieleden, huisdieren, vrienden, collega’s, stripfiguren, etc.;
b. Computernamen en -termen, commando’s, naam van de software of hardware, naam van het bedrijf dat het heeft geleverd;
c. Woorden verwijzend naar organisatie, object of locatie, bijvoorbeeld: Rijkswaterstaat, Amaliasluis, Rotterdam;
d. Geboortedata en andere persoonlijke informatie als adres en telefoonnummers;
e. Eén van de voorafgaande woordsoorten, gevolgd door een getal (bijvoorbeeld: geheim01, welkom123, GuustFlater13, etc.).

CSR 7.2.2 Gegevensversleuteling

Voor versleuteling van gegevens t.b.v. gegevensuitwisseling dienen wachtwoorden te voldoen aan:

a. Wachtwoordlengte: minimaal 8 karakters;
b. Wachtwoord complexiteit: combinatie van hoofdletters, kleine letters, cijfers en leestekens, tenminste 2 van elk.

CSR 7.2.3 Soorten accounts

Voor de IA-omgeving van objecten worden verschillende accounts onderkend, met elk hun eigen vereisten voor wachtwoordgebruik.

Standaardaccount fabrikant: Standaard accounts en -wachtwoorden die toegepast worden in ICT- en IA-producten van fabrikanten mogen niet worden gebruikt en dienen te zijn uitgeschakeld.

SCADA-Operatoraccount
Een persoonlijk account dat wordt gebruikt voor de bediening van SCADA systemen
Soort: persoonsgebonden (terug te herleiden naar een individu)
Wachtwoord vervanging: 180 dagen
Wachtwoordlengte: minimaal 20 karakters
Wachtwoord complexiteit: combinatie van hoofdletters, kleine letters, cijfers en leestekens, tenminste 2 van elk.

SCADA-applicatiebeheeraccount
Een persoonlijk account dat wordt gebruikt om de applicatie op het SCADA systeem te beheren
Soort: persoonsgebonden (terug te herleiden naar een individu)
Wachtwoord vervanging: 180 dagen
Wachtwoordlengte: minimaal 20 karakters
Wachtwoord complexiteit: combinatie van hoofdletters, kleine letters, cijfers en leestekens, tenminste 2 van elk.

SCADA-Systeemaccount (service/applicatie account)
Een account dat ervoor zorg draagt dat een applicatie zonder menselijke interventie applicatieopdrachten kan uitvoeren onder speciale rechten.
Soort: service
Wachtwoord vervanging: 365 dagen
Wachtwoordlengte: minimaal 20 karakters
Wachtwoord complexiteit: combinatie van hoofdletters, kleine letters, cijfers en leestekens, tenminste 2 van elk.

SCADA-Administratoraccount
Een persoonlijk account dat op de systemen volledig beheer heeft d.m.v. administrator rechten.
Soort: persoonsgebonden (terug te herleiden naar een individu)
Wachtwoord vervanging: 180 dagen
Wachtwoordlengte: minimaal 20 karakters
Wachtwoord complexiteit: combinatie van hoofdletters, kleine letters, cijfers en leestekens, tenminste 2 van elk.

Kantoorautomatiseringsaccount (KA-account)
Het persoonlijke gebruikers account waarmee men kan werken op de Rijkswaterstaat Kantoorautomatiseringsomgeving.
Soort: persoonsgebonden (terug te herleiden naar een individu)
Wachtwoord vervanging: 90 dagen
Wachtwoordlengte: minimaal 8 karakters
Wachtwoord complexiteit: combinatie van hoofdletters, kleine letters, cijfers en leestekens, tenminste 1 van elk.

CSR 7.2.4 Tips voor het omgaan met wachtwoorden
Enkele tips:

a. Gebruik een wachtwoord dat is gebaseerd op een zin, een songtekst of een rijmpje. Zet de eerste letters van ieder woord achterelkaar, en probeer letters door cijfers te vervangen (Bijvoorbeeld: Het rijmpje “Als het regent in mei is april voorbij en leggen alle vogels een ei!” wordt “Ahri5i4velavee!”, waarbij de maanden zijn vervangen door cijfers).
b. Gebruik een zin (passphrase) in plaats van een wachtwoord (password). Typ de woorden van een makkelijke zin achterelkaar en vervang woorden of letters door hoofdletters, getallen of lettertekens (Bijvoorbeeld: 3KleineKleutertjesdiezatenopeen###).
c. Gebruik een elektronische wachtwoordkluis die speciaal voor dit doel is ontwikkeld. Binnen RWS is Keepass 2 een goedgekeurde wachtwoordkluis. Enkele andere voorbeelden van veelgebruikte wachtwoordkluizen zijn Roboform, Dashlane, LastPass.

d. Als een wachtwoord in een elektronische wachtwoordkluis wordt opgeslagen, dan is een wachtwoord nodig om die applicatie te openen. Daarvoor geldt dezelfde wachtwoordrichtlijn voor het meest complexe opgeslagen wachtwoord in de kluis.
e. Gebruik voor je bedrijfs-account niet hetzelfde wachtwoord als voor je privéaccounts (bijvoorbeeld: persoonlijke gmail, facebook, ANWB site, bol.com, etc.).
f. Gebruik binnen het bedrijf niet overal hetzelfde wachtwoord. Gebruik een verschillend wachtwoord voor je gewone desktopomgeving, je bedienplek of je yammer account.
g. Deel je wachtwoord met niemand, tenzij dit is vereist volgens de procedures.
h. Wachtwoorden mogen nooit worden opgeschreven of digitaal worden opgeslagen zonder te zijn vercijferd.
i. Schrijf nooit een wachtwoord in e-mail, chat of ander communicatiemiddel.
j. Praat niet over je wachtwoord, geef geen hints over je wachtwoord aan anderen.
k. Indien een wachtwoord fysiek moet worden opgeslagen (bijvoorbeeld, omdat dat volgens een veiligheidsprocedure moet), sla het wachtwoord dan op in een fysieke kluis. Zorg er dan voor dat de sleutel niet eenvoudig te vinden is of dat de kluis op een andere locatie staat.

CSR 7.2.5 Wijzigen van wachtwoorden

Als het wijzigen van wachtwoorden niet automatisch wordt afgedwongen, zorg dan dat het procedureel wordt afgedwongen. Dit kan simpelweg door zelf (bijvoorbeeld op de eerste maandag van de maand) het wachtwoord te wijzigen en dit vast te leggen in een korte procedure.

Bijlage CSR 8 Patch management

CSR 8.1 Doelstelling

Vrijwel alle apparatuur aanwezig op een object heeft te maken met software en/of firmware. Om het aantal kwetsbaarheden in deze apparatuur tot een minimum beperkt te houden, is het van belang om de software en firmware up-to-date te houden en regelmatig te patchen. Deze richtlijn helpt Opdrachtnemers een effectief patch management regime op te stellen en te volgen, waarbij aandacht is voor de risicobeoordeling van de patch op de functies van het object en daarmee ook de business impact voor het (al dan niet) uitvoeren van patches.

CSR 8.2 Best practice

CSR 8.2.1 Bepalen van uit te rollen patches

Opdrachtnemers kunnen tenminste de volgende zaken in hun patch management procedures opnemen, om te bepalen welke patches relevant zijn voor het object en uitgerold dienen te worden:

a. Inventariseer voor het object welke software en firmware er op elk apparaat draait en neem dit op in het (bij voorkeur centrale) CMDB;
b. Houd bij welke kwetsbaarheden er zijn en worden ontdekt voor de systemen die in gebruik zijn. Beoordeel de risico's van de kwetsbaarheden voor het object (zie paragraaf CSR 8.2.2);
c. Houd bij welke patches er uitkomen voor alle apparaten en controleer welke relevant zijn. Indien patches een invloed kunnen hebben op de werking van (b.v. SCADA-) software, houdt bij welke patches zijn goedgekeurd door de leverancier;
d. Maak een alternatief mitigatievoorstel indien besloten wordt om een specifieke patch niet te installeren; Bepaal de risico's die overblijven indien wordt gekozen voor de alternatieve migratie;
e. Houd voor beheer en onderhoud een lijst bij met alle te installeren patches en de systemen waarop dit dient te gebeuren.

CSR 8.2.2 Risicobeoordeling

Zolang een kwetsbaarheid niet is verholpen door installatie van een patch of door een andere vorm van mitigatie, is er kans op misbruik van de kwetsbaarheid. Het risico hierop dient te worden bepaald. Dit gebeurt middels een risicobeoordeling. Hierbij worden kans en impact beschouwd.

Kans

De kans dat een kwetsbaarheid wordt uitgebuit is afhankelijk van de blootstelling van de kwetsbaarheid en de uitvoerbaarheid van het exploiteren van de kwetsbaarheid.

De kans dat de kwetsbaarheid wordt uitgebuit		Omschrijving kans en daarmee het benutten van de kwetsbaarheid
1	Verwaarloosbaar *t > 5 jaar*	De kans en daarmee het falen of misbruik van de functie van het object wordt niet binnen 5 jaar verwacht.
2	Klein (*3 jaar < t ≤* 5 *jaar*)	De kans en daarmee het falen of misbruik van de functie van het object wordt tussen 3 jaar en 5 jaar na nu verwacht.
3	Middelmatig (2 *jaar < t ≤ 3 jaar)*	De kans en daarmee het falen of misbruik van de functie van het object wordt tussen 2 jaar en 3 jaar na nu verwacht.
4	Groot (1 jaar < *t ≤ 2 jaar*)	De kans en daarmee het falen of misbruik van de functie van het object wordt tussen 1 jaar en 2 jaar na nu verwacht.
5	Zeker (*t ≤ 1 jaar)*	De kans en daarmee het falen of misbruik van de functie van het object wordt tussen nu en 1 jaar verwacht.

Impact

Indien de kwetsbaarheid wordt uitgebuit dan heeft dit een bepaalde impact op het object. Deze impact dient te worden bepaald op basis van consequenties. Deze consequenties kunnen in verschillende categorieën van RAMSSHEEP liggen. De mee te nemen consequentiecategorieën zijn mede afhankelijk van het object. De categorie met de grootste impact consequentie wordt overgenomen voor de risicomatrix en bepaalt uiteindelijk samen met de kans het risico die in de risicomatrix wordt weergegeven voor het object.

RAMSSHEEP

- R: Reliability (Betrouwbaarheid)
- A: Availability (Beschikbaarheid)
- M: Maintainability (Onderhoudbaarheid)
- S: Safety (veiligheid)
- Se: Security (Beveiliging)
- H: Health (Gezondheid)
- E: Environment (Omgeving en Milieu)
- €: Economics (Levensduurkosten)
- P: Politics (Politiek)

	Impact			
	Verwaarloosbaar (1)	Beperkt (2)	Groot (3)	Ernstig (4)
R	Het niet patchen leidt tot een niet compliancy registratie en rapportage en heeft negatieve invloed op de betrouwbaarheid van het betreffend object maar heeft een verwaarloosbare invloed op de hoofdfunctie.	Het niet patchen leidt tot een niet compliancy registratie en rapportage en heeft negatieve invloed op de betrouwbaarheid van het betreffende object en heeft een minimale negatieve invloed op de hoofdfunctie.	Het niet patchen leidt tot een niet compliancy registratie en rapportage en heeft negatieve invloed op de betrouwbaarheid van het betreffend object en heeft ernstige negatieve invloed op de hoofdfunctie.	Het niet patchen leidt tot een niet compliancy registratie en rapportage en heeft negatieve invloed op de betrouwbaarheid van het betreffend object en heeft catastrofale negatieve invloed op de hoofdfunctie.
A	Het niet patchen leidt tot een niet compliancy registratie en rapportage en heeft negatieve invloed op de beschikbaarheid van het betreffend object maar heeft een verwaarloosbare invloed op de hoofdfunctie.	Het niet patchen leidt tot een niet compliancy registratie en rapportage en heeft negatieve invloed op de beschikbaarheid van het betreffend object maar heeft een minimale invloed op de hoofdfunctie.	Het niet patchen leidt tot een niet compliancy registratie en rapportage en heeft negatieve invloed op de beschikbaarheid van het betreffend object en heeft ernstige negatieve invloed op de hoofdfunctie.	Het niet patchen leidt tot een niet compliancy registratie en rapportage en heeft negatieve invloed op de beschikbaarheid van het betreffend object en heeft catastrofale negatieve invloed op de hoofdfunctie.
M	Het niet patchen leidt tot een niet compliancy registratie en rapportage en maakt dat onderhoud in een later stadium verwaarloosbaar moelijker uitgevoerd kan worden binnen de randvoorwaarden van gebruik.	Het niet patchen leidt tot een niet compliancy registratie en rapportage en maakt dat onderhoud in een later stadium minimaal moeilijker uitgevoerd kan worden binnen de randvoorwaarden van het gebruik.	Het niet patchen leidt tot een niet compliancy registratie en rapportage en maakt dat onderhoud in een later stadium niet uitgevoerd kan worden binnen de randvoorwaarden van gebruik, hetgeen ernstige negatieve invloed heeft op de prestaties van de netwerkschakel.	Het niet patchen leidt tot een niet compliancy registratie en rapportage en maakt dat onderhoud in een later stadium niet uitgevoerd kan worden binnen de randvoorwaarden van gebruik, hetgeen catastrofale negatieve invloed heeft op de prestaties van de netwerkschakel.
S	Het niet patchen leidt tot een niet compliancy registratie en rapportage en	Het niet patchen leidt tot een niet compliancy registratie en rapportage en	Het niet patchen leidt tot een niet compliancy registratie en rapportage en leidt	Het niet patchen leidt tot een niet compliancy registratie en rapportage en

	Impact			
	Verwaarloosbaar (1)	Beperkt (2)	Groot (3)	Ernstig (4)
	heeft een verwaarloosbare invloed op gebruiksveiligheid van het object, maar dit blijft binnen geaccepteerde grenzen.	leidt tot een situatie die de geaccepteerde grenzen voor gebruiksveiligheid benaderd en leidt daardoor tot een minimaal aantal extra ongelukken met tijdelijke gezondheidsschade of letsel zonder verzuim.	tot het niet voldoen aan gestelde eisen ten aanzien van gebruiksveiligheid wat daardoor leidt tot een ernstige toename van het aantal ongelukken met blijvend letsel of met blijvende gezondheidsschade.	heeft een catastrofaal negatief effect op de gebruiksveiligheid wat leidt tot extra dodelijk gevaar bij normaal gebruik.
Se	Het niet patchen leidt tot een niet compliancy registratie en rapportage en heeft negatieve invloed op de fysieke en of logische toegangsbeveiliging van het betreffende object maar heeft een minimale invloed op de hoofdfunctie.	Het niet patchen leidt tot een niet compliancy registratie en rapportage en heeft negatieve invloed op de fysieke en of logische toegangsbeveiliging van het betreffende object en heeft een minimale negatieve invloed op de hoofdfunctie.	Het niet patchen leidt tot een niet compliancy registratie en rapportage en heeft negatieve invloed op de fysieke en of logische toegangsbeveiliging van het betreffend object die tot security incidenten leiden en heeft hiernaast ernstige negatieve invloed op de hoofdfunctie.	Het niet patchen leidt tot een niet compliancy registratie en rapportage en heeft negatieve invloed op de fysieke en of logische toegangsbeveiliging van het betreffende object die tot security incidenten leiden en heeft hiernaast catastrofale negatieve invloed op de hoofdfunctie en of de prestaties van de netwerkschakel.
H	Het niet patchen heeft een verwaarloosbare negatieve invloed op de gezondheid.	Het niet patchen heeft een minimale negatieve invloed op de gezondheid.	Het niet patchen heeft een ernstige negatieve invloed op de gezondheid.	Het niet patchen heeft een catastrofale negatieve invloed op de gezondheid en veroorzaakt overlijden.
E	Het niet patchen heeft een verwaarloosbaar negatief effect op het gebruik.	Het niet patchen heeft een beperkt negatief effect op het gebruik en beperkt zich tot consequenties voor het lokale netwerk.	Het niet patchen maatregel heeft een ernstig negatief effect op het gebruik en heeft consequenties voor het regionale netwerk.	Het niet patchen heeft een catastrofaal negatief effect op het gebruik en heeft consequenties voor het landelijke netwerk.
€	Uitstel patch geeft < 50 k Euro aan extra onderhoudskosten	Uitstel patch geeft < 500 k Euro aan extra onderhoudskosten	Uitstel patch geeft < 1000 k Euro aan extra onderhoudskosten.	Uitstel patch geeft > 1000 k Euro aan extra onderhoudskosten
P	Het niet patchen leidt tot een niet compliancy registratie en rapportage en heeft verder geen politieke consequenties.	Het niet patchen leidt tot een niet compliancy registratie en rapportage en is mogelijk aanleiding voor verscherpte controles door toezichthouders.	Het niet patchen leidt tot een niet compliancy registratie en rapportage en is mogelijk aanleiding voor negatieve media berichtgeving die tot kamer vragen kunnen leiden.	Het niet patchen leidt tot een niet compliancy registratie en rapportage en de positie van DG, de Minister of Staatssecretaris staat ter discussie.

Risico
Het uiteindelijke risico wordt gepaald door het combineren van kans en impact in een risicomatrix.

		Impact			
		Verwaarloosbaar (1)	Beperkt (2)	Groot (3)	Ernstig (4)
Kans	Verwaarloosbaar (1)	Acceptabel (1)	Acceptabel (2)	Acceptabel (3)	Acceptabel (4)
	Klein (2)	Acceptabel (2)	Acceptabel (4)	Ongewenst (6)	Ongewenst (8)
	Gemiddeld (3)	Acceptabel (3)	Ongewenst (6)	Ongewenst (9)	Ongewenst (12)
	Groot (4)	Acceptabel (4)	Ongewenst (8)	Ongewenst (12)	Onacceptabel (16)
	Zeker (5)	Ongewenst (5)	Ongewenst (10)	Onacceptabel (15)	Onacceptabel (20)

De risicoscore wordt eenvoudig bepaald door kans- en impactscore met elkaar te vermenigvuldigen. De hoogte van dit getal geeft aan hoe noodzakelijk een beheersmaatregel in de vorm van een patch is. Hierin worden drie niveaus onderscheiden: onacceptabel (rood), ongewenst (oranje) of acceptabel (groen).

1. Onacceptabel — Risicoscore 15 t/m 20
Er moeten direct beheersmaatregelen worden getroffen om het risico te beheersen. Dat kan door de patch zo snel mogelijk te implementeren of minimaal (tijdelijk) compenserende maatregelen te treffen.
2. Ongewenst — Risicoscore 5 t/m 12
De patch moet worden doorgevoerd om het risico te beheersen ofwel worden aangetoond waarom dit nu niet haalbaar/noodzakelijk is. Een planning voor het doorvoeren van de patch is vereist naast tijdelijke compenserende maatregelen om zolang het risico te reduceren.
3. Acceptabel — Risicoscore 1 t/m 4
De patch hoeft niet direct doorgevoerd te worden en kan gewoon worden doorgevoerd binnen het geplande reguliere onderhoudsmoment van de systemen.

CSR 8.2.3 Inplannen van patches
Afhankelijk van de urgentie van de patches, kunnen deze tijdens regulier periodiek onderhoud worden geïnstalleerd. Hiertoe dient instructie te worden gegeven aan de monteur van Opdrachtnemer. Het is soms noodzakelijk apparatuur opnieuw op te starten na installatie van patches. Tijdens zulke herstarts is het mogelijk dat het object niet kan worden bediend. Inplannen van patches dient dan ook altijd te gebeuren in overleg met RWS.

CSR 8.2.4 Testen van patches
Om te voorkomen dat de uitrol van patches problemen geeft op het object, dienen patches vooraf te worden getest op werking en integriteit. Bij voorkeur gebeurt dit in een OTA-omgeving. Uitsluitend patches die dienen te worden geïnstalleerd dienen te worden getest.

CSR 8.2.5 Verantwoord uitrollen van ingeplande en geteste patches
Plan voor roll-back bij falende patches
a. Opdrachtnemer dient ervoor te zorgen dat er altijd en goed werkende back-up is, waarop kan worden teruggevallen indien een patch problemen geeft na installatie;
b. Opdrachtnemer kan overwegen een extra back-up te maken vlak voordat patches worden geïnstalleerd;
c. Opdrachtnemer dient gedurende de geplande onderhoudswerkzaamheden tijd te reserveren voor een eventuele roll-back van back-up op apparatuur.

Controleren of patches succesvol zijn uitgerold
a. Opdrachtnemer dient na de uitrol van de patch te controleren of de uitrol is geslaagd en goed is afgerond;
b. Indien de patch succesvol is uitgerold, dient Opdrachtnemer te controleren of de werking van het object niet is aangetast en of alle toepassingen nog functioneren als verwacht.

Controleren of systeem hardening niet is aangetast

a. Tot slot dient Opdrachtnemer te controleren of de mate van systeem hardening niet is aangetast door het installeren van de patch. Bijvoorbeeld:
    i. Zijn afgesloten poorten niet opengezet;
    ii. Zijn uitgeschakelde of verwijderde programma's en/of DLL's niet terug geïnstalleerd en geactiveerd;
b. Indien de hardening is aangetast, dient het niveau van hardening te worden hersteld.

Bijlage CSR 9 Hardening

CSR 9.1 Doelstelling

Hardening betreft het verwijderen of uitschakelen van overbodige en/of ongebruikte functionaliteit van een apparaat en is van toepassing op software, hardware en netwerk. Hardening zorgt ervoor dat systemen minder kwetsbaar zijn voor malware en minder snel gecompromitteerd kunnen worden. Hardening wordt toegepast op zowel IT als IA componenten.

Er worden drie methoden van hardening toegepast, te weten software hardening, hardware hardening en netwerk hardening:

a. Software hardening is van toepassing op operating systemen (bijvoorbeeld Microsoft Windows, Linux, iOS, Android) en applicaties (bijvoorbeeld HMI of engineering software, configuratietools, maar ook MS Office, Acrobat reader, Active-X controls en Adobe Flash);
b. Hardware hardening is van toepassing op bijvoorbeeld firmware, alsook het uitschakelen van niet gebruikte communicatiepoorten, antennes, en overige niet gebruikte functionaliteit;
c. Netwerk (Process Control Network) hardening is van toepassing op bijvoorbeeld uitschakelen van onveilige en niet gebruikte protocollen, het beperken van netwerkverkeer (firewalls) en segmentatie/zonering van het netwerk.

Maak indien mogelijk gebruik van de aanwezig security opties van de fabrikant/leverancier.

CSR 9.2 Best practices

CSR 9.2.1 Basistips

Enkele basistips voor hardening zijn:

a. Software
    i. Operating System;
        - De operationele OS versie dient altijd te worden ondersteund door de OS leverancier;
        - Gebruik waar mogelijk de nieuwste (mogelijke) versie[3];
        - Installeer de laatste (mogelijke) patches[1];
        - Schakel niet-gebruikte system services uit of verwijder deze[4];
    ii. Virtualization layer;
        - Gebruik de nieuwste (mogelijke) versie[1]; Deze versie dient wel te worden ondersteund door de softwareleverancier;
        - Installeer de laatste (mogelijke) patches[1];
        - Schakel niet-gebruikte functionaliteit uit of verwijder deze;
    iii. Applicaties
        - Verwijder alle niet noodzakelijke applicaties;
        - Installeer de nieuwste versie van applicaties[1]; Deze versie dient wel te worden ondersteund door de softwareleverancier;
        - Installeer de laatste (mogelijke) patches[1];
        - Zorg voor secure coding tijdens ontwikkeling van eigen software[5];
    iv. Firmware
        - Installeer de laatste (mogelijke) firmware[1];
b. Hardware
    v. Schakel niet-gebruikte poorten uit
        - Gebruik portblockers als niet-gebruikte poorten niet kunnen worden uitgeschakeld om abusievelijk gebruik te voorkomen en tamper-evident stickers (void stickers) om manipulatie te detecteren;

[3] Download alleen van gevalideerde vendorlocaties en controleer de integriteit van downloads middels een checksum.
[4] Zie ook Hardeningprofielen zoals hierna behandeld.
[5] Zie SSD document van CIP

- Beperk de gebruiksmogelijkheden van de nog openstaande poorten (bv. USB alleen voor hid (muis/keyboard)); Gebruik tamper-evident stickers (void stickers) om manipulatie te detecteren;

vi. Schakel niet noodzakelijke draadloze toegang uit (bv. WiFi, Bluetooth, IR, NFC, 4G, 5G, LoRa);

vii. Schakel niet gebruikte functionaliteit uit en verwijder deze waar mogelijk (bv. ingebouwde 4G/5G modem, antennes, I/O);

c. Netwerk

viii. Schakel niet-noodzakelijke communicatieprotocollen uit (bv. FTP, SMB, telnet);

ix. Pas netwerksegmentatie toe. Scheidt hierbij essentiële delen voor de besturing van niet essentiële delen;

x. Beperkt netwerkverkeer tussen verschillende netwerkzones middels firewalls.

CSR 9.2.2 Hardening-profielen

Op Internet zijn de nodige hulpmiddelen te vinden ter ondersteuning van het hardening-proces. Hardening (en tooling daarvoor) kan en mag alleen ingezet worden wanneer met zekerheid gesteld kan worden dat de inzet hiervan geen risico vormt voor de continuïteit van werking van het systeem. Het is van belang dit zowel vooraf als achteraf te testen.

Enkele van deze hulpmiddelen zijn:

CIS

De 'Security Benchmarks' van CIS heeft op internet standaard hardening-profielen beschikbaar voor de meeste platformen: http://www.cisecurity.org/

CIS Benchmarks: https://www.cisecurity.org/cybersecurity-best-practices/

Microsoft

Microsoft Security Baselines (Security Compliance Toolkit - SCT): https://docs.microsoft.com/en-us/windows/security/threat-protection/security-compliance-toolkit-10

Microsoft Baseline Security Analyzer (MBSA): https://www.microsoft.com/en-us/download/details.aspx?id=19892

Defense Information System Agency (DISA)

Security Technical Implementation Guides (STIGs): https://public.cyber.mil/stigs/downloads/

Bijlage CSR 10 Logging

CSR 10.1 Doelstelling

Vanuit de BIO is logging vereist, waarbij de nadruk ligt op het vastleggen van gebruikershandelingen binnen applicaties, t.b.v. auditing. Deze logvereisten zijn vertaald naar logging voor IA systemen, waarbij de nadruk ligt op het systeemgedrag en –activiteiten. Logging binnen de IA-omgeving heeft dan ook meer betrekking op het waarborgen van beschikbaarheid en integriteit van de IA, door:

a. Het verzamelen, analyseren en reageren op status info van de ICT en ISC/SCADA deelsystemen binnen de IA;
b. Het ontdekken van menselijke fouten of systeem fouten, zoals fouten bij de bediening, maar ook het ontdekken van indringers in systemen;
c. Het ontdekken van corruptie van data of programmatuur;
d. Het ondersteunen van onderzoek na een incident.

CSR 10.2 Best practice

De volgende maatregelen sluiten aan bij de doelstelling van logging van IA systemen:

a. Een syslog server inrichten die de syslog events vanuit de gelaagd opgebouwde objectnetwerk verzamelt en toegankelijk maakt voor analysedoeleinden en automatische waarschuwingen;
b. De syslogserver wordt voorzien van malware protectie, hardening en logging van de activiteiten op de server zelf (toegang, config/systeemaanpassingen en kopieer acties);
c. De syslogserver en syslog database is alleen toegankelijk voor geautoriseerden;
d. De syslog database kan niet gewijzigd of vernietigd worden door beheerders;
e. Het openen van een nieuw logbestand maar ook het verwijderen ervan dient te worden gelogd;
f. De bewaartermijn van de syslog database moet instelbaar zijn met een minimum van een maand;
g. Op aangeven van Opdrachtgever wordt de syslog database langer bewaard;
h. De syslog database dient zodanig ingericht te worden dat deze via het RWS netwerk toegankelijk is voor het Security Operations Centre van RWS;
i. De ICT en ICS/SCADA systemen die ingezet worden voor het object dienen de syslog gebeurtenissen door te geven aan de syslogserver voor vastlegging in de syslog database;
j. Het ICT of ICS/SCADA deelsysteem binnen de IA dat de logregel veroorzaakt staat vaak niet in de logregel zelf, in dat geval moet de syslog server deze toevoegen aan de opgenomen logregel;
k. Om meldingen goed te kunnen correleren is het essentieel dat tijdsynchronisatie (NTP) is ingericht. Hiervoor dient de interne tijdserver te worden gebruikt. Niet alleen de logserver dient te worden geconfigureerd op een tijdserver, maar ook alle aangesloten componenten zoals PLC's welke logregels genereren op de logserver;
l. Indien mogelijk dient Transport Layer Security (TLS) via TCP op poort 6514 gebruikt te worden (RFC 5425). Indien dit niet mogelijk is omdat de gebruikte apparatuur dit niet ondersteunt, kan gebruik gemaakt worden van UDP port 514 voor transmissie naar de logserver;
m. Voor zover de ICT en ICS/SCADA systeemcomponenten hierin voorzien dienen de volgende events aangeleverd te worden aan de syslogserver:

Event:	Omschrijving:
Log In	Succesvolle login (lokaal of op afstand)
Manual Log Out	Gebruiker logt zelf uit
Timed Log Out	Uitloggen door voor-ingestelde tijd (time-out)
Value Forcing	Handmatig aangepaste waarde (overschrijving)
Configuration Access	Download van de PLC configuratie naar datadrager
Configuration Change	Upload van de PLC configuratie naar de PLC
Firmware Change	Nieuwe firmware installatie op de PLC
ID/Password Creation or Modification	Creatie of modificatie van een gebruiker of wachtwoord

Event:	Omschrijving:
ID/Password Deletion	Wissen van een gebruiker en wachtwoord in de PLC
Audit Log Access	Toegang tot de logbestanden in de PLC
Time/Date Change	Datum/Tijd aanpassing van de PLC
Unsuccessful Login Attempt	Onjuiste inlog poging op de PLC
Reboot	Herstart van de PLC
Attempted Use of Unauthorized Configuration Software	Ongeautoriseerde poging tot toegang van de PLC configuratie
Invalid Configuration or Firmware Download	Ongeldige configuratie of firmware download
Unauthorized Configuration or Firmware File	Ongeautoriseerde configuratie of firmware bestand
Unexpected Time Signal Out of Tolerance	Onverwachte tijd/datum wijziging
Invalid Field Hardware Changes	Ongeldige hardware aangesloten

n. Het aanleverformaat voor de syslogserver is:
<timestamp> <IP> <Host> <facility> <Severity level> <message>

Voorbeeld:
<Oct 14 2015 22:09:12> <10.1.2.40> <123> <auth> <Alert> <Attempted Use of Unauthorized Configuration Software>

waarbij:

i. <timestamp> bij default tijd in het formaat ‘date "+%b %d %Y %H:%M:%S"’, zoals hierboven;
ii. <IP> IP adres van het device, bijvoorbeeld 10.1.2.40;
iii. <Host> hostnaam of ID van het busdevice, in dit voorbeeld “123” in geval van een computer de hostnaam van de computer;
iv. <facility> soort log gebeurtenis, bijvoorbeeld: kern, user, auth, syslog;
v. <Severity level> bijvoorbeeld Emergency, Alert, Critical, Error, Warning;
vi. <message> het syslog bericht, bijvoorbeeld: Attempted Use of Unauthorized Configuration Software;

Bijlage CSR 11 Malware scanning en opschoning middels een USB

CSR 11.1 Doelstelling

Malware besmettingen zijn vandaag de dag niet meer uit te sluiten. Derhalve worden voor de bescherming van ICT en IA systemen tegen malware oplossingen gevraagd. Bij nieuwbouw systemen dient vanaf het ontwerp hier voldoende aandacht en uitwerking aan gegeven te worden. Echter de maatregelen voor de detectie van en preventie tegen malware kunnen bij de ontwerpkeuzes dilemma's opleveren. In die situaties dient contact en afstemming gezocht te worden met de Opdrachtgever voor de uiteindelijke keuze. Ook kunnen er bestaande omgevingen zijn waar (nog) geen antimalware voorzieningen op de ICT en IA systemen zijn getroffen maar waar u meer zekerheid wilt verkrijgen over eventuele aanwezigheid van malware.

Het is van belang dat in deze gevallen malware gedetecteerd en opgeschoond kan worden, door medewerkers die beheer- en onderhoudswerkzaamheden uitvoeren aan ICT en IA systemen.

CSR 11.2 Best practice

CSR 11.2.1 Randvoorwaarden

Een risico bij malware scanning en opschoning is dat wanneer er daadwerkelijk een besmetting heeft plaatsgevonden u niet vooraf weet in welke mate (of met welk soort malware) de computers zijn besmet. Het installeren van een conventionele antivirus oplossing brengt een nieuw risico met zich mee, indien de antivirus software een besmet bestand aantreft op de computer zullen de meeste antivirus software oplossingen (bij standaardinstellingen) deze bestanden proberen op te schonen, in quarantaine te plaatsen of te verwijderen. Dit is uiteraard onwenselijk aangezien de besmette bestanden mogelijk vitaal zijn of noodzakelijk voor de juiste werking voor de bediening van het object.

Randvoorwaarde is dat de ingezette oplossing voor malware scanning zo ingesteld wordt dat het alleen detecteert en rapporteert. Er mag niets verwijderd worden.

De volgende paragrafen schetsen een goede manier om het scannen aan te pakken.

CSR 11.2.2 Voorbereiden USB-stick met antimalware software

a. Gebruik bij voorkeur een nieuwe USB stick waar de malwarescan software op geïnstalleerd gaat worden;
b. Als extra beveiliging voor de USB-stick met antimalware software dient bij voorkeur een USB stick met schrijfbeveiliging (of een SD-kaart met schrijfbeveiliging, in combinatie met een SD-kaart lezer) gebruikt te worden. Door de schrijfbeveiliging te activeren voordat de USB-stick in het besmette systeem geplaatst wordt, wordt besmetting van de USB-stick voorkomen;
c. Scan de USB stick voor elk gebruik op een computer buiten het object met een actuele malwarescan software;
d. De USB-stick moet voor elk gebruik voorzien worden van de juiste –en meest actuele- antimalware software en malwaredefinities.

Een voorbeeld van een dergelijke antimalware software is de vrij verkrijgbare software van ClamAV welke als portable applicatie kan worden geïnstalleerd op een USB stick en kan worden voorzien van updates op een andere computer.
Voor Windows computers kunt u bijvoorbeeld de nieuwste versie van ClamWin downloaden via http://nl.clamwin.com/ (Voor Linux computers is deze via de website http://www.clamav.net/ verkrijgbaar).

Installeer de software via het installatie programma op een USB stick en na dat de software is voorzien van de laatste versie antivirus definities kan de USB stick gebruikt worden op de object computers welke niet zijn aangesloten op internet.

Standaard staat ClamWin zo ingesteld dat een besmetting alleen zal worden gerapporteerd, indien u er zeker van bent dat een eventueel besmet bestand geen cruciale rol heeft voor de werking van het bedieningssysteem kunt u vanuit het programma het virus verwijderen.

Uiteraard kunnen ook andere antimalware programma's worden gebruikt, mits zo ingesteld dat besmettingen uitsluitend worden gerapporteerd en niet in quarantaine worden geplaatst.

Om er zeker van te zijn dat alle bestanden kunnen worden gescand is het noodzakelijk het scanprogramma met verhoogde rechten op te starten. In Windows is dit "Als administrator starten" of "Run as administrator" en in Linux als "Root" of "Sudo".

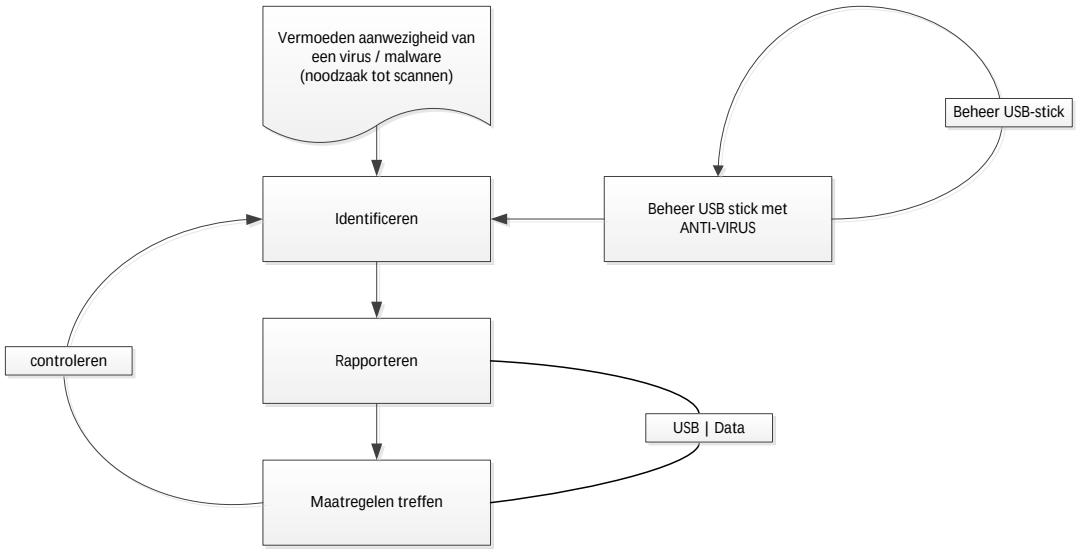
CSR 11.2.3 Voorbereiden op malwarescanning

Handel volgens onderstaande werkwijze:

a. Update de USB stick met de laatste antimalware software en laatst beschikbare malwaredefinities;
b. Scan de USB stick met antimalware software voor elk gebruik op een computer buiten het object met een actuele malwarescan software;
c. Zet op deze USB stick een malwarescan tool/software die uitsluitend een rapportage geeft over de besmetting zonder automatische handelingen;
d. Gebruik een malwarescanner welke geen verbinding met internet nodig heeft om op te kunnen starten (bijvoorbeeld i.v.m. licentie controle);
e. Gebruik een USB stick waar de antimalware software als een portable applicatie op kan worden geïnstalleerd;
f. De rapportage dient verzameld te worden op los media zoals een USB-stick. Gebruik hiervoor bij voorkeur een nieuwe andere stick dan die waarop de malwarescan software staat;
g. Scan de USB stick met antimalware software ook na elk gebruik op een computer buiten het object met een actuele malwarescan software.

CSR 11.2.4 Scannen en opschonen

In onderstaand schema wordt een bedoelde werkwijze getoond om een dergelijk object te schonen. Het proces kent de volgende stappen:



Identificeren

Gebruik de offline malwarescan tool om het systeem te controleren op virussen. Zorg voor correcte rapportage op een centrale plaats. Deze rapportage moet op een apart systeem weggeschreven worden, zodat het proces minimaal verstoord wordt.

Rapporteren

Verzamel de rapportage op aparte media zoals een USB-stick. Gebruik hiervoor bij voorkeur een nieuwe andere stick dan die waarop de malwarescan software staat.

Houdt ook bij de verzameling van rapportage rekening met voldoende controle op verwisselbare media: Bij plaatsen van een USB-stick in een besmet object is de kans op besmetting van de USB-stick reëel aanwezig. Herhaal hiertoe stap 6 van de instructie voorbereiding malwarescanning.

Maatregelen treffen

Bij constatering van malware dient in overleg met de objectbeheerder/eigenaar gekeken te worden naar mogelijke oplossingen voor het opschonen. Na autorisatie door de objectbeheer/eigenaar kunnen de te nemen stappen gepland en uitgevoerd worden. Houdt bij het treffen van de maatregelen weer rekening met de mogelijke besmetting van verwisselbare media. Extra aandachtspunt in dit geval is ook: Zorg dat de vervangen / vernieuwde bestanden (als daarvan sprake is) bij plaatsing niet besmet worden. Gebruik zo mogelijk checksums op bron en bestemming om de juistheid van de bestanden te controleren.

Controleren

Herhaal ter controle ten minste de eerste stap (Identificeren).

Bijlage CSR 12 Continuïteitsplan voor energievoorziening

CSR 12.1 Doelstelling

Het continuïteitsplan beschrijft per object de ingezette middelen voor continuïteit van de energievoorziening en acties die door de Opdrachtnemer moeten worden uitgevoerd om voorbereid te zijn op het herstel na stroomstoringen op objecten. In geval van omvangrijke stroomstoringen is het functioneren van de kritieke ICT en IA systemen geborgd.

De scope van het continuïteitsplan omvat alle kritieke ICT en IA systemen en de daarvoor benodigde energie voorzieningen die noodzakelijk zijn voor de functioneren en veilige werking van het object.

CSR 12.2 Best practice

Elk object heeft een eigen continuïteitsplan voor de energievoorziening. Een continuïteitsplan dient per object te worden opgesteld en tenminste het volgende te bevatten:

a. Risicoanalyse en afweging;
b. Overzicht van systemen, applicaties en services en back-up voorzieningen voor elektriciteit;
c. Overzicht van alle noodzakelijke systeemdocumentatie;
d. Organisatie en borging continuïteitsbeheer;
e. Periodieke beproeving en onderhoud van het continuïteitsplan voor energievoorziening.

Risicoanalyse en afweging

Een risicoanalyse en risicoafweging gebaseerd op de functionele kaders die door de Opdrachtgever zijn meegegeven en de ontwerpkeuzes die door de Opdrachtnemer zijn gemaakt, om de kritieke ICT en IA systemen, applicaties services en de benodigde back-up voorzieningen voor de daarvoor benodigde energievoorzieningen in beeld te brengen.

Overzicht van systemen, applicaties en services en back-up voorzieningen

Dit betreft een overzicht van alle kritieke ICT en IA systemen, applicaties en services die operationeel moeten blijven in het geval van uitval van de primaire energie voorzieningen (zoals elektriciteit).

Overzicht van alle noodzakelijke systeemdocumentatie

Dit betreft een overzicht van actuele documentatie die benodigd is voor de noodvoorzieningen voor energie (bijvoorbeeld aansluittekeningen, gebruikshandleiding en procedures voor schakelen tussen noodstroomvoorziening en reguliere stroomvoorziening). De documentatie dient zowel digitaal als in hardcopy op twee fysiek gescheiden locaties bewaard te worden, waarbij wordt voldaan aan de gestelde eisen voor het omgaan met vertrouwelijke informatie.

Organisatie en borging continuïteitsbeheer energievoorziening

Dit betreft een beschrijving van de wijze waarop het beheer en onderhoud van het continuïteitsplan is belegd in de (project)organisatie van de Opdrachtnemer. Tevens dient er een overzicht te zijn van rolhouders, hun bereikbaarheid en vervangers inclusief hun verantwoordelijkheden en bevoegdheden. Ook dient de afschaling te worden beschreven.

Periodieke beproeving en onderhoud van het continuïteitsplan voor energievoorziening

Dit betreft een beschrijving op welke wijze het continuïteitsplan minimaal jaarlijks wordt beproefd, alsmede een beschrijving van de wijze waarop het continuïteitsplan na iedere activering wordt geëvalueerd en geactualiseerd. Hierbij dient nadrukkelijk aandacht te worden besteed aan de werking van de (nood) energievoorzieningen en gerelateerde voorraden hiervan.

Bijlage CSR 13 Handelswijze bij SOC incident melding en verhoogde dreiging

CSR 13.1 Doelstelling SOC incidentmeldingen

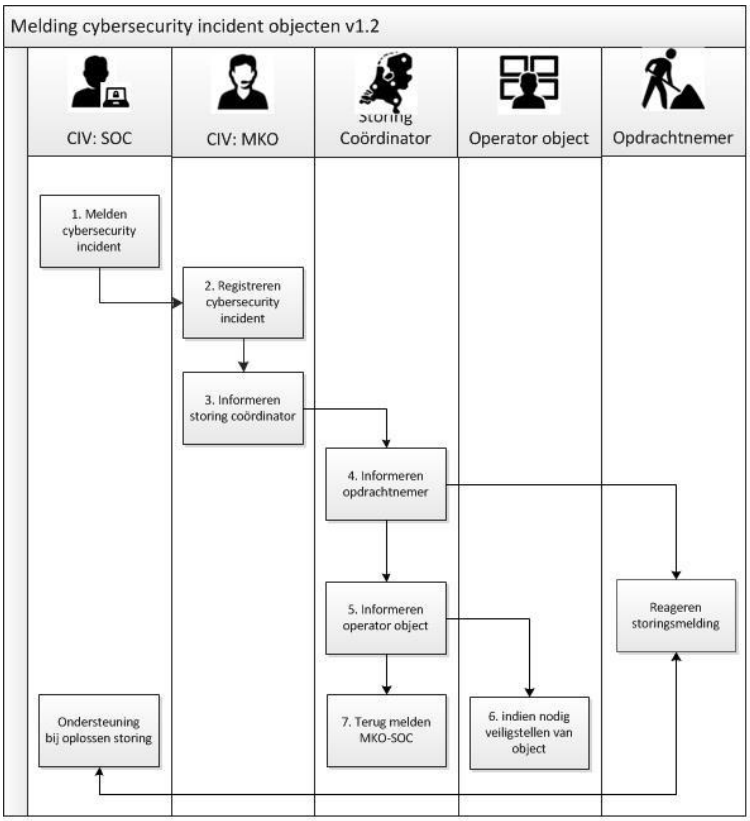
Het Security Operations Centre (hierna SOC) van Rijkswaterstaat ontwikkelt als één van haar diensten het monitoren van (loggings van) systemen en netwerkomgevingen van Rijkswaterstaat. Technische maatregelen worden ingevoerd om het ontsluiten en monitoren van (loggings op) regionale systemen en netwerkomgevingen mogelijk te maken. Resultaten worden door het SOC geanalyseerd, waardoor mogelijke cybersecurity incidenten vroegtijdig kunnen worden gesignaleerd.

Om bij aangetroffen cybersecurity incidenten zo snel mogelijk in te kunnen grijpen is het van belang deze direct te kunnen melden aan de eigenaar en/of de betreffende operator van het object. Hieronder volgt het proces voor meldingen van (mogelijke) cybersecurity incidenten aan de regio die vanuit het monitoringproces zijn ontdekt. In de regio worden cybersecurity incidenten ook cybersecurity storingen genoemd.

CSR 13.2 Algemeen

Na het ontdekken of vermoeden van een cybersecurity incident door het SOC meldt het SOC dit als een (mogelijk) cybersecurity incident aan de Missie Kritieke Ondersteuning (MKO). De MKO ontvangt de melding van het cybersecurity incident en registreert deze in Topdesk. Het MKO informeert op haar beurt de storing coördinator van de regio van het betreffende object. De storing coördinator informeert daarna de bedienaar en betreffende Opdrachtnemer van het object. Vervolgens wordt het al geïmplementeerde storingsmeldings en cybersecurity incident response proces gevolgd welke aansluit op het storingsproces van het object. Schematisch geeft dit de volgende processtappen.

CSR 13.3 Overzicht processtappen



CSR 13.4 RACI

In onderstaande RACI-matrix is voor elke activiteit aangegeven welke rollen welke verantwoordelijkheden hebben. Daartoe zijn per activiteit letters aan rollen toegekend. Zie voor de betekenis van elke letter de legenda onder de matrix:

Activiteiten Rapportage	CIV: SOC	CIV: MKO	District: Storing coördinator	CNB: Operator object	Opdrachtnemer	Regio
1. Melden cybersecurity incident	RA	I				
2. Registreren cybersecurity incident		RA				
3. Informeren storing coördinator		RA	I			
4. Informeren opdrachtnemer			RA	I	I	
5. Informeren operator object			RA	I		
6. Indien nodig veiligstellen van object			C	RA	C	C
7. Terug melden MKO – SOC	I	I	RA		C	

Legenda:

- R = Responsible:
  Degene (rol) die de activiteit uitvoert.
  Deze letter dient bij elke activiteit aan 1 rol te worden toegekend.
- A = Accountable:
  Degene (rol) aan wie door de verantwoordelijke (R) verantwoording wordt afgelegd.
  Deze letter dient bij elke activiteit aan 1 rol te worden toegekend.
- C = Consulted:
  Degene (rol) die een bijdrage kan leveren in het beoogde resultaat van de activiteit.
  Deze letter kan aan meerdere rollen worden toegekend.
- I = Informed:
  Degene (rol) die geïnformeerd wordt.
  Deze letter kan aan meerdere rollen worden toegekend.

CSR 13.5 Detailbeschrijving processtappen

1. Melden cybersecurity incident
Doel: constateren en melden van een (mogelijk) cybersecurity incident.

Het SOC monitort technische logging van objecten op (mogelijke) cybersecurity incidenten. Indien een (vermoeden van een) cybersecurity incident is geconstateerd dan meldt het SOC dit aan de MKO. Indien het incident ernstig van aard is belt het SOC tevens de MKO om de doorlooptijd zo kort mogelijk te maken.

2. Registreren cybersecurity incident
Doel: het registreren van het (mogelijke) cybersecurity incident.

De MKO registreert het (mogelijke) cybersecurity incident in Topdesk aan de hand van de verkregen informatie van het SOC.

In de registratie legt de MKO vast:
- welk object het betreft.
- welk systeem (hostnaam) of welk netwerk (netwerknaam) het betreft.

- onder welk centraal meldpunt het object valt.
- korte beschrijving van het cybersecurity incident.
- behandelaarsgroep (kan ook het SOC zijn)
- de ernst van het cybersecurity incident (deze is standaard niet urgent)

3. Informeren storing coördinator

Doel: het infomeren van de storing coördinator over het (mogelijke) cybersecurity incident.

De MKO informeert de (aan het object gerelateerde) storing coördinator over het (mogelijke) cybersecurity incident. Daarbij worden de van het SOC verkregen gegevens over het (mogelijke) cybersecurity incident telefonisch doorgegeven en eventueel per mail bevestigd. Hierbij wordt duidelijk aangegeven dat het om een mogelijk cybersecurity incident gaat.

4. Informeren opdrachtnemer

Doel: het infomeren van de opdrachtnemer over het (mogelijke) cybersecurity incident.

De storing coördinator informeert de opdrachtnemer van het object waar het (mogelijke) cybersecurity incident is geconstateerd per telefoon.
De gegevens over het cybersecurity incident van het SOC worden hierbij doorgegeven. Een monteur van de opdrachtnemer gaat op pad om het gemelde cybersecurity incident nader te onderzoeken.

De storing coördinator registreert het cybersecurity incident van het SOC als storing in het beheerdermanagementsysteem, hierbij worden de van MKO ontvangen gegevens vastgelegd.

5. Informeren operator object

Doel: het infomeren van de operator over het (mogelijke) cybersecurity incident.

De storing coördinator informeert de operator van het object over het cybersecurity incident van het SOC en de in gang gezette actie om de monteur van de opdrachtnemer het incident te laten onderzoeken.

6. Indien nodig veiligstellen van object

Doel: voorkomen van ongevallen en incidenten.

De operator van het object stelt het object veilig indien de melding van het SOC daar aanleiding toe geeft.

7. Terug melden MKO – SOC

Doel: Het SOC kan contact leggen met de dienstdoende monteur.

De storing coördinator geeft de naam en telefoonnummer van de monteur door aan de MKO. De MKO legt deze gegevens vast in Topdesk en informeert daarmee het SOC. Het SOC kan vervolgens contact opnemen met de monteur om het cybersecurity incident toe te lichten en de monteur te ondersteunen.

Voorbeelden SOC cybersecurity incident meldingen

Het SOC kan in principe 8 verschillende meldingen (use cases) uit het systeem krijgen. Dit kan per object verschillen.

1. Mislukte autorisatie pogingen
2. Verboden protocollen geconstateerd
3. Poging uitgaand verkeer
4. Koppeling met KA geconstateerd
5. Malware virusmelding
6. Configuratie wijziging in beveiligingsinstellingen
7. Afwijkend remote beheer gedrag
8. Software, configuratie gewijzigd

In de melding wordt in ieder geval opgenomen:

- zo gedetailleerd als mogelijk welk object het betreft: sluis, eventueel welke kolk en/of hoofd, brug, spuiwerk, enz. .
- Welke melding het betreft, een van de 8 bovengenoemde meldingen, eventueel aangevuld met extra beschikbare informatie.
- Urgentie: in principe NIET urgent.

Standaard CS vragen aan de bedienaar:

- Heb ik toestemming gegeven voor het overnemen van mij IA-werkplek?
- Zie ik ongecontroleerde muisbewegingen en/of vensters open en dicht gaan?
- Zie ik ongecontroleerde bedienhandelingen van het object?
- Zie ik verkeerstekens van kleur wijzigingen zonder dat ik daar een handeling voor heb verricht?
- Zie ik objectbewegingen plaatsvinden zonder aanleiding, geen bewuste handeling?

CSR 13.6 Doelstelling verhoogde dreiging

Het is van belang dat de Opdrachtnemer tijdens een periode van verhoogde dreiging de juiste acties neemt om de risico's te mitigeren. Deze dreigingen vraagt om een specifieke handelswijze van medewerkers van de Opdrachtnemer die beheer- en onderhoudswerkzaamheden uitvoeren aan ICT en IA systemen van Opdrachtgever.

CSR 13.7 Best practice voor verhoogde dreiging

Er is sprake van verhoogde dreiging als blijkt dat er een mogelijke (digitale) aanval op objecten van Rijkswaterstaat op handen is. Zo een aanval bevat mogelijk cyber elementen. Extra aandacht voor de ICT en IA systemen is daarom ook noodzakelijk. Er hoeft daarbij nog geen sprake te zijn van een daadwerkelijke hackaanval.

Soms worden deze aanvallen aangekondigd door de groepering die deze aanval gaat uitvoeren, soms kan deze informatie ook uit andere bronnen zijn verkregen waarbij het minder duidelijk is op welk moment de aanval kan plaatsvinden. Alertheid is daarom geboden.

Een aantal objecten van Rijkswaterstaat zijn aangesloten op het proces en Alerteringssysteem Terrorismebestrijding (ATb) van het ministerie van Justitie en Veiligheid. Een aantal objecten van Rijkswaterstaat is vitaal en valt onder de meldplicht Wbni (Wet Beveiliging Netwerk- en Informatiesystemen) en Bbni (Besluit beveiliging netwerk- en informatiesystemen).

Indien er sprake is van een verhoogde cyberdreiging dan meldt het DCC-IenW (Departementaal Coördinatiecentrum Crisisbeheersing van het ministerie van Infrastructuur en Waterstaat) dit aan het lijnmanagement van Rijkswaterstaat, alsmede op welk specifiek object de dreiging mogelijk is gericht.

De Opdrachtnemer wordt vervolgens via het storingsmeldingsproces op de hoogte gebracht van de verhoogde dreiging.

De Opdrachtnemer neemt de volgende acties:

a. De Opdrachtnemer neemt naar aanleiding van de storingsmelding contact op met de door Opdrachtgever aangegeven contractpersoon voor afstemming van uit te voeren acties en het tijdstip waarop deze acties nodig zijn;
b. Indien er sprake is van een acute dreiging dan zorgt de Opdrachtnemer er voor dat, afhankelijk van het verzorgingsgebied van de Opdrachtnemer, er voldoende monteurs stand-by zijn om de objecten in dat verzorgingsgebied waar en indien nodig te ‘servicen’;
c. Indien de dreiging zich manifesteert in daadwerkelijke acties treed het incident response plan in actie.

Bijlage CSR 14 Incident response

CSR 14.1 Doelstelling

Indien een incident optreedt, is het van belang dat de Opdrachtnemer op efficiënte wijze hierop acteert. Om op uniforme wijze met incidenten om te kunnen gaan, dient Opdrachtnemer een incident response plan IA op te stellen. Dit plan beschrijft de te nemen stappen vanaf het optreden van het incident, tot aan het activeren van het recoveryplan en terugkeren naar de normale situatie. Het voorbereiden van de organisatie op herstel is geen onderdeel van incident response of herstel zelf en dient vooraf te worden uitgewerkt en uitgevoerd. Ook de herstelwerkzaamheden zelf die kunnen voorvloeien uit het incident vallen buiten de scope van dit plan en horen thuis in een apart recoveryplan.

Dit plan omvat de incident response als gevolg van een melding vanuit het SOC van RWS of cybercalamiteit op de IA-omgeving. Hierbij valt te denken aan een hack van een object, een (D)DoS aanval op een object, of de uitbraak van malware (b.v. cryptolocker malware). Er is mogelijk sprake van een cybercalamiteit op het object, als:

a. Het object in beweging is gebracht, zonder dat de bedienaar hier bewust opdracht toe heeft gegeven via de IA omgeving;
b. Fysieke acties op het object afwijken van de genomen acties binnen de IA omgeving/HMI;
c. Bediening en besturing werken niet zoals verwacht, of reageren helemaal niet;
d. Er verlies van controle of zicht is op de IA omgeving/HMI.

CSR 14.2 Best practices

CSR 14.2.1 Beoogd publiek voor het incident response plan IA

Het Incident Response Plan IA beschrijft het incident response plan van Opdrachtnemer voor de IA-omgeving van RWS. Dit document beschrijft de te nemen stappen om, tijdens het optreden van een incident op de IA systemen van een object, op een zo effectief mogelijke en veilige wijze te reageren op dit incident teneinde de gevolgen ervan zoveel mogelijk te beperken en daarna een effectief herstel mogelijk te maken.

Beoogd publiek voor dit document is:

a. Opdrachtnemer verantwoordelijk voor het operationeel houden van het object (Operations manager voor het object, security specialisten, bedienaars en onderhoudsmedewerkers);
b. RWS objecteigenaar;
c. RWS Security team (ter kennisgeving);
d. RWS SOC (i.v.m. adviserende rol).

Eenieder die een verantwoordelijkheid heeft in dit plan, dient een papieren versie van dit plan thuis op een veilige plek te bewaren.

CSR 14.2.2 Hoe dit plan te gebruiken

In geval een incident optreed op een object, dient het incident zo snel mogelijk te worden bedwongen, waardoor het incident niet kan escaleren en eventueel noodzakelijk herstel kan worden uitgevoerd. Dit incident response plan beoogt een basis te creëren waarmee Opdrachtnemer een verdere uitwerking kan doen welke specifiek is voor het object.

CSR 14.2.3 Incident response doelen voor het object

Primaire doelstelling van dit plan is incidenten op een efficiënte wijze te managen en controleren, waarna de IA-omgeving van een object in een werkende staat teruggebracht kan worden middels het recoveryplan. Dit incident response plan beoogt uitsluitend aanwijzingen te geven teneinde (cyber-) incidenten in de IA-omgeving van het object te managen.

De incident response doelen zijn als volgt geprioriteerd:

a. Detecteren dat een incident optreedt en een eerste analyse van de dreiging;
b. Insluiten van de dreiging en beheersen van het incident;
c. Bestrijden van de dreiging;

d. Communiceren met het recoveryteam;
e. Rapporteren.

Deze stappen zijn verder uitgewerkt in paragraaf CSR 14.2.5.

CSR 14.2.4 Incident Response organisatie

CSR 14.2.4.1 Rollen en verantwoordelijkheden
Het object heeft een incident response team, waarbij deelnemers afhankelijk van hun functie binnen de organisatie een rol bedeeld krijgen. Werknemers van zowel Opdrachtnemer als RWS zijn betrokken bij incident response, waarbij RWS een adviserende functie heeft.

Met betrekking tot het incident response team geldt het volgende:
a. Het incident response team bestaat uit belangrijke stakeholders binnen de Opdrachtnemer;
b. De stakeholders kennen en steunen het incident response plan;
c. Elke medewerker kan een incident melden aan het incident response team. Dit kan ook gebeuren door medewerkers van RWS, bijvoorbeeld het RWS SOC;
d. Elke deelnemer in het incident response team heeft een kaart met essentiële contactinformatie van het team en draagt deze bij zich;
e. Elke deelnemer in het incident response team bewaart een papieren kopie van het incident response plan thuis op een veilige plaats;
f. De rollen en verantwoordelijkheden van het incident response team dienen bekend te zijn bij eenieder die werkzaam is op of voor het object, zodat zij weten wie verantwoordelijk zijn voor incident response.

De volgende rollen kunnen worden onderkend binnen het incident response team:

Rol	Verantwoordelijkheden
Operations manager Opdrachtnemer voor het object	• Contact voor Incident Respons Organisatie; • Neemt contact op met RWS objecteigenaar bij eerste kennisname van incident; • Stemt af met RWS objecteigenaar.
RWS objecteigenaar	• Wordt geïnformeerd door Operations manager over incident en verwachte impact van de calamiteit; • Overleg met RWS SOC en RWS Security team m.b.t. impact en strategie voor mitigeren van het incident.
RWS SOC	• Kan incident melden aan Opdrachtnemer; • Is adviserend betrokken bij incident respons.
RWS Security team	• Kan adviserend worden betrokken bij incident response.
Security specialisten opdrachtnemer	• Onderzoek naar en afhandeling van het incident.
Bedienaars, onderhoudsmedewerkers	• Identificeren van incident; • Melden van incident aan operations manager; • Overleg met RWS security team en RWS SOC; • Rapporteren naar Opdrachtnemer.

CSR 14.2.4.2 Contactpersonen
Voor elk object dient een lijst met contactpersonen te worden opgesteld, voorzien van actuele contactgegevens. De tabel hierna kan worden gebruikt als template voor het opstellen van zo'n lijst.

Naam	Functie	Mobiele nummer	Email	Opmerkingen

CSR 14.2.5 Stappen in de incident response fase

CSR 14.2.5.1 Detecteren van het incident
Opdrachtnemer is verantwoordelijk voor het bedienen en onderhouden van het object. Op elk moment kan Opdrachtnemer een security incident opmerken. Dit kan zijn een incident op het IA netwerk, of een incident gerelateerd aan de procedures rondom cybersecurity. Ook kan een incident worden opgemerkt door RWS SOC, die het incident dan meldt aan Opdrachtnemer.
Zodra een incident wordt gedetecteerd, wordt het incident response team van Opdrachtnemer actief voor een eerste analyse van de dreiging.

CSR 14.2.5.2 Eerste analyse van de dreiging
Het incident response team van Opdrachtnemer doet op basis van de eerste beschikbare gegevens over het incident een eerste analyse van de dreiging. Hierbij wordt het incident gecategoriseerd, op basis waarvan het incident binnen de organisatie wordt geëscaleerd en de securityorganisatie wordt opgeschaald.

CSR 14.2.5.3 Insluiten van de dreiging en beheersen van het incident
Gedurende deze fase wordt op basis van de eerste analyse besloten op welke wijze de dreiging wordt aangepakt. Hierbij kan het RWS SOC een adviserende rol spelen. Zodra de aanpak is vastgesteld, wordt de dreiging ingesloten zodat deze zich niet verder kan uitbreiden binnen of buiten het object. Op deze wijze wordt de dreiging onder controle gebracht zodat deze in de volgende fase bestreden kan worden. Het RWS SOC kan ook verzoeken om bestanden en systemen veilig te stellen voor mogelijk forensisch onderzoek. De instructies hiertoe dienen strikt opgevolgd te worden door Opdrachtnemer.

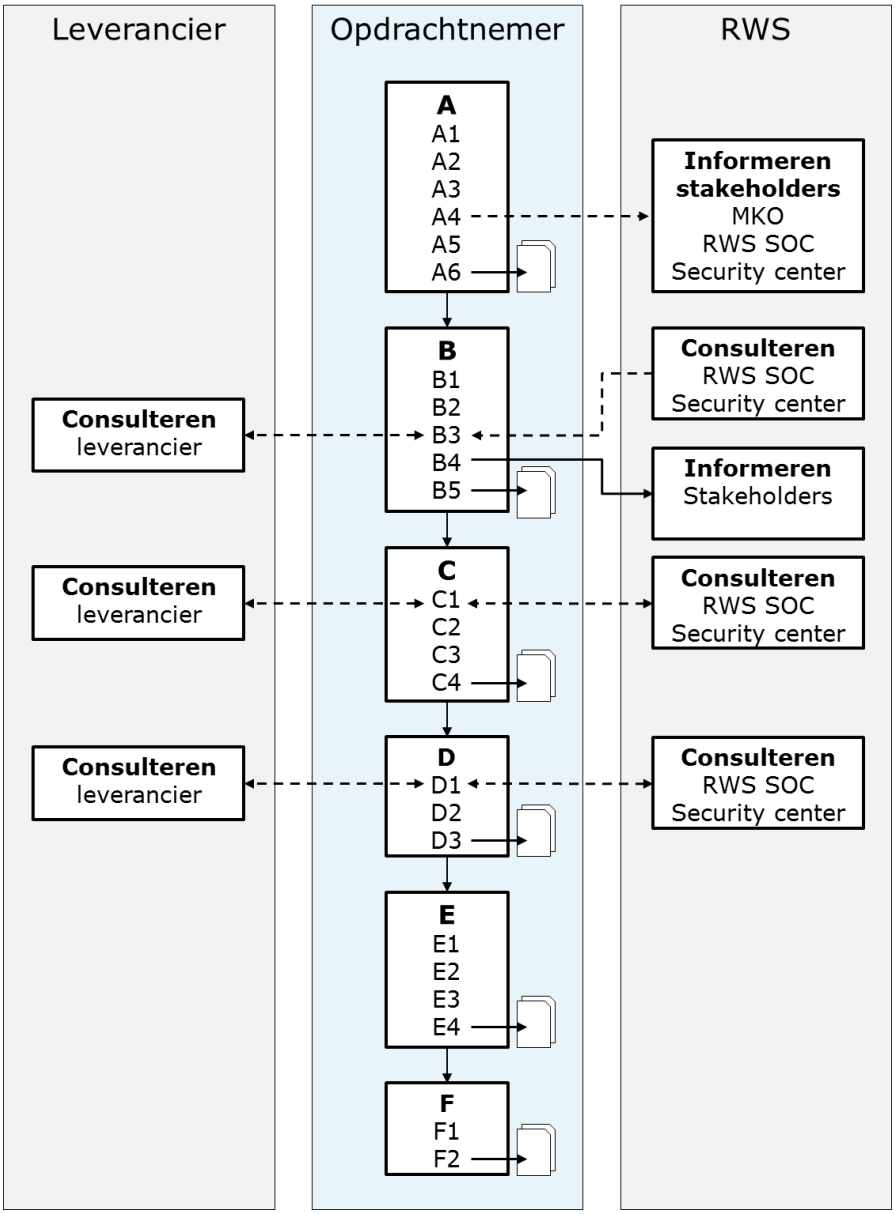
CSR 14.2.5.4 Bestrijden van de dreiging en beheersen van het incident
Het bestrijden van de dreiging wordt in algemeenheid uitgevoerd door het incident response team. In voorkomende gevallen is het bestrijden van de dreiging en incident alleen mogelijk tezamen met, of door herstel van het object. Het RWS SOC kan bij de beheersing van de dreiging en incident een adviserende en of sturende rol spelen.

CSR 14.2.5.5 Communiceren met het recoveryteam
Wanneer de dreiging bestreden is, of wanneer het incident volledig onder controle is, kan het recoveryteam aan de slag. Het recoveryteam zal in nauwe samenwerking met het incident response team de normale situatie gaan herstellen, waardoor het object weer volledig functioneel kan opereren.
Het incident response team
informeert het herstel team over alle relevante informatie die over de dreiging beschikbaar is en mogelijk relevant is voor herstel.

CSR 14.2.5.6 Rapporteren
Zodra het recoveryteam aangeeft dat de normale situatie is hersteld, zal het incident response team het incident afsluiten en de rapportage daaromtrent afronden.

CSR 14.2.6 Incident response activiteiten

CSR 14.2.6.1 Inleiding
De activiteiten gedurende elk van de in de vorige paragraaf genoemde stappen zijn in de figuur hierna grafisch weergegeven en worden in de daaropvolgende paragrafen toegelicht.



CSR 14.2.6.2 Activiteit tijdens detecteren van het incident

Nr.	Activiteit	Omschrijving
A1	Detectie incident	Incident wordt gedetecteerd door systeem, Bedienaar, Onderhoudsmedewerker, RWS SOC, of …
A2	Bevestigen incident	Opdrachtnemer onderzoekt of het inderdaad een incident opgetreden is.
A3	Informeren	Indien er inderdaad een incident opgetreden is, wordt Operations manager geïnformeerd.
A4	Beslissen opschaling	Operations manager beslist of onmiddellijk wordt opgeschaald naar overige stakeholders, of dat eerst verdere analyse van de dreiging dient plaats te vinden.
A5	Vervolgstappen	Operations manager zorgt dat de vervolgstappen worden genomen zodat een eerste analyse van het incident wordt gedaan en de dreiging wordt ingesloten.

A6	Rapporteren	Maak de relevante gegevens betreffende detectie beschikbaar voor rapportage.

CSR 14.2.6.3 Activiteiten tijdens eerste analyse van de dreiging

Nr.	Activiteit	Omschrijving
B1	Informeren	Security specialist van Opdrachtnemer wordt geïnformeerd.
B2	Analyseren	Security specialist doet een eerste onderzoek naar het incident. Betreft het bijvoorbeeld malware, een cyberaanval (hack), een (D)DOS (Denial Of Service), of een poging tot verkrijgen van ongeautoriseerde toegang).
B3	Consulteren	Security specialist consulteert RWS SOC of leverancier indien nodig.
B4	Informeren	De resultaten van het onderzoek worden gebruikt om Operations manager te informeren, die op zijn beurt RWS informeert.
B5	Rapporteren	Maak de analyse van de dreiging beschikbaar voor rapportage.

CSR 14.2.6.4 Activiteiten tijdens insluiten van de dreiging en beheersen van het incident

Nr.	Activiteit	Omschrijving
C1	Bepalen aanpak	In samenspraak tussen security specialist van Opdrachtnemer, Operations manager en indien relevant RWS SOC, wordt besloten wat de beste aanpak is voor het insluiten van de dreiging.
C2	Insluiten dreiging	Acties worden uitgevoerd om ervoor te zorgen dat de dreiging wordt ingesloten en zich niet kan verplaatsen/uitbreiden. Hierbij kan bijvoorbeeld worden gedacht aan het isoleren van getroffen systemen, blokkeren van netwerkverbindingen, monitoring van communicatie.
C3	Beheersen situatie	Zodra de dreiging is ingesloten en de situatie onder controle is kan begonnen worden met de volgende stap, het bestrijden van de dreiging.
C4	Rapporteren	Maak de informatie beschikbaar voor rapportage.

CSR 14.2.6.5 Activiteiten tijdens bestrijden van de dreiging en incident

Nr.	Activiteit	Omschrijving
D1	Bepalen aanpak	In samenspraak tussen security specialist van Opdrachtnemer, Operations manager en indien relevant RWS SOC, wordt besloten wat de beste aanpak is voor het bestrijden van de dreiging.
D2	Bestrijden dreiging	De stappen uit de aanpak worden gevolgd om de dreiging te bestrijden.
D3	Rapporteren	Maak de informatie beschikbaar voor rapportage.

CSR 14.2.6.6 Activiteiten tijdens communiceren met het recoveryteam

Nr.	Activiteit	Omschrijving
E1	Overdracht incident response --> herstel	Draag alle beschikbare informatie uit de eerdere fasen van het incident response plan m.b.t. het incident over aan het recoveryteam.

E2	Ondersteuning	Ondersteun het recoveryteam met aanvullende informatie waar nodig.
E3	Overdracht herstel -> incident response	Verzamel informatie beschikbaar gesteld door het recoveryteam.
E4	Rapporteren	Maak de informatie beschikbaar voor rapportage.

CSR 14.2.6.7 Activiteiten tijdens rapporteren

Nr.	Activiteit	Omschrijving
F1	Informatie verzamelen	Verzamel alle informatie die beschikbaar is gemaakt voor rapportage.
F2	Rapporteren	Stel rapport op zodat het incident en de afhandeling ervan op een later moment geëvalueerd kan worden.

CSR 14.2.7 Testen en onderhoud van het incident response plan

CSR 14.2.7.1 Testen van het incident response plan
Voor het testen van het incident response plan geldt het volgende:

a. Het incident response plan dient bekend te zijn bij het incident respons team en het recoveryteam, zodat een ieder weet wat de verantwoordelijkheden zijn;
b. Door het incident response plan regelmatig te oefenen/testen raakt betrokken staf van verschillende organisaties (opdrachtnemer, RWS) op elkaar ingespeeld en kunnen betrokkenen snel en juist handelen in geval van nood;
c. Elk jaar dient het incident response plan als volgt te worden getest:
    i. Eén (1) volledige oefening. Gedurende deze oefening acteren alle betrokkenen alsof een echt cybersecurity incident is opgetreden en doorloopt men alle stappen van het incident response plan;
    ii. Twee (2) table top oefeningen. Hierbij kunnen afzonderlijke onderdelen van het incident response plan worden getest;
d. Oefeningen dienen te worden gedocumenteerd. Deze informatie dient te worden gebruikt als input tijdens de evaluatie van de oefening. Hierdoor:
    i. Leren betrokkenen wat goed ging, en vooral ook wat verbeterd kan worden;
    ii. Kunnen de geleerde lessen gebruikt worden om het plan te verbeteren en gedeeld worden met andere RWS objecten als best practice.

CSR 14.2.7.2 Onderhoud van het incident response plan
Het incident response plan dient periodiek te worden onderhouden. Ook na het testen van het incident response plan dient het plan te worden geëvalueerd, met aandacht voor het volgende:

a. Effectiviteit van het plan;
b. Volledigheid van het plan;
c. Aansluiting van het plan op de actuele situatie bij het specifieke object.

Het incident response plan dient te worden geactualiseerd, als:

a. Evaluatie van het plan hiertoe aanleiding geeft;
b. Een nieuwe Opdrachtnemer het beheer van een object op zich neemt;
c. Er een significante verandering is in de IA-omgeving van het object;
d. Er een significante verandering is in de consequentie van incidenten;
e. Er nieuwe middelen beschikbaar komen voor onderzoek naar en afhandelen van incidenten;
f. Er een significante verandering is in de risicomatrix voor het object.

Bijlage CSR 15 Recoveryplan

CSR 15.1 Doelstelling

Het is essentieel dat schade, ontstaan door het optreden van een incident, op effectieve wijze hersteld kan worden. Hiertoe dient de Opdrachtnemer een recoveryplan op te stellen. Dit plan beschrijft de hersteldoelen, rollen en verantwoordelijkheden, de verschillende fasen van herstel, herstelactiviteiten en het onderhouden van het recoveryplan.

Dit recoveryplan omvat het herstel van de IA-omgeving als gevolg van een cyber-calamiteit. Hierbij valt te denken aan een hack van een object, een (D)DoS aanval op een object, of de uitbraak van malware (b.v. cryptolocker malware).

Dit plan is opgesteld als een template voor Opdrachtnemers en dient als basis voor hen om een recoveryplan specifiek voor het object waarvoor zij verantwoordelijk zijn op te stellen. De initiële incident respons valt buiten de scope van dit plan en hoort thuis in een apart incident respons plan.

CSR 15.2 Best practices

CSR 15.2.1 Beoogd publiek voor het recoveryplan

Het recoveryplan IA-omgeving Objecten beschrijft de te nemen stappen om, na uitval van de IA systemen van een object door een cyberincident, dit object op een zo effectief mogelijke en veilige wijze weer operationeel te krijgen.

Beoogd publiek voor dit document is:

a. RWS objecteigenaar;
b. RWS Security team;
c. RWS SOC;
d. Opdrachtnemer verantwoordelijk voor het operationeel houden van het object (operations manager, medewerkers onderhoud).

Eenieder die een verantwoordelijkheid heeft in dit plan, dient een papieren versie van dit plan thuis op een veilige plek te bewaren.

CSR 15.2.2 Hoe het recoveryplan te gebruiken

In geval een object de beoogde functie niet meer kan vervullen als gevolg van een calamiteit, dient deze functie zo spoedig mogelijk te worden hersteld. Dit recoveryplan beoogt een basis te creëren waarmee Opdrachtnemers een verdere uitwerking kunnen doen welke specifiek is voor het object.

CSR 15.2.3 Hersteldoelen voor het object

Primaire doelstelling van dit plan is de IA-omgeving van een object terug te brengen in een werkende staat, waarbij veiligheid van personen en object voorop staan. Dit plan beoogt uitsluitend aanwijzingen te geven teneinde de IA-omgeving van het object te herstellen. Herstel van fysieke schade aan het object valt buiten de scope van dit recoveryplan. In het recoveryplan dient per systeem aandacht te zijn voor de Recovery Time Objective (RTO) en Recovery Point Objective (RPO), waarbij de laatste een relatie heeft met de back-up frequentie.

De hersteldoelen zijn als volgt geprioriteerd:

a. Herstel van functionaliteit van, en controle over, de veiligheidssystemen (safety);
b. Herstel van functionaliteit van, en controle over, de kritieke controle systemen binnen de IA-omgeving;
c. Herstel van functionaliteit van, en controle over, de overige controle systemen binnen de IA-omgeving;
d. Herstel van functionaliteit van, en controle over, de overige systemen binnen de IA-omgeving.

Onderstaande tabel kan door Opdrachtnemer worden gebruikt om een overzicht samen te stellen van de IA-systemen die binnen elke categorie vallen.

Prioriteit	Systeem categorie	Lijst met systemen binnen de categorie	Maximale hersteltijd
1	Safety/SIS	• .. • .. •	
2	Kritieke controle systemen	• .. • .. •	
3	Overige controle systemen	• .. • .. •	
4	Overige systemen	• .. • .. •	

Met safety systemen worden de systemen bedoeld die betrokken zijn bij de safety/ veiligheidsfuncties van het object. Onder kritieke controle systemen worden die systemen bedoeld die direct het primaire proces aansturen. Overige controle systemen zijn die systemen die niet direct betrokken zijn bij de aansturing van het primaire proces. Overige systemen zijn alle overige systemen binnen de IA-omgeving.

CSR 15.2.4 Recovery organisatie

CSR 15.2.4.1 Rollen en verantwoordelijkheden
Het object heeft een recoveryteam, waarbij deelnemers afhankelijk van hun functie binnen de organisatie een rol bedeeld krijgen. Werknemers van zowel Opdrachtnemer als RWS kunnen deelnemer zijn in de recovery organisatie.

Met betrekking tot het recoveryteam geldt het volgende:

a. Het recoveryteam bestaat uit belangrijke stakeholders binnen de organisatie;
b. De stakeholders kennen en steunen het recoveryplan;
c. Het recoveryteam heeft de risico's van het opereren onder het recoveryplan in kaart gebracht, samen met de extra mitigerende maatregelen om deze risico's terug te brengen;
d. Het recoveryplan kan alleen door daartoe bevoegde personen uit de recovery organisatie worden geactiveerd;
e. Communicatie binnen het team vind plaats via (waar relevant) Atex-proof portofoons en waar nodig voor gegevensuitwisseling, via email;
f. Elke deelnemer in het recoveryteam heeft een kaart met essentiële contactinformatie van het team en draagt deze bij zich;
g. Elke deelnemer in het recoveryteam bewaart een papieren kopie van het recoveryplan thuis op een veilige plaats;
h. De rollen en verantwoordelijkheden van het recoveryteam dienen bij eenieder die werkzaam is op of voor het object, zodat zij weten wie verantwoordelijk zijn voor herstel.

De volgende rollen kunnen worden onderkend binnen het recoveryteam:

Rol	Verantwoordelijkheden
Operations manager Opdrachtnemer voor het object	• Contact voor Incident Respons Organisatie; • Neemt contact op met RWS objecteigenaar bij eerste kennisname van incident; • Stemt herstel af met RWS objecteigenaar.
RWS objecteigenaar	• Wordt geïnformeerd door Operations manager over calamiteit, verwachte impact van de calamiteit en hersteltermijn; • Overleg met RWS SOC en RWS Security team m.b.t. impact en strategie voor herstel en overige continuïteitsmaatregelen.
Contactpersoon leverancier	• Wordt door Opdrachtnemer benaderd voor levering hardware/software/apparatuur indien dit niet (voldoende) voorradig is; • Levert hardware/software/apparatuur en ondersteuning aan Opdrachtnemer.
RWS SOC	• Is betrokken bij incident respons; • Beslist mede wanneer herstelwerkzaamheden kunnen worden uitgevoerd
RWS Security team	• Is betrokken bij incident respons; • Bewaakt namens RWS het recoveryproces.
Medewerker onderhoud	• Uitvoeren van de herstelwerkzaamheden; • Overleg met RWS security team en RWS SOC; • Rapporteren naar Opdrachtnemer.

CSR 15.2.4.2 Contactpersonen

Voor elk object dient een lijst met contactpersonen te worden opgesteld, voorzien van actuele contactgegevens. De tabel hieronder kan door Opdrachtnemer worden gebruikt om deze lijst samen te stellen.

Naam	Functie	Mobiele nummer	Email	Opmerkingen

CSR 15.2.5 Fasen van recovery

CSR 15.2.5.1 Voorbereiden op recovery

Om een spoedig herstel te kunne borgen is het van belang dat Opdrachtnemer hierop is voorbereid. Daarvoor is het noodzakelijk om de beschikking te hebben over actuele en relevante (systeem-)informatie van het object. Hieronder valt tenminste:

a. Geïnstalleerde hardware, inclusief firmware en configuraties;
b. Geïnstalleerde Operating Systems en software, inclusief configuraties;
c. Actuele back-ups van de systemen;
d. Netwerk configuratie, inclusief gebruikte communicatiemiddelen;
e. Documentatie (online en offline);
f. Recoveryorganisatie en communicatieplan;
g. Recoverymiddelen en werkprocedures;
h. Testprocedures;
i. Inbedrijfstellingsprotocollen.

CSR 15.2.5.2 Optreden van calamiteit

Deze fase begint met het optreden van de calamiteit. Gedurende de calamiteit treedt het incident respons plan in werking. Het incident respons plan houdt zich vooral bezig met de eerste reactie op de calamiteit en de afhandeling daarvan. Belangrijke activiteiten gedurende deze fase zijn vaststellen van

de calamiteit, notificatie van het management Opdrachtnemer en RWS, incident respons activiteiten en waar nodig inschakelen van RWS SOC. Deze activiteiten vallen buiten de scope van dit document.

CSR 15.2.5.3 Activeren van het recoveryplan
Gedurende deze fase wordt het recoveryplan geactiveerd. Gedurende deze fase worden betrokkenen (Opdrachtnemer, RWS en mogelijk leveranciers) geïnformeerd en dienen zij actief hun rol te vervullen in het recoveryplan. Het recoveryplan wordt geactiveerd slechts nadat de calamiteit is beheerst. Het nemen van eventuele noodmaatregelen voor continuïteit kan parallel lopen aan het recoveryplan. Deze noodmaatregelen voor bedrijfscontinuïteit van het object vallen buiten de scope van dit document.

CSR 15.2.5.4 Activiteiten m.b.t. recovery
Gedurende de recoveryfase dienen een aantal activiteiten te worden verricht. Deze activiteiten zijn, op hoofdpunten:

a. Vaststellen schade en benodigde acties t.b.v. recovery;
b. Recoveryactiviteiten t.b.v. netwerkapparatuur;
c. Recoveryactiviteiten t.b.v. veiligheidsvoorzieningen;
d. Recoveryactiviteiten t.b.v. machinebesturing;
e. Recoveryactiviteiten t.b.v. bediening en beheer;
f. Recoveryactiviteiten t.b.v. overige systemen.

Deze activiteiten worden in paragraaf CSR 15.2.6 verder uitgewerkt.

CSR 15.2.5.5 De-escalatie naar normale operationele status van het object
Op het moment dat alle activiteiten voor recovery zijn afgerond en het object weer werkzaam is, dient de normale operationele status van het object weer te worden bereikt. Dit gebeurt door het overdragen van de installatie door het recoveryteam aan het operationele team.

Met deze de-escalatie wordt het beheer en de bediening van het object teruggegeven aan de operatie. Het recoveryteam kan vervolgens het recoveryplan afsluiten met de benodigde rapportage.

CSR 15.2.6 Recoveryactiviteiten

CSR 15.2.6.1 Inleiding
De recoveryactiviteiten worden hierna toegelicht. Deze bevatten de stappen die genomen dienen te worden als onderdeel van het recoveryplan, zoals besproken in paragraaf CSR 15.2.5.4.

CSR 15.2.6.2 Recoveryactiviteit netwerkapparatuur

Nr.	Activiteit	Omschrijving
A1	Uitvoeren risico- en impactanalyse	Bepaal de risico's en mogelijke impact van de uit te voeren recoverywerkzaamheden.
A2	Vervang defecte hardware	Indien defecte hardware aanwezig, dient deze vervangen te worden door reserve exemplaren.
A3	Laad de configuratiefiles	Zet de laatste back-ups van de apparaat configuraties terug op de betreffende apparaten.
A4	Check de configuraties	Loop de configuratie na van de betrokken systemen. Denk aan IP instellingen, accountinstellingen, rechten, hardening, etc.
A5	Test de systemen op juiste werking	Doe een regressietest op functionaliteit en connectiviteit.
A6	Bijwerken back-ups	Maak, indien nodig, nieuwe back-ups en leg dit vast in het software beheersysteem.
A7	Bijwerken CMDB	Logboek en configuratiewijzigingen (hard- en software) verwerken in CMDB.
A8	Rapporteren	Stel rapport met bevindingen en aanbevelingen op.

CSR 15.2.6.3 Recoveryactiviteit veiligheidsvoorzieningen

Nr.	Activiteit	Omschrijving
B1	Uitvoeren risico- en impactanalyse	Bepaal de risico's en mogelijke impact van de uit te voeren recoverywerkzaamheden.
B2	Vervang defecte hardware	Indien defecte hardware aanwezig, dient deze eerst vervangen te worden door reserve exemplaren.
B3	Restore de software	Zet de laatste backups van de systemen terug op de betreffende systemen.
B4	Check de configuraties	Loop de configuratie na van de betrokken systemen. Denk aan IP instellingen, accountinstellingen, rechten, hardening, etc.
B5	Test de systemen op juiste werking	Doe een regressietest op functionaliteit en connectiviteit.
B6	Bijwerken backups	Maak, indien nodig, nieuwe backups en leg dit vast in het software beheersysteem.
B7	Bijwerken CMDB	Logboek en configuratiewijzigingen (hard- en software) verwerken in CMDB.
B8	Rapporteren	Stel rapport met bevindingen en aanbevelingen op.

CSR 15.2.6.4 Recoveryactiviteit PLC's, VSD/VFD, smart sensors

Nr.	Activiteit	Omschrijving
C1	Uitvoeren risico- en impactanalyse	Bepaal de risico's en mogelijke impact van de uit te voeren recoverywerkzaamheden.
C2	Vervang defecte hardware	Indien defecte hardware aanwezig, dient deze eerst vervangen te worden door reserve exemplaren.
C3	Restore de software	Zet de laatste back-ups van de systemen terug op de betreffende systemen.
C4	Check de configuraties	Loop de configuratie na van de betrokken systemen. Denk aan IP instellingen, accountinstellingen, rechten, hardening, etc.
C5	Test de systemen op juiste werking	Doe een regressietest op functionaliteit en connectiviteit.
C6	Bijwerken back-ups	Maak, indien nodig, nieuwe back-ups en leg dit vast in het software beheersysteem.
C7	Bijwerken CMDB	Logboek en configuratiewijzigingen (hard- en software) verwerken in CMDB.
C8	Rapporteren	Stel rapport met bevindingen en aanbevelingen op.

CSR 15.2.6.5 Recoveryactiviteit HMI, SCADA, EWS, OWS, computerapparatuur

Nr.	Activiteit	Omschrijving
D1	Uitvoeren risico- en impactanalyse	Bepaal de risico's en mogelijke impact van de uit te voeren recoverywerkzaamheden.
D2	Vervang defecte hardware	Indien defecte hardware aanwezig, dient deze eerst vervangen te worden door reserve exemplaren.
D3	Restore de software	Zet de laatste back-ups van de systemen terug op de betreffende systemen.
D4	Check de configuraties	Loop de configuratie na van de betrokken systemen. Denk aan IP instellingen, accountinstellingen, rechten, hardening, etc.
D5	Test de systemen op juiste werking	Doe een regressietest op functionaliteit en connectiviteit.

D6	Bijwerken back-ups	Maak, indien nodig, nieuwe back-ups en leg dit vast in het software beheersysteem.
D7	Bijwerken CMDB	Logboek en wijzigingen (hard- en software) verwerken.
D8	Rapporteren	Stel rapport met bevindingen en aanbevelingen op.

CSR 15.2.6.6 Recoveryactiviteit overige systemen

Veel overige systemen zoals bijvoorbeeld een telefooncentrale en de CCTV installatie zijn leverancier specifieke installatiedelen en alleen door de leverancier zelf in te richten. Wij verwijzen daarvoor dan ook naar de specifieke leveranciers.

CSR 15.2.6.7 Testen van het recoveryplan

Voor het testen van het recoveryplan geldt het volgende:

a. Het recoveryplan dient bekend te zijn bij het incident respons team en het recoveryteam, zodat een ieder weet wat de verantwoordelijkheden zijn;
b. Door het recoveryplan regelmatig te oefenen/testen raakt betrokken staf van verschillende organisaties (opdrachtnemer, RWS, leverancier) op elkaar ingespeeld en kunnen betrokkenen snel en juist handelen in geval van nood;
c. Elk jaar dient het recoveryplan als volgt te worden getest:
    i. Eén (1) volledige oefening. Gedurende deze oefening acteren alle betrokkenen alsof een echt cybersecurity incident is opgetreden en doorloopt men alle stappen van het recoveryplan;
    ii. Twee (2) table top oefeningen. Hierbij kunnen afzonderlijke onderdelen van het recoveryplan worden getest;
d. Oefeningen dienen te worden gedocumenteerd. Deze informatie dient te worden gebruikt als input tijdens de evaluatie van de oefening. Hierdoor:
    iii. Leren betrokkenen wat goed ging, en vooral ook wat verbeterd kan worden;
    iv. Kunnen de geleerde lessen gebruikt worden om het plan te verbeteren en gedeeld worden met andere RWS objecten als best practice.

CSR 15.2.6.8 Onderhoud van het recoveryplan

Het recoveryplan dient periodiek te worden onderhouden. Ook na het testen van het recoveryplan dient het plan te worden geëvalueerd, met aandacht voor het volgende:

a. Effectiviteit van het plan;
b. Volledigheid van het plan;
c. Aansluiting van het plan op de actuele situatie bij het specifieke object.

Het recoveryplan dient te worden geactualiseerd, als:

a. Evaluatie van het plan hiertoe aanleiding geeft;
b. Er een significante verandering is in de IA-omgeving van het object;
c. Er een significante verandering is in de consequentie van incidenten;
d. Er een significante verandering is in de risicomatrix voor het object.

Bijlage CSR 16 Registratie assets in een configuratiemanagement database (CMDB)

CSR 16.1 Doelstelling

Het doel van de CMDB (Configuration Management DataBase) Industriële Automatisering en Cybersecurity is het beheer van gegevens en informatie over industriële automatisering CI's (configuratie items / assettypes) ten behoeve van (operationeel en tactisch) assetmanagement en cybersecurity. Middels dit document wordt een kader geschapen voor het eenduidig vastleggen van afspraken over de gegevensvastlegging en de presentatie daarvan ten behoeve van Industriële Automatisering en Cybersecurity in het assetmanagementproces.

CSR 16.1.1 Presentatiemodel

In een informatiemodel wordt vastgelegd over welke zaken een administratie wordt bijgehouden: Configuratie Items (CI's). Daarbij beschrijft het "Conceptueel Datamodel IV Asset–en Configuratiemanagement" wat hierover vastgelegd wordt: Informatiebehoefte en Relaties.
Dit document beschrijft de assetmanagement informatiebehoefte en hoe de informatie aangeleverd en verwerkt dient te worden: Presentatiemodel. Dit presentatiemodel is een 'data-view' op het informatiemodel waarbij data uit verschillende CI's worden samengevoegd en aan de gebruiker gepresenteerd op een voor de gebruiker werkbare manier.

Daar waar de IV dienstverlening de focus legt op de totale landelijke dienstverlening, legt het assetmanagementproces de focus op systemen/netwerkschakels, objecten of onderdelen van de objecten. Het is daarom noodzakelijk om voor dit assetmanagementproces de informatie op de juiste wijze te presenteren vanuit het informatiemodel.
Als we spreken over een 'asset' of 'asset-type' in deze CMDB, dan wordt een te beheren en onderhouden onderdeel van de Operationele Technologie (OT) installatie bedoeld. We spreken hier expliciet niet over een fysiek object of kunstwerk in zijn geheel.

Aanvullend op dit presentatiemodel wordt het template *CMDB IA OT – Informatiebehoefte en presentatie Excel Format* beschikbaar gesteld. Deze bevat aanwijzingen en templates om de gegevens in het voor u liggende model aan te leveren. Zie paragraaf CSR 16.4 voor uitleg en voorbeelden.
Dit document, als beschrijvend presentatiemodel, is een voorzet voor het ontwerp van een CMDB als beheertool.

CSR 16.1.2 Scope

Het presentatiemodel CMDB Industriële Automatisering en Cybersecurity kan worden gezien als een gedetailleerde beschrijving van de informatiebehoefte van de objecteigenaren in het kader van assetmanagent (AM) en cybersecurity (CS). Het model stelt eisen aan de database(s) waarin de betreffende asset-types of attributen dienen te worden vastgelegd, maar bepaalt niet in welke database(s) dit zou moeten gebeuren alsook niet het daadwerkelijk gebruikte informatiemodel.
In dit presentatiemodel wordt per asset-type de verplicht in te vullen attributen beschreven. Voor ieder attribuut geldt één van de onderstaande situaties (meerdere gelijktijdige situaties zijn niet mogelijk):

1. *Minimum set IA/OT*;
   Dit veld met gegevens dient minimaal aanwezig en gevuld te zijn in de CMDB. Dit biedt met name bij de start van het vullen of aanmaken van een object CMDB een praktische aanpak om 'mee te starten'.
2. *Standaard set IA/OT*;
   Dit veld met gegevens dient standaard aanwezig en gevuld te zijn in de CMDB bij renovatie of nieuwbouw van de IACS installatie of delen daarvan. Bij oplevering van het renovatie- of nieuwbouwproject, dienen deze gegevens as-built aangeleverd te worden in de CMDB.
3. *Optioneel*;
   Dit veld met gegevens is optioneel aanwezig in de database indien van toepassing op de installatie. Uit de 'definitie' of 'schrijfwijze' zal ON moeten opmaken of dit veld al dan niet van toepassing is binnen het contract en noodzakelijke informatie bevat voor beheer van de installatie.

4. Er is nog een vierde situatie: Het is mogelijk dat de beheerder/OG gegevens (CI's) of attributen heeft geregistreerd, naast de in dit document genoemde attributen die dienen bijgewerkt te worden. Bij conflicten tussen de datamodellen, dan gaat het datamodel van de beheerder allereerst voor op de voorgestelde database of datamodel vanuit dit document of van de onderhoudspartijen.

Gebruik van bestaande CMDB van Opdrachtgever (OG):
In het geval er al een (onvolledige) CMDB aanwezig is bij de beheerder/OG, dient in dat geval met de beheerder/OG overeen gekomen te worden dat ofwel de bestaande CMDB wordt uitgebreid met de benodigde attributen en CI's ofwel ON zet zelfstandig een losse database op voor beheerder/OG om aanvullende registratie van gegevens mogelijk te maken. Een mogelijk wijze van data-uitwisseling is middels het template *CMDB IA OT – Informatiebehoefte en presentatie Excel Format*. De beheerder/OG zal in dit geval aangeven welke velden minimaal gevuld dienen te worden op basis van de bestaande CMDB.

Één van de databases van de beheerder is bijvoorbeeld het Onderhoudsmanagementsysteem (OMS) ten behoeve van assetmanagement. In dit document zal op veel plaatsen een verwijzing aangebracht zijn naar het OMS. Indien het OMS dit attribuut niet bevat, dan dient dit veld alsnog op alternatieve wijze te worden geregistreerd en onderhouden. Indien het attribuut wel beschikbaar is, kan middels het attribuut 'OMS ID' aangegeven worden hoe het asset-type gekoppeld is aan het OMS.

CSR 16.1.3 Disclaimer
Het opslaan en beheren van documenten, behoort niet tot de scope van de *CMDB Industriële Automatisering en Cybersecurity*. Er kan wel verwezen worden naar (mogelijk) bestaande beheersystemen. Het asset type 'Documentatie' bevat attributen ten behoeve van de aanwezige documentatie welke (veelal) aanwezig is in een bestaand documentbeheersysteem (e.g. Meridian). Daarnaast kunnen de attributen in de asset-types 'Locatie' en 'Verantwoordelijke' al aanwezig zijn in een onderhoudsbeheersysteem.

CSR 16.1.4 Beheer en Eigenaarschap
Dit presentatiemodel wordt beheerd door het CIV Security Center, team Security-by-Design IA als onderdeel van de CSIR. Wijzigingen die betrekking hebben op de modellering of andere aanpassingen van het proces of procedures of functionele eisen van de tooling worden alleen op basis van een Request for Change (RFC) besproken.

CSR 16.1.5 Data Vertrouwelijkheid
De informatieclassificatie geeft de aard van de documentatie weer en helpt de gebruiker bij het bepalen hoe een document verwerkt dient te worden. De informatie in de CMDB heeft informatieclassificatie 'RWS Bedrijfsvertrouwelijk'. De informatie in de CMDB is uitsluitend toegankelijk voor diegenen die de informatie nodig hebben om hun werkzaamheden uit te kunnen voeren en wordt op basis van need-to-know verstrekt.

Zie CSIR bijlage CSR 1 "Omgaan met vertrouwelijke informatie en documenten" en paragraaf 16.4 in dit document over hoe de informatie uitgewisseld kan.

CSR 16.1.6 Wijzigingsverzoeken
Het Presentatiemodel CMDB Industriële Automatisering en Cybersecurity bevat een overzicht van nu bekende, voor Assetmanagement en Cybersecurity relevante, asset-types en attributen. Het is echter mogelijk dat de opdrachtnemer relevante assets beheert of levert die nog niet in dit model staan beschreven en wat betreft functionaliteit ook niet vergelijkbaar zijn. Dit vraagt een aanvulling op het voor u liggende model en de bovengenoemde templates.
Wanneer er een wijzigingen van het presentatiemodel nodig is (bijvoorbeeld de toevoeging of verwijdering van een asset-type), wordt deze wijziging voorgelegd aan de contactpersoon bij RWS en pas na schriftelijke goedkeuring door de aangewezen contactpersoon bij RWS doorgevoerd in de templates. Daarbij levert de opdrachtnemer een beschrijving van de betreffende wijziging zodat deze kan worden doorgevoerd in het Presentatiemodel CMDB Industriële Automatisering en Cybersecurity

en indien noodzakelijk, ook in het Conceptueel Datamodel IV Asset–en Configuratiemanagement. Indien de wijziging toch vragen oproept bij relevante RWS-medewerkers, wordt de wijziging toegelicht en zo nodig aangepast totdat deze door de betreffende RWS-medewerkers als begrijpelijk wordt ervaren.

CSR 16.1.7 Toekomst
Dit model zal met nieuwe kennis worden bijgewerkt.

CSR 16.1.8 Leeswijzer
Paragraaf CSR 16.2 geeft een overzicht van de Asset-types en Relatietypes van het *Data model CMDB Industriële Automatisering en Cybersecurity*.
Paragraaf CSR 16.2.1 start met het schematisch overzicht. Begrippen uit dit overzicht worden daaropvolgend toegelicht.
In paragraaf CSR 16.2.2 volgt een beschrijving van de Asset-types en Relatietypes. Deze start met overzichten van de Assettypes (paragraaf 16.2.2.1) en de Relatietypes (paragraaf 16.2.2.2).

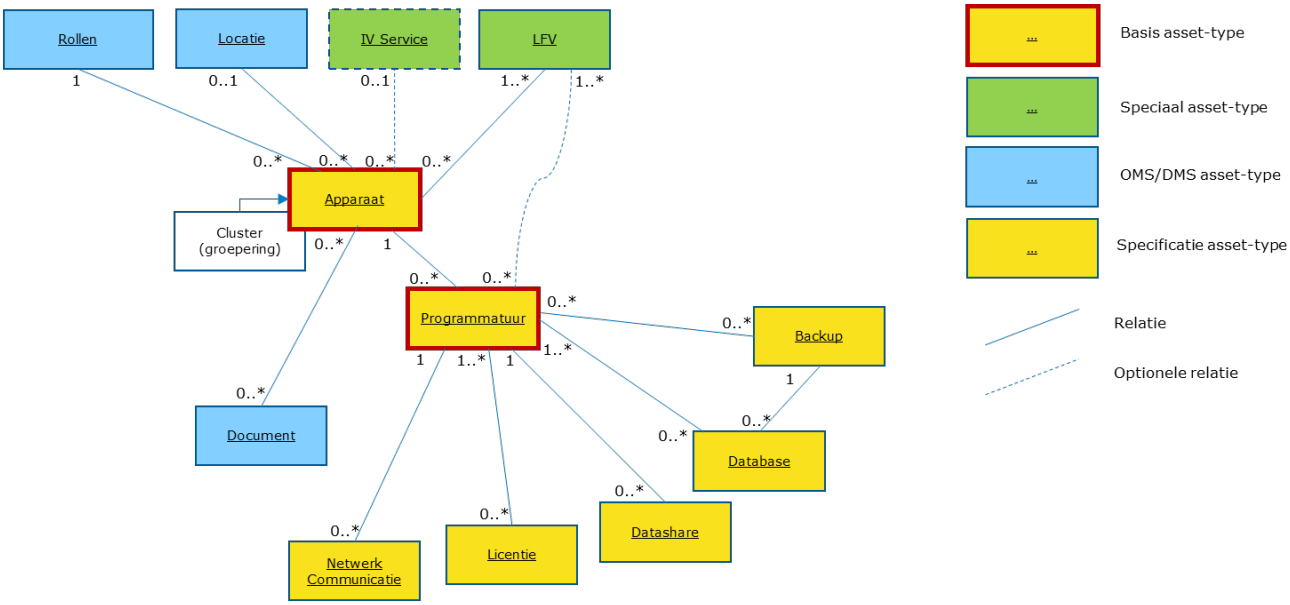
Tot slot is voor alle Asset-types een korte definitie opgesteld en worden de attribuuttypes beschreven. Dit is beschreven in de paragraaf “Asset-types uitgelicht” (deel 16.3).

CSR 16.2 Overzicht assets en relaties

CSR 16.2.1 Schematisch overzicht

In dit document worden relaties met verschillende asset-types en hun aanvullende eigenschappen (ook gedefinieerd als asset-types) benoemd. Zie §CSR 16.2.2.2 voor uitleg over deze relaties.

Onderstaande figuur toont een model op basis van logische relaties tussen de asset-types.



Figuur 1: Vereenvoudigd presentatiemodel

De gele blokken met rode omlijning bevatten de basis van de CMDB IA/OT. Een Apparaat heeft een “één op veel” relatie met Programmatuur. Middels het attribuut ‘cluster’ kunnen verschillende apparaten gegroepeerd worden bij de inrichting van virtuele apparaten in combinatie met fysieke apparaten. Zie hiervoor het asset-type ‘apparaat’.

De blauwe blokken bevatten, waar mogelijk, een koppeling met een onderhoudsmangementsysteem (OMS) of documentbeheersysteem (DMS) waar de benodigde informatie al aanwezig kan zijn. Voor de aanlevering van gegevens, voor deze Asset-types, is overleg nodig met de gegevensbeheerder van de regio.

De groene blokken verwijzen naar een relatie met het tactisch assetmanagement. Voor OT assetmanagement betreft het de logische functie vervuller (zie asset-type ‘LFV’ voor uitleg). Dit is momenteel nog beperkt tot logische functies die door de opdrachtnemer in overleg met de regio bepaald dienen te worden, maar zal in de toekomst mogelijk uitgebreid worden met verwijzing naar de Landelijke Tunnelstandaard (LTS) en Landelijke Bruggen en Sluizen standaard (LBS).

De gele blokken met blauwe omlijning zijn de eigenschappen van een bovenliggend asset type.

CSR 16.2.2 Beschrijving asset-types en relaties

CSR 16.2.2.1 Overzicht asset-types

Binnen het presentatiemodel kunnen asset-types gezien worden als een beschrijving van de dataview op de database en het conceptueel datamodel, voor een specifiek deel van het te beheren en onderhouden asset.
Afhankelijk van ingevulde attributen, is het mogelijk om gerelateerde attributen (on)zichtbaar te maken waardoor de presentatie overzichtelijker wordt. Deze gerelateerde attributen worden in dit document echter zeer beperkt benoemd.

Onderstaande tabel toont een overzicht van de, in dit document, uitgewerkte asset-types.

Asset-type	Beknopte beschrijving
Apparaat	Samenstel van onderdelen of systemen met één of meerdere functies.
Programmatuur	Set programmaregels of software zoals die door een computer kan worden gebruikt om een bepaald resultaat tot stand te brengen.
Data opslag:	
- Database	Data-opslag medium voor diverse programmatuur
- Datashare	Data-opslag medium specifiek op een besturingssysteem
Licentie	Het recht op het gebruik van software/programmatuur en hardware.
Back-up	Vastleggen van vereiste back-up en recovery gegevens.
Document	META data per documentsoort.
LFV	Overall-functie van het asset in een Operationele Technologie (OT) omgeving.
IV-Service	Koppeling van een apparaat aan de Informatievoorziening (IV) ofwel Informatie Technologie (IT) dienstverlening.
Netwerkcommunicatie	Netwerk configuratie items om een asset te kunnen laten communiceren met andere assets.
Locatie	Specificatie van de locatie van het asset.
Rollen	Lijst met verschillende rollen met een bepaalde verantwoordelijkheid t.a.v. data, beheer en onderhoud.

CSR 16.2.2.2 Overzicht Relaties

In paragraaf 16.2.1 wordt een schematische weergave getoond van het te gebruiken datamodel. Hieruit valt te herleiden welke asset-types gebruikt worden en wat de relaties zijn tussen de asset-types. Verwacht wordt dat opdrachtnemer de data kan opleveren middels dit presentatiemodel (attributen, asset-types en relaties) en het bijgevoegde vergelijkbare template "*CMDB IA OT – Informatiebehoefte en presentatie Excel Format* v#.#.*xlsx*".

Zie paragraaf 16.3 voor het gebruik van de attributen en asset-types. In iedere paragraaf wordt onder de uitwerking van het asset-type, een lijst getoond met relaties naar onderliggende asset-types.
Zie paragraaf 16.4 voor een uitleg over het gebruik de relaties in het presentatiemodel en de template.

In de basis kennen we de volgende relaties:

- '1 op 1' relaties: Deze wordt vermeden. Het samenvoegen van asset-types waarbij een één op één relatie te maken valt heeft de voorkeur.

- '1 op n' of 'n op 1' relaties: Hierbij is n een variabele ofwel 1..* (één tot oneindig) ofwel 0..* (nul tot oneindig) en in sommige gevallen 0..1 (nul of één).

  1.. Verwacht minimaal één relatie met gevulde attributen in de database.*
  0.. Verplicht niet het aanwezig zijn van de data. Dit is afhankelijk van de daadwerkelijke omstandigheden.*
  0..1 Verplicht niet de aanwezigheid van data, maar indien aanwezig dan mag er niet meer dan één relatie bestaan.

- 'n op n' relaties: Hierbij is n een variabele ofwel 1..* (één tot oneindig) ofwel 0..* (nul tot oneindig) en in sommige gevallen 0..1 (nul of één).
  Zie daarbij de uitleg van de voorgaande relatie.

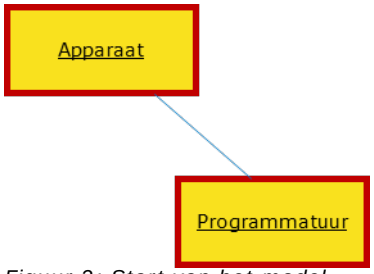
CSR 16.3 Asset-types uitgewerkt

Hieronder volgt een gedetailleerde uitwerking van de in paragraaf CSR 16.2 beschreven asset-types.

In dit model worden per asset-type de in te vullen velden beschreven. Zie paragraaf ‘scope’ (16.1.1) voor uitleg over welk soort velden verplicht zijn of optioneel.
Voor alle datumvelden geldt dat deze worden uitgewerkt volgens de ISO8601: JJJJ-MM-DD.

De start van het presentatiemodel
In paragraaf 16.2.1 wordt het model in zijn geheel visueel weergegeven. De CMDB begint bij de basis asset-types ‘apparaat’ en ‘programmatuur’. Binnen het assetmanagement en deze CMDB wordt gestart met de fysieke (en virtuele) identificatie van de te onderhouden en beheren middelen ofwel apparaten welke aanwezig zijn op een fysieke locatie ten behoeve van de Operationele Technologie (OT) en Industriële Automatisering (IA) installatie. Als basis kan gesteld worden dat dit alle apparaten betreft die niet enkel en specifiek voor de kantoorautomatisering (KA) dienen.

Zie voor de exacte definities de verschillende paragrafen hierna. Grofweg kan gesteld worden dat een apparaat ‘rekenkracht’ levert en dat ‘programmatuur’ de rekenkracht benut. Een apparaat, in de definitie binnen deze CMDB, levert eenzelfde functie zowel ‘in de doos’ als ingebouwd op een locatie. Programmatuur levert pas een bepaalde functie zodra het apparaat is aangesloten en voorzien van voedingsspanning (en eventueel een netwerkaansluiting).



Figuur 2: Start van het model

CSR 16.3.1 Apparaat asset-type

Hieronder volgt een overzicht van de attribuuttypes die in zijn algemeenheid gelden voor alle apparaten. Een apparaat is het samenstel van onderdelen of systemen met één of meerdere functies. Een virtueel apparaat bootst een fysiek apparaat na en kent daardoor nagenoeg dezelfde eigenschappen als een fysiek apparaat en is opgenomen binnen dit asset-type.
ABDL: apparaat.

In de sub-paragrafen kunnen de definities/omschrijvingen gevonden worden van de verschillende soorten hardware.

Let op: Zie paragraaf 16.4 over welke apparatuur minimaal geregistreerd dient te worden.

Attribuut	Definitie	Schrijfwijze	Scope
Entiteit ID	Unieke identificatie van de CI record	Uniek ID zoals geregistreerd/gegenereerd in de database	Minimum set
OMS ID	Veelal wordt het onderhoudsmanagementsysteem (OMS) van RWS (als onderdeel van de CMDB) gebruikt voor registratie van gegevens over het fysieke apparaat. Veel velden zullen in de database van het OMS al aanwezig zijn	De unieke ID waarmee dit asset-type ook in het RWS OMS bekend staat (zoals bouwdeel ID in Ultimo of bouwdeel/DR code in Infor RWS)	Minimum set*
Visuele identificatie	Tagnaam, (TOLGI) codering of herkenbare naam ter identificatie van het asset-type. Fysieke asset; a) naam op het asset, b) naam in de elektrotechnische tekening. Virtuele asset; naamgeving in de hypervisor en vul het attribuut 'serienummer' met de UUID	Open veld	Minimum set*
Omschrijving	Omschrijving van het asset-type zoals deze regulier wordt benoemd of in het OMS bekend is	Open veld	Minimum set*
Soort Apparaat (zie §16.3.1.x)	Functionaliteit van het item / Asset-type	Keuzelijst (niet beperkt tot): Toerenregelinstallatie, PLC, I-O module, Remote I-O module / Kopstation, HMI display, Server, Network DNS, Blade Server, PC Server, Hypervisor-Host, Controller, Desktop, …	Minimum set
Virtueel apparaat?	Betreft het bij dit asset-type virtuele apparatuur	ja/nee	Minimum set
Clusternaam	Indien dit asset-type onderdeel is van een cluster met fysieke hardware en virtuele machines, registreer dan clusternaam om de apparaten te kunnen relateren en groeperen. Indien het een cluster betreft met maar één fysieke server, vul dan de servernaam in (bijv. hostnaam of visuele identificatie)	Open veld	Minimum set*

Serienummer	Het serienummer of UUID zoals veelal gevonden kan worden op het product of in de (virtuele) applicatie	Open veld (mogelijk gebruik OMS ID naar OMS)	Minimum set
Leverancier	De systeem-integrator welke het asset-type nieuw op locatie heeft geïnstalleerd of geplaatst. Niet te verwarren met 'producent' of 'onderhoudsaannemer'. Dit zijn respectievelijk een ander attribuut ofwel rol.	Open veld	Minimum set
Aanschafdatum	Leverdatum van het item. Veelal de start van de garantieperiode van de producent	Volgens ISO 8601: JJJJ-MM-DD	Minimum set
Installatiedatum	Datum dat dit Asset-type op locatie is geïnstalleerd. Veelal de start van de garantieperiode van de leverancier	Volgens ISO 8601: JJJJ-MM-DD	Minimum set
EOL-End of Life datum	Wordt gecommuniceerd door de producent (theoretische levensduur) of RWS OBR (praktische levensduur)	Volgens ISO 8601: JJJJ-MM-DD	Minimum set
EOS-End of Service datum	Wordt gecommuniceerd door de producent en/of leverancier, is een waarschuwing voor de EOL. De producent en/of leverancier biedt geen ondersteuning meer voor het betreffende Asset-type	Volgens ISO 8601: JJJJ-MM-DD	Minimum set
Status Apparaat	Geeft aan in welke toestand het Asset-type zich bevindt	Keuzelijst: Voorraad, Gereserveerd, Actief, Tijdelijke opslag, Vermist, Reparatie/Onderhoud, Af te voeren, Uit beheer, Gedeactiveerd	Minimum set
Mac-adres	Het unieke adres van een netwerkkaart op het netwerk in de vorm van cijfers en letters	Open veld (bij meerdere netwerkpoorten dan meerdere MAC adressen 'komma'-gescheiden registreren)	Minimum set
Opmerking	Opmerkingen over het asset-type, die niet met de attributen zoals hier vermeld, kunnen worden aangeduid	Open veld	Minimum set
OTA(L)-omgeving?	Betreft het een Asset-type in een niet-productie omgeving. Ontwikkel, Test, Acceptatie en Leeromgeving.	Ja/nee	Standaard set
Type server	Het soort server dat het hier betreft	Keuzelijst: N.v.t., Applicatieserver, Databaseserver, Licenseserver, Loadbalancer, Webserver, Werkstation, Overig	Standaard set
Aantal CPU	Beschikbaar aantal CPU's voor dit asset-type	Positief geheel getal	Standaard set
Aantal RAM	Beschikbaar aantal RAM voor dit asset-type	Positief getal in GB's, 1 decimaal nauwkeurig	Standaard set
Aantal Disk	Beschikbaar hoeveelheid DISK ruimte voor dit asset-type. Specificeer ofwel per schijf/partitie ofwel totaal beschikbare ruimte (afhankelijk van de CMDB invulling)	Positief geheel getal in GB's. Meerdere DISK's/partities gescheiden met een ';' beginnende met de primaire partitie (bijv. 100GB;50GB voor resp. OS-partitie en data partitie)	Standaard set

Missie Kritiek Systeem (MKS)?	Betreft het een asset-type voor een RWS 'missie kritiek systeem'. Voor een IA systeem betreft het eigenlijk altijd een MKS.	ja/nee (standaard ja, tenzij anders bekend)	Optioneel
Aanschafprijs	De aanschafprijs is interessant indien het een apparaat betreft wat periodiek onderhouden dient te worden waarbij het geheel vervangen wordt. De aanschafprijs is inclusief engineering, inbedrijfname/systeemintegratie en oplevering	Gehele Euro's	Optioneel
	Onderstaande attributen dienen gevuld te worden bij fysieke apparatuur.		
Attribuut	Definitie	Schrijfwijze	Scope
Producent/Merk	Overkoepelende naam, waaronder de 'Producent' zijn producten verkoopt	Open veld (mogelijk gebruik OMS ID naar OMS)	Minimum set
Type	Typebeschrijving die volgens de producent wordt gehanteerd	Open veld (mogelijk gebruik OMS ID naar OMS)	Minimum set
Ordernummer/ Productnummer	Veelal een bestelnummer afgegeven door de producent voor het product	Open veld	Standaard set*
CPU fabrikant	Fabrikant van de central processing unit	Open veld (veelal Intel of AMD)	Standaard set*
CPU familie	Familie van de central processing unit	Open veld	Standaard set*
CPU type	Type van de central processing unit	Open veld (veelal het aantal cores)	Standaard set*

N.b. attributen waarbij de scope is gemarkeerd met een asterix (*) zijn nieuw toegevoegd aan de asset-type ten opzichte van CSIR versie 2.x.

Gekoppelde (onderliggende) asset-type

De volgende asset-typen zijn gekoppeld aan dit asset-type volgens eerdere CSIR versie 2.x:

- Locatie**
- Verantwoordelijke**
- Documentatie
- Programmatuur

De volgende asset-typen zijn minimaal gekoppeld aan dit asset-type t.b.v. de minimum set aan informatie:

- LFV

**Aangezien veel attributen ook gebruikt zullen worden in het onderhoudsmanagementsysteem (OMS) van de beheerder, volstaat veelal een juiste link naar OMS middels de OMS ID van dit asset-type. Hierna hoeft het asset-type 'Locatie' en 'Verantwoordelijke' niet meer gevuld te worden.

CSR 16.3.1.1 Definitie Toerenregelinstallatie

Volgens de NEN2767: “Installatie die de snelheid van bewegende delen automatisch regelt.” Hieronder vallen onder andere hydrauliek-regelkaart, frequentieregelaar etc.

CSR 16.3.1.2 Definitie Programmable Logic Controller

Volgens de NEN2767: “Verwerkingseenheid, die op basis van de informatie op zijn ingangen, zijn uitgangen aanstuurt, bedoeld om machines en installaties aan te sturen.” Hieronder vallen onder andere processor (CPU), ingangs- en uitgangskaarten etc.

CSR 16.3.1.3 I-O module

Een I-O module (ook wel Input-Output module genoemd) maakt communicatie mogelijk tussen een computersysteem en een randapparaat. Denk hierbij ook aan speciale kaarten om industriële apparatuur (zoals een PLC) te koppelen met de logische functievervullers. Dit kan via digitale, analoge ofwel specifieke communicatie signalen.

CSR 16.3.1.4 Remote I-O module / Kopstation

Onderdeel van een groter (PLC) systeem bestaande uit de centrale processor (zie ‘Definitie Programmable Logic Controller’) en decentrale, gedistribueerde I-O. De remote I-O bevat een kopstation en aanvullende I-O modules waarbij de apparaat soort ‘Remote I-O / Kopstation’ de communicatie verzorgt met de centrale eenheid.

CSR 16.3.1.5 HMI display

Een Human Machine Interface (HMI) display is een (veelal industrieel uitgevoerd) scherm al dan niet uitgevoerd met intern een mini-computer. Vanwege het gemak zijn deze veelal uitgevoerd met een touch-scherm. Een HMI panel bevindt zich veelal in het veldbus netwerk en direct bij de machine of het object. Hieronder valt ook een ‘mobile’ panel.

CSR 16.3.1.6 Definitie Server

Computer die centraal taken afhandelt voor een of meer clients. De computer kan in verschillende gedaantes voorkomen:

- Network DNS: Een Domain Name System (DNS) server die gebruikt wordt om namen van computers en systemen naar numerieke adressen (IP-adressen) te vertalen en omgekeerd.
- Blade server: Een blade server is een fysieke computer waarop programma's draaien om diensten te verlenen aan gebruikers. Een blade server is een computer met een modulair ontwerp dat is geoptimaliseerd om het gebruik van fysieke ruimte en energie te minimaliseren.
- PC server: Een server is een fysieke computer waarop programma's draaien om diensten te verlenen aan gebruikers. Een PC server is een computer in “tower” of “rack” behuizing.
- Server: Een server is een fysieke computer waarop programma's draaien om diensten te verlenen aan gebruikers. Onder deze categorie vallen de overige servers waarbij geen type behuizing wordt aangegeven, bijvoorbeeld de Moxa embedded computers.
- Hypervisor-Host: Fysieke server waarop virtuele servers worden gedeployed.

CSR 16.3.1.7 Definitie Controller

Aansturingcomponent van enclosures of diskkabinetten. Onder de noemer controller valt ook de ‘On Board Administrator’.

CSR 16.3.1.8 Definitie Desktop
Een niet-draagbare computer, uniek geïdentificeerd door een samentrekking van merk en model/type, welke door productmanagement is geclassificeerd als een ”werkstation”.

CSR 16.3.1.9 Definitie Dongle
Een dongle is een klein stukje hardware dat aangesloten wordt op de PC.

CSR 16.3.1.10 Definitie Laptop
Een draagbare computer, voorzien van accu, toetsenbord en een beeldscherm, welke geschikt is voor gebruik buiten de thuis- of kantooromgeving.

CSR 16.3.1.11 Definitie Monitor
Een beeldscherm welke als output device van het mens/machine interface fungeert.

CSR 16.3.1.12 Definitie NAS
Network Attached Storage (NAS) is een opslagmedium op een netwerk (meestal een harde schijf) dat vanaf elke computer aan dat netwerk (mits in bezit van de juiste rechten) kan worden aangesproken.

CSR 16.3.1.13 Definitie Power Supply Unit
Een Power Supply Unit (PSU) is dat onderdeel van elektrische of elektronische apparaten dat de ingangsspanning (afkomstig van het lichtnet of van batterijen) geschikt maakt voor de verschillende onderdelen van die apparaten. Hierbij wordt de spanning vaak getransformeerd naar (een) ander(e) voltage(s) en indien van toepassing kan er een omzetting van wisselspanning naar gelijkspanning (of andersom) plaatsvinden.

CSR 16.3.1.14 Definitie Printer
Een hardcopy uitvoerapparaat.

CSR 16.3.1.15 Definitie SAN
Storage Area Network (SAN): concept van netwerkopslagsystemen met als bedoeling het normale ethernet-netwerk te ontlasten.

CSR 16.3.1.16 Definitie Sensor Module
Een sensor vertaalt de werkelijke toestand naar een digitale toestand zodat de digitale toestand door een applicatie verwerkt kan worden.

CSR 16.3.1.17 Definitie Thin Client
Een relatief zwakke computer die de hoofdmoot van het benodigde computercapaciteit van een server of een centrale computer betrekken en één gebruiker tegelijk "bedient". De kleine computer fungeert daarbij als client ('klant') van de centrale computer.

CSR 16.3.1.18 Definitie Modem

Modem (modulator-demodulator): Een apparaat dat een analoge draaggolf zodanig moduleert, dat deze op betrouwbare wijze digitale informatie kan overdragen, en tevens in staat is om deze analoge, gemoduleerde draaggolf om te zetten naar een originele, digitale boodschap.

CSR 16.3.1.19 Definitie Netwerkbeveiligingsapparaat
We kennen verschillende typen Netwerkbeveiligingsapparaten, bijvoorbeeld:

- Firewall: Veiligheidsbarrière tussen het private bedrijfsnetwerk en het publieke Internet. Dient vooral om infiltratie van buiten het netwerk door hackers te voorkomen, maar kan ook de interne gebruikers beperken in hun verbindingen op het Internet. Een firewall bestaat meestal uit een combinatie van hardware en software.
- IDS (Intrusion Detection System): Een Intrusion Detection System of IDS is een geautomatiseerd systeem dat ongeautoriseerde toegang tot een informatiesysteem of netwerk detecteert.
- Network security device: Een network security device is een systeem om netwerken te beschermen tegen ongeoorloofde toegang van buitenaf, aanvallen, ongewenst verkeer of het voorkomen van aftappen van data.

CSR 16.3.1.20 Definitie Network Card
Een network card is een hardware-onderdeel in een systeem, nodig om dat systeem met andere systemen te laten communiceren hierdoor maakt het systeem deel uit van een computernetwerk.

CSR 16.3.1.21 Definitie Network Module
Een netwerk module is een onderdeel van een netwerksysteem dat in het veld uitwisselbaar is. Een network module is onderdeel van bijvoorbeeld een switch, router of PLC-rack maar kan ook een ethernet media converter zijn.

CSR 16.3.1.22 Definitie Router
Een apparaat, dat actief is op OSI-laag 3 en twee of meer verschillende computernetwerken met elkaar verbindt, door te functioneren als schakelapparaat voor datapakketten.

CSR 16.3.1.23 Definitie Switch
Een apparaat, dat actief is op OSI-laag 2 en op intelligente wijze binnengekomen datapakketten doorgeeft naar alleen die poorten op het netwerk, waar het betreffende datapakket voor bedoeld is.

Dit asset-type kent de volgende subtypes:

- SAN-Switch: Een switch gekoppeld aan een SAN waardoor verschillende servers gebruik kunnen maken van de geboden storage van de SAN.
- Network Switch: Een switch is een apparaat in de infrastructuur van pakket geschakelde netwerken dat tot doel heeft toestellen met elkaar te verbinden door het ontvangen, verwerken en doorzenden van ontvangen frames.

CSR 16.3.1.24 Definitie WLAN access point

Een Wireless LAN (WLAN) access point is een apparaat waarmee draadloze systemen een verbinding op kunnen zetten met een draadloos netwerk volgens één van de wifistandaarden.

CSR 16.3.1.25 Definitie Unmanaged Device
Een apparaat in het OT netwerk of in de IA installatie welke bekend dient te zijn voor assetmanagement, maar geen specifieke configuratie kent.
Een unmanaged apparaat is als het ware een basisapparaat. U voorziet het apparaat van voeding, steekt de netwerkkabels erin of sluit stuurstroom kabels aan en het is klaar voor gebruik. Denk aan een unmanaged switch of glasvezel- naar koperaansluiting converter.

CSR 16.3.1.26 IoT Device
Het Internet of Things (IoT) bestaat uit fysieke voorwerpen, zoals auto's, huishoudelijke apparaten en wearables, die met internet (dus geen veldbus of RWS intern netwerk) zijn verbonden en online gegevens kunnen verzenden. Denk hierbij ook aan het maken van een draadloze verbinding middels 5G, LoRa enz. Een IoT device kan een sensor of netwerk apparaat zijn welke is geprogrammeerd voor één bepaald doel.

CSR 16.3.1.27 Camera (vast)
Camera uitgerust met een vaste oriëntatie en beeldvergroting.
De camera kan individueel gezien worden alsook compleet met behuizing en eventuele verwarmingselement.

CSR 16.3.1.28 Camera (beweegbaar)
Camera uitgerust met een variabele oriëntatie en beeldvergroting.
De camera kan individueel gezien worden alsook compleet met behuizing en eventuele verwarmingselement. Veelal is de besturing (PTZ) van de camera in de bedien- of verkeerscentrale aanwezig.

CSR 16.3.1.29 Intercom
Installatiedeel waarmee tweeweg communicatie mogelijk is met een (alarm)centrale.

CSR 16.3.1.30 Luidspreker
Installatiedeel voor het verspreiden en versterken van geluid.

CSR 16.3.1.31 Versterker
Samenstel van elektrotechnische componenten dat bedoeld is om elektrische signalen te versterken.

CSR 16.3.1.32 Verwijderbare media
Een verwisselbaar medium, een gegevensopslagmedium dat zo is ontworpen dat het eenvoudig in een systeem kan worden geplaatst en eruit kan worden verwijderd. Veelal is het medium aangesloten via USB.

CSR 16.3.1.33 Decoder / encoder
Een decoder is een geheel van functies die een signaal decodeert die volgens een afgesproken protocol gecodeerd is geweest.

Deze functies kunnen volledig softwarematig opgelost worden of hardware-matig in al of niet specifieke decoder-chips.

CSR 16.3.2 Programmatuur asset-type

De (door Opdrachtnemer op te leveren) set programmaregels of software zoals die, op directe of indirecte wijze, door een computer kan worden gebruikt om een bepaald, nader omschreven, resultaat tot stand te brengen. Programmatuur kan worden onderscheiden in Standaard- en Maatwerkprogrammatuur.
ABDL: Programmatuur > Computerprogramma

Let op: Zie paragraaf 16.4 over welke programmatuur minimaal geregistreerd dient te worden.

Attribuut	Definitie	Schrijfwijze	Scope
Parent ID	ID van bovenliggend asset-type	Format: <asset-type>:<Entiteit ID>	Minimum set
Entiteit ID	Unieke identificatie van de CI record	Uniek ID zoals geregistreerd/gegenereerd in de database	Minimum set
Type programmatuur (zie §16.3.2.x)	Het soort applicatie/programmatuur	Keuzelijst: Firmware, Embedded programmatuur, Stuurprogramma, Standalone applicatie, Web applicatie, Client applicatie, Mobiele app(licatie), Plug-in, Clouddienst (SAAS), Serverapplicatie (backend), Besturingssysteem, Antimalware, Overig	Minimum set
Omschrijving	Omschrijving van het asset-type zoals deze regulier wordt benoemd	Open veld	Minimum set*
Status programmatuur	Installatie status van het asset-type	Keuzeveld: Ge-Deïnstalleerd, Geïnstalleerd, Niet geïnstalleerd, Ontwikkelen	Minimum set: *Registreer enkel geïnstalleerde applicaties*
Status updates	Wat is het update regime (bijv. Dagelijks, wekelijks, maandelijks, jaarlijks, ..)	Open veld	Minimum set*
Datum laatste patch	De datum van de laatste patch (en/of wijziging) van dit asset-type	Volgens ISO 8601: JJJJ-MM-DD	Minimum set*
Leverancier	De systeem-integrator welke het asset-type nieuw op locatie heeft geïnstalleerd of geplaatst. Niet te verwarren met 'producent' of 'onderhoudsaannemer'. Dit zijn respectievelijk een ander attribuut ofwel rol.	Open veld	Minimum set
Programmeertaal	Taalcode van de software confodrm ISO-693-3	Open veld (of selectielijst)	Minimum set
Hostnaam	Betreft de unieke naam van de programmatuur op het netwerk in de vorm van letters (oa besturingssysteem)	Open veld	Minimum set
Opmerking	Opmerkingen over het asset-type, die niet met de attributen zoals hier vermeld, kunnen worden aangeduid	Open veld	Minimum set

Cruciaal?	Betreft het programmatuur welke cruciaal is voor een veilige werking van de bediening en besturing conform de machineverordening Denk aan safety-programmatuur, maar ook aan CCTV voor een veilige bediening-op-afstand.	Ja/nee	Standaard set*
Maatwerktype	In hoeverre er hier sprake is van maatwerk en welk type maatwerk het betreft.	Selectielijst: COTS, MOTS (modified of the shelf), Maatwerk	Standaard set
OTA(L)-omgeving?	Betreft het een Asset-type in een niet-productie omgeving. Ontwikkel, Test, Acceptatie en Leeromgeving.	Ja/Nee	Standaard set
Missie Kritiek Systeem (MKS)?	Betreft het een asset-type voor een RWS 'missie kritiek systeem'. Voor een IA systeem betreft het eigenlijk altijd een MKS.	ja/nee (standaard ja, tenzij anders bekend)	Optioneel
	Aanvullende attributen per programmatuur asset-type: - Indien het wel maatwerk programmatuur betreft zijn deze attributen bedoeld t.a.v. ontwikkel-/configuratieprogrammatuur - Indien het geen maatwerk programmatuur betreft, zijn deze attributen (aanvullend op voorgaande) op hetgeen geïnstalleerd is		
Producent/Merk	Overkoepelende naam, waaronder de 'Producent' zijn producten verkoopt.	Open veld	Minimum set
Productnaam	Naam van het product, zoals uitgegeven door de 'Producent'. Indien er zowel een 'Volledige naam' als een afkorting bestaat, dient hier de afkorting te worden ingevuld	Open veld	Minimum set
Versie/Build	Een specifieke variatie of verdere ontwikkeling van een origineel product	Zonder voorloop-V, nummers gescheiden door punten	Minimum set
Aanschafdatum	Leverdatum van het item. Veelal de start van de garantieperiode van de producent	Volgens ISO 8601: JJJJ-MM-DD	Minimum set
Installatiedatum	Datum dat dit Asset-type op locatie is geïnstalleerd. Veelal de start van de garantieperiode van de leverancier	Volgens ISO 8601: JJJJ-MM-DD	Minimum set
EOL End-of-Life datum	Wordt gecommuniceerd door de producent	Volgens ISO 8601: JJJJ-MM-DD	Minimum set
EOS End-of-Service datum	Wordt gecommuniceerd door de producent en/of leverancier, is een waarschuwing voor de EOL. De producent en/of leverancier biedt geen ondersteuning meer voor het betreffende Asset-type	Volgens ISO 8601: JJJJ-MM-DD	Minimum set
Ordernummer/ Productnummer	Veelal een bestelnummer afgegeven door de producent voor het product	Open veld	Standaard set
Aanschafprijs	De aanschafprijs is interessant indien het een apparaat betreft wat periodiek onderhouden dient te worden waarbij	Gehele Euro's	Optioneel

	het geheel vervangen wordt. De aanschafprijs is inclusief engineering, inbedrijfname/systeemintegratie en oplevering		
	Aanvullende attributen specifiek ten behoeve van registratie van logische toegangsbeveiliging ofwel 'Identity and Access Management.		
Attribuut	Definitie	Schrijfwijze	Scope
Soort IAM	Logische toegangsbeveiliging van het asset-type (standaard wachtwoord toegepast ='niet geconfigureerd')	Keuzelijst: N.v.t., Niet volledig ingesteld (wel mogelijk), Wel ingesteld	Standaard set*
AD/LDAP domein	De Windows Active Directory of Linux Lightweight Directory Access Protocol domein server	Open veld (voorbeeld: foo.example.org)	Standaard set*
IAM conform CSIR?	Is de logische toegangsbeveiliging geconfigureerd en procedureel conform cybersecurity eisen (CSIR)	ja/nee	Standaard set*
Wachtwoordbeleid	Is er voor dit asset-type een wachtwoordprocedure aanwezig en door wie wordt het wachtwoord actief beheerd	Keuzelijst: N.v.t., Geen/deels afspraken, Beheer door opdrachtnemer, Beheer door RWS	Standaard set*

N.b. attributen waarbij de scope is gemarkeerd met een asterix (*) zijn nieuw toegevoegd aan de asset-type ten opzichte van CSIR versie 2.x.

<u>Gekoppelde (onderliggende) asset-type</u>

De volgende asset-typen zijn gekoppeld aan dit asset-type volgens eerdere CSIR versie 2.x:

- Netwerkcommunicatie

De volgende asset-typen zijn minimaal gekoppeld aan dit asset-type t.b.v. de minimum set aan informatie:

- LFV
- Back-up
- Database
- Datashare
- Licentie

CSR 16.3.2.1 Definitie Firmware

Firmware is programmatuur die in de hardware is ingeprogrammeerd. Dit kan eenmalig zijn, maar met moderne techniek zoals flashgeheugen kan het mogelijk zijn om firmware te vernieuwen. De CMDB registratie betreft vooral firmware welke te vernieuwen is. Firmware maakt het voor computerprogramma's en besturingssystemen mogelijk om te communiceren met de fysieke hardware en is specifiek voor dit doel bestemd. In sommige gevallen bevat de firmware een configuratie voor specifiek gebruik (denk aan BIOS of de configuratie van een eenvoudige managed switch). Dit valt dan alsnog onder firmware met als maatwerktype MOTS (modified of the shelve).

CSR 16.3.2.2 Definitie Embedded programmatuur

Embedded programmatuur is een programma of broncode wat is gemaakt om hardware en machines te sturen die niet vallen onder wat we in het dagelijkse spraakgebruik zien als computers.
Onder Embedded programmatuur valt bijvoorbeeld (generieke) firmware als besturingsprogramma voor bijvoorbeeld een Programmable Logic Controller (PLC).

CSR 16.3.2.3 Definitie Stuurprogramma

Een specifiek stuk programmatuur die de verbinding legt tussen de hardware en het besturingssysteem. Denk aan een driver voor communicatie tussen SCADA en een PLC.

CSR 16.3.2.4 Definitie Standalone applicatie

Dit betreft een applicatie enkel bedoeld is voor gebruik binnen het besturingssysteem of op de hardware én geen netwerkconnectie benodigd buiten de hardware.

CSR 16.3.2.5 Definitie Web applicatie

Een web-applicatie is programmatuur (veelal een combinatie met een web-service) welke op een (web)server draait en enkel via een webbrower te benaderen is.

CSR 16.3.2.6 Definitie Client applicatie

Client programmatuur is bedoeld voor de gebruiker en bevat een gebruikersinterface met knoppen, labels, invulvelden etc. Een client applicatie werkt zelfstandig (zoals bijvoorbeeld Microsoft Word of Excel) of in combinatie met een server applicatie (zoals bijvoorbeeld een SCADA server of database).

CSR 16.3.2.7 Definitie Mobiele app(licatie)

Een mobiele app betreft programmatuur welke enkel bedoeld is voor gebruik op een mobiel apparaat met specifiek platform zoals Android of iOS (telefoon, tablet enz.) Deze programmatuur communiceert veelal met een server applicatie en kan lokaal toegang hebben tot bestanden, camera of GPS.

CSR 16.3.2.8 Definitie Plug-in

Programmatuur om andere programmatuur uit te breiden. Een plug-in kan niet zelfstandig functioneren en heeft een 'hoofd-applicatie' nodig.

CSR 16.3.2.9 Definitie Clouddienst (SAAS)

Sofware As A Service (SAAS) is dienstverlening waarbij de gebruiker de programmatuur niet hoeft aan te schaffen, maar als ‘online’ dienst wordt aangeboden. De software wordt door de dienstverlener ‘on premise’ geïnstalleerd en kan vanaf een andere applicatie benaderd worden. Nb dit betreft dus geen besturingssysteem die vanaf een andere locatie te benaderen is met bijvoorbeeld ‘Remote Desktop’ of ‘VNC’.

CSR 16.3.2.10 Definitie Server applicatie (backend)
Een server applicatie is de tegenhanger van client applicatie. Een server applicatie betreft bijvoorbeeld de database of uitgebreide scripting waarbij meer rekenkracht benodigd is dan normaliter op een desktop plaats zal vinden. Een server applicatie bevat standaard ook geen gebruikersinterface en bestaat veelal uit Windows Services of Linux Daemons.

CSR 16.3.2.11 Definitie Besturingssysteem
Een verzameling van programmatuur om na het opstarten hiervan de hardware aanstuurt. Het fungeert als medium tussen de hardware en de gebruiker. Het stelt overige programmatuur, op dezelfde hardware, in staat te functioneren zonder rekening te hoeven houden met de verschillende fysieke hardware.

CSR 16.3.2.12 Definitie Antimalware
Programmatuur die ontwikkeld is voor de detectie van, de bescherming tegen en de verwijdering van kwaadaardige programmatuur, scripts e.d.

CSR 16.3.3 Data

De volgende datadragers worden geregistreerd:

- Database
  Een database, gegevensbank of databank is een (meestal digitaal opgeslagen) gegevensverzameling, ingericht met het oog op flexibele raadpleging en gebruik. Databases spelen een belangrijke rol bij het archiveren en actueel houden van gegevens van onder meer de overheid, financiële instellingen en bedrijven, in de wetenschap, en ze worden op kleinere schaal ook privé gebruikt.

- Share
  Het delen van bestanden is de praktijk waarbij digitale media, zoals computerprogramma's, multimedia (audio, afbeeldingen en video), documenten of elektronische boeken worden gedistribueerd of toegang wordt verleend. Het delen van bestanden kan op een aantal manieren worden bereikt. Veelgebruikte methoden voor opslag, verzending en verspreiding zijn onder meer handmatig delen met gebruikmaking van verwijderbare media, gecentraliseerde servers op computernetwerken, op het World Wide Web gebaseerde hyperlinked documenten en het gebruik van gedistribueerde peer-to-peer netwerken.

  We onderkennen o.a. de volgende typen shares:
  i. NFS
     Dit is een netwerkbestandssysteem dat alle bestandssystemen op het netwerk kan delen. Als er een Windows-machine in uw netwerk is, moet u Samba gebruiken. Windows ondersteunt geen NFS; NFS, of Network File System, is een samenwerkingssysteem dat begin jaren 80 door Sun Microsystems is ontwikkeld en waarmee gebruikers bestanden op een externe computer kunnen bekijken, opslaan, bijwerken of delen alsof het een lokale computer is.
  ii. Samba
     Wordt gebruikt voor het delen van Linux-bestanden met Windows-netwerk. De server wordt geconfigureerd om bestanden te delen met elke cliënt op het netwerk zonder om een wachtwoord te vragen.

Hierna volgt de uitwerking van verschillende asset-types behorende bij dataopslag:
- Database
- Datashare

CSR 16.3.3.1 Database asset-type

Dit asset-type wordt als minder (of niet) relevant beschouwd voor IA instandhouding en beheer en is als geheel benoemd als ‘standaard set’.

Het database asset-type betreft de database zelf. Veelal wordt de database voor een specifiek doel of specifieke functie aangemaakt. De programmatuur waarmee de database actief is op het systeem en programmatuur waarmee de database beheerd wordt, dient ook als programmatuur beschreven te worden.

ABDL: Database

Let op: Zie paragraaf 16.4 over welke databases geregistreerd dienen te worden.

Attribuut	Definitie	Schrijfwijze	Scope
Parent ID	ID van bovenliggend asset-type	Format: <asset-type>:<Entiteit ID>	Standaard set
Entiteit ID	Unieke identificatie van de CI record	Uniek ID zoals geregistreerd/gegenereerd in de database	Standaard set
Omschrijving	Omschrijving van het asset-type zoals deze regulier wordt benoemd	Open veld	Standaard set*
Status werking	Is dit asset-type actief	Actief/Inactief	Standaard set
Producent/Merk	Overkoepelende naam, waaronder de ‘Producent‘ zijn producten verkoopt.	Open veld	Standaard set
Productnaam	Naam van het product, zoals uitgegeven door de ‘Producent‘. Indien er zowel een ‘Volledige naam‘ als een afkorting bestaat, dient hier de afkorting te worden ingevuld (bijv. MsSQL, Oracle, Postgres)	Open veld	Standaard set
Versie	Een specifieke variatie of verdere ontwikkeling van een origineel product	Zonder voorloop-V, nummers gescheiden door punten	Standaard set
Soort database	Soort database	Keuzelijst: Relationeel; Flatfile; Distributed; NoSQL; Object-oriented; CAD; Graphic, Overig	Standaard set
Database management systeem	Geef het type van het database systeem. Het betreft de service die het de gebruikers mogelijk maakt om de data te bewerken of doorzoeken.	Keuzelijst: Access, MySQL, Microsoft SQL server, Oracle, DBase, SQLlite, Firebird, PostgreSQL, Overig	Standaard set
OTA(L)-omgeving?	Betreft het een database in een niet-productie omgeving. Ontwikkel, Test, Acceptatie en Leeromgeving.	Ja/Nee	Standaard set
Aantal Disk	Beschikbaar hoeveelheid DISK ruimte voor dit asset-type. Specificeer ofwel per schijf/partitie ofwel totaal beschikbare ruimte (afhankelijk van de CMDB invulling)	Positief geheel getal in GB's. Meerdere DISK's/partities gescheiden met een ';' beginnende met de primaire partitie (bijv. 100GB;50GB voor resp. OS-partitie en data partitie)	Standaard set
Opmerking	Opmerkingen over het asset-type, die niet met de attributen zoals hier vermeld, kunnen worden aangeduid	Open veld	Standaard set
	Aanvullende attributen specifiek ten behoeve van registratie van logische toegangsbeveiliging ofwel ‘Identity and Access Management.		
Attribuut	Definitie	Schrijfwijze	Scope

Soort IAM	Logische toegangsbeveiliging van het asset-type (standaard wachtwoord toegepast =’niet geconfigureerd’)	Keuzelijst: N.v.t., Niet volledig ingesteld (wel mogelijk), Wel ingesteld	Standaard set*
AD/LDAP domein	De Windows Active Directory of Linux Lightweight Directory Access Protocol domein server	Open veld (voorbeeld: foo.example.org)	Standaard set*
IAM conform CSIR?	Is de logische toegangsbeveiliging geconfigureerd en procedureel conform cybersecurity eisen (CSIR)	ja/nee	Standaard set*
Wachtwoordbeleid	Is er voor dit asset-type een wachtwoordprocedure aanwezig en door wie wordt het wachtwoord actief beheerd	Keuzelijst: N.v.t., Geen/deels afspraken, Beheer door opdrachtnemer, Beheer door RWS	Standaard set*

N.b. attributen waarbij de scope is gemarkeerd met een asterix (*) zijn nieuw toegevoegd aan de asset-type ten opzichte van CSIR versie 2.x.

Gekoppelde (onderliggende) asset-type

De volgende asset-typen zijn minimaal gekoppeld aan dit asset-type t.b.v. de minimum set aan informatie:

- Back-up

CSR 16.3.3.2 Datashare asset-type

Dit asset-type wordt als minder (of niet) relevant beschouwd voor IA instandhouding en beheer en is als geheel benoemd als ‘standaard set’.

ABDL: -

Let op: Zie paragraaf 16.4 over welke datashares geregistreerd dienen te worden.

Attribuut	Definitie	Schrijfwijze	Scope
Parent ID	ID van bovenliggend asset-type	Format: <asset-type>:<Entiteit ID>	Standaard set
Entiteit ID	Unieke identificatie van de CI record	Uniek ID zoals geregistreerd/gegenereerd in de database	Standaard set
Omschrijving	Omschrijving van het asset-type zoals deze regulier wordt benoemd	Open veld	Standaard set*
Soort Share		Vaste keuzes: NFS, Samba, SMB, Anders	Standaard set
Status werking	Is dit asset-type actief	Actief/Inactief	Standaard set
Share naam	Share naam-kort (volledige naam in ‘opmerking’ attribuut)	Open veld	Standaard set
OTA(L)-omgeving?	Betreft het een database in een niet-productie omgeving. Ontwikkel, Test, Acceptatie en Leeromgeving.	Ja/Nee	Standaard set
Aantal Disk	Beschikbaar hoeveelheid DISK ruimte voor dit asset-type. Specificeer ofwel per schijf/partitie ofwel totaal beschikbare ruimte (afhankelijk van de CMDB invulling)	Positief geheel getal in GB's. Meerdere DISK's/partities gescheiden met een ';' beginnende met de primaire partitie (bijv. 100GB;50GB voor resp. OS-partitie en data partitie)	Standaard set
Opmerking	Opmerkingen over het asset-type, die niet met de attributen zoals hier vermeld, kunnen worden aangeduid.	Open veld	Standaard set
	Aanvullende attributen specifiek ten behoeve van registratie van logische toegangsbeveiliging ofwel ‘Identity and Access Management.		
Attribuut	Definitie	Schrijfwijze	Scope
Soort IAM	Logische toegangsbeveiliging van het asset-type (standaard wachtwoord toegepast =’niet geconfigureerd’)	Keuzelijst: N.v.t., Niet volledig ingesteld (wel mogelijk), Wel ingesteld	Standaard set*
AD/LDAP domein	De Windows Active Directory of Linux Lightweight Directory Access Protocol domein server	Open veld (voorbeeld: foo.example.org)	Standaard set*
IAM conform CSIR?	Is de logische toegangsbeveiliging geconfigureerd en procedureel conform cybersecurity eisen (CSIR)	ja/nee	Standaard set*
Wachtwoordbeleid	Is er voor dit asset-type een wachtwoordprocedure aanwezig en door wie wordt het wachtwoord actief beheerd	Keuzelijst: N.v.t., Geen/deels afspraken, Beheer door ON, Beheer door RWS	Standaard set*

N.b. attributen waarbij de scope is gemarkeerd met een asterix (*) zijn nieuw toegevoegd aan de asset-type ten opzichte van CSIR versie 2.x.

CSR 16.3.4 Licentie asset-type

Het recht op het gebruik van software/programmatuur en hardware.
ABDL: licentie
Let op: Zie paragraaf 16.4 over welke licenties geregistreerd dienen te worden.

Attribuut	Definitie	Schrijfwijze	Scope
Parent ID	ID van bovenliggend asset-type	Format: <asset-type>:<Entiteit ID>	Minimum set
Entiteit ID	Unieke identificatie van de CI record	Uniek ID zoals geregistreerd/gegenereerd in de database	Minimum set
Omschrijving	Omschrijving van het asset-type zoals deze regulier wordt benoemd	Open veld	Minimum set*
Soort licentie	Het soort licentie dat is afgesloten	Keuzeveld: Proprietary, Open Source, geen (PD)	Minimum set
Locatie	De (digitale) locatie waar het bestand te vinden is en beheerd wordt. Indien het geen digitale locatie betreft, specificeer dan de papieren locatie conform het 'locatie asset-type'.	Open veld (bijvoorbeeld het document beheer systeem 'Meridian' of een netwerklocatie)	Standaard set
Leverancier	De systeem-integrator welke het asset-type nieuw op locatie heeft geïnstalleerd of geplaatst. Niet te verwarren met 'producent' of 'onderhoudsaannemer'. Dit zijn respectievelijk een ander attribuut ofwel rol.	Open veld	Standaard set*
Ordernummer/ Productnummer	Veelal een bestelnummer afgegeven door de producent voor het product	Open veld	Standaard set
Support contract?	Is er een supportcontract afgesloten met de producent waarop RWS en indirect de leverancier kan terugvallen	ja/nee	Standaard set
Licentie contract?	Is er een licentie contract afgesloten waarbij licenties actueel gehouden worden door de producent. Veelal in de vorm van subscription/abonnement	ja/nee	Standaard set
Berekeningsbasis	De wijze waarop de licentiekosten berekend worden, die men verschuldigd is als gevolg van het aanvaarden van de licentie	Keuzeveld: Per gebruiker, Per installatie, Per gebruik, Overig	Standaard set
Aantal licenties	Het aantal legale, ingekochte licenties van deze soort en berekeningsbasis	Positief geheel getal	Standaard set
EOL End-of-Life datum	Einde looptijd van de licentie	Volgens ISO 8601: JJJJ-MM-DD	Standaard set
Opmerking	Opmerkingen over het asset-type, die niet met de attributen zoals hier vermeld, kunnen worden aangeduid	Open veld	Optioneel*

N.b. attributen waarbij de scope is gemarkeerd met een asterix (*) zijn nieuw toegevoegd aan de asset-type ten opzichte van CSIR versie 2.x.

CSR 16.3.5 Back-up asset-type

Het betreft hier twee eisen die per back-up geregistreerd worden:

1. Er moet periodiek een back-up worden gemaakt of geverifieerd.
2. Daarbij moet periodiek worden getest of de back-up voldoet voor een goede recovery. Zijn de media bijvoorbeeld leesbaar? De resultaten van die test moeten elders ook worden vastgelegd (buiten de CMDB).

ABDL: Back up

Let op: Zie paragraaf 16.4 over welke back-ups geregistreerd dienen te worden.

Attribuut	Definitie	Schrijfwijze	Scope
Parent ID	ID van bovenliggend asset-type	Format: <asset-type>:<Entiteit ID>	Minimum set
Entiteit ID	Unieke identificatie van de CI record	Uniek ID zoals geregistreerd/gegenereerd in de database	Minimum set
Backupnaam	Naam van de backup of omschrijving van het asset-type zoals deze regulier wordt benoemd	Open veld	Minimum set*
Locatie	De (digitale) locatie waar het bestand te vinden is en beheerd wordt. Indien het geen digitale locatie betreft, specificeer dan de papieren locatie conform het 'locatie asset-type'.	Open veld (bijvoorbeeld het document beheer systeem 'Meridian' of een netwerklocatie)	Minimum set
Datum laatste Back-up	De datum van de laatste backup-up	Volgens ISO 8601: JJJJ-MM-DD	Minimum set
Datum laatste Back-up verificatie	De datum van de laatste backup-up verificatie	Volgens ISO 8601: JJJJ-MM-DD	Minimum set
Datum laatste recovery test	De datum van de laatste succesvolle recovery test	Volgens ISO 8601: JJJJ-MM-DD	Minimum set
	Aanvullende gegevens, per back-up, ten aanzien van het product waarmee de backup is gemaakt en waarmee de recovery is uitgevoerd:		
Attribuut	Definitie	Schrijfwijze	Scope
Producent/Merk	Overkoepelende naam, waaronder de 'Producent' zijn producten verkoopt.	Open veld	Standaard set
Productnaam	Naam van het product, zoals uitgegeven door de 'Producent'. Indien er zowel een 'Volledige naam' als een afkorting bestaat, dient hier de afkorting te worden ingevuld.	Open veld	Standaard set
Versie/Build	Een specifieke variatie of verdere ontwikkeling van een origineel product	Zonder voorloop-V, nummers gescheiden door punten	Standaard set

Ordernummer/ Productnummer	Veelal een bestelnummer afgegeven door de producent voor het product	Open veld	Standaard set
Opmerking	Opmerkingen over het asset-type, die niet met de attributen zoals hier vermeld, kunnen worden aangeduid	Open veld	Optioneel*

N.b. attributen waarbij de scope is gemarkeerd met een asterix (*) zijn nieuw toegevoegd aan de asset-type ten opzichte van CSIR versie 2.x.

CSR 16.3.6 Document asset-type

ABDL: Document.
De volgende documenten dienen geregistreerd te worden in de CMDB.

In het kader van beheer en onderhoud:

1. Beheer en onderhouds-instructie; Specifieke IA en OT onderhoudsinstructies per asset-type.
2. Backup procedure; (Geteste) backup procedures voor besturingssystemen en programmatuur.
3. Vervangings-instructie; (Geteste) recovery procedures.
4. Wachtwoord procedure; Procedure voor wachtwoord wijziging op locatie inclusief de beschrijving waar deze dienen te worden opgeslagen.
5. Status van het onderhoud; Toestandsrapportages, is de onderhoudsbehoefte van de beheerder met budget aanvraag.
6. Update/patch procedure; werkwijze voor het implementeren of doorvoeren van een update en/of patch

In het kader van data-communicatie en netwerkontwerp:

7. Fysieke topologie; Het fysieke ontwerp van het netwerk. Het samenhangend geheel van elementen (o.a. routers, switches, koperdragers en glasvezels) waarover gegevens elektronisch worden getransporteerd.
8. Logisch topologie; hoe gegevens daadwerkelijk wordt overgedragen in een netwerk onafhankelijk van het fysieke ontwerp. Een voorbeeld van een logisch netwerk is het Virtual Private Network (VPN).
9. IP-plan van datacommunicatie-netwerk; Netwerkschema met fysieke apparatuur en verbindingen tussen de apparaten (bij voorkeur zonder daadwerkelijk IP adres, maar met een verwijzing naar de CMDB asset).
10. Netwerkprotocol beschrijving; Een set van regels en afspraken voor de representatie van data, signalering, authenticatie en foutdetectie, nodig voor het verzenden van informatie over een communicatiemedium.

In het kader van programmatuur:

11. Documentatie t.b.v. programmatuur; Een functionele en technische beschrijving van de programmatuur met bedieninstructies.
12. Escrow; Escrow omvat alle niet openbaargemaakte informatie die de opdrachtgever redelijkerwijs nodig heeft voor foutherstel, onderhoud, verder ontwikkelen en beheer van de standaardprogrammatuur zodat hij daarvan het overeengekomen gebruik kan blijven maken. Escrow voldoet aan hetgeen dienaangaande ten tijde van het afsluiten daarvan op de Nederlandse markt gebruikelijk is. COTS programmatuur valt buiten de scope van Escrow

Voor ieder document dienen de volgende attributen geregistreerd te worden:

Attribuut	Definitie	Schrijfwijze	Scope
Parent ID	ID van bovenliggend asset-type	Format: <asset-type>:<Entiteit ID>	Minimum set
Entiteit ID	Unieke identificatie van de CI record	Uniek ID zoals geregistreerd/gegenereerd in de database	Minimum set
Documentnaam	Documentnaam of omschrijving van het asset-type zoals deze regulier wordt benoemd	Open veld	Minimum set*
Soort document	Het soort document (indien geen eenduidig doel, kies dan wat het beste past)	Keuzelijst: Beheer en onderhouds-instructie, Backup procedure, Vervangings-instructie, Wachtwoord procedure, Status van onderhoud, Update/patch procedure, Fysieke topologie, Logische topologie, IP-plan van datacommunicatie-netwerk, Netwerkprotocol beschrijving, Documentatie t.b.v. programmatuur, Escrow, Overig	Minimum set
Datum laatste wijziging	De datum van de laatste wijziging van dit asset-type	Volgens ISO 8601: JJJJ-MM-DD	Minimum set
Aanleiding wijziging	Referentie aan changeproces	Open veld	Minimum set
Gewijzigd door	Naam, organisatie en contactgegevens van de persoon die de laatste wijziging van de documentatie heeft doorgevoerd.	Open veld	Minimum set
Locatie	De (digitale) locatie waar het bestand te vinden is en beheerd wordt. Indien het geen digitale locatie betreft, specificeer dan de papieren locatie conform het ‘locatie asset-type’.	Open veld (bijvoorbeeld het document beheer systeem ‘Meridian’ of een netwerklocatie)	Minimum set
Opmerking	Opmerkingen over het asset-type, die niet met de attributen zoals hier vermeld, kunnen worden aangeduid	Open veld	Optioneel*
	Aanvullende attributen specifiek ten behoeve van registratie van ESCROW deponering.		
Attribuut	Definitie	Schrijfwijze	Scope
Datum eerste deponering	Datum waarop de eerste deponering van de Escrow heeft plaatsgevonden	Volgens ISO 8601: JJJJ-MM-DD	Standaard set
Datum laatste deponering	Datum waarop de laatste deponering van de Escrow heeft plaatsgevonden	Volgens ISO 8601: JJJJ-MM-DD	Standaard set
Escrow agent	Naam, organisatie en contactgegevens van de Escrow agent. De in te zetten Escrow agent heeft expertise om het gedeponeerde product en bijbehorende materialen te controleren op aanwezigheid, volledigheid en bruikbaarheid	Open veld	Standaard set

N.b. attributen waarbij de scope is gemarkeerd met een asterix (*) zijn nieuw toegevoegd aan de asset-type ten opzichte van CSIR versie 2.x.

CSR 16.3.7 LFV asset-type

Het asset-type LFV (Logische Functie Vervuller) verwijst naar de overall-functie van het asset in een OT omgeving. Het is mogelijk dat meerdere assets zijn verbonden aan een LFV asset-type ofwel meerdere LFV asset-types zijn verbonden aan een enkel asset (n:n relatie). LFV betreft een functie en geen fysiek ding. LFV kan het beste vergeleken worden met een SATO functie/installatie (Specifieke Aspecten TunnelOntwerp) welke in tunnels gebruikt wordt als standaard naamgeving en installatie-codering.
ABDL: -

Toekomst LFV asset-type
Ten aanzien van dit gedefinieerde LFV asset-type, zal dit asset-type worden doorontwikkeld naar een definitieve versie. Tot dat moment is het aan te raden om de SATO naamgeving en codering aan te houden als LFV naam. Het is echter een open veld zolang er landelijk geen definitie is voor de logische functies ofwel LFV's van alle soorten beheerobjecten.

Attribuut	Definitie	Schrijfwijze	Scope
Parent ID	ID van bovenliggend asset-type	Format: <asset-type>:<Entiteit ID>	Minimum set*
Entiteit ID	Unieke identificatie van de CI record	Uniek ID zoals geregistreerd in de database	Minimum set*
LFV Naam	Logische functievervuller waar asset-type onderdeel van uit maakt (unieke naam van installatie bv 'video/CCTVinstallatie', 'besturingssysteem' etc.)	Open veld (Unieke naam of ID die dient als verwijzing naar een '*functionele decompositie*')	Minimum set*
Opmerking	Opmerkingen over het asset-type, die niet met de attributen zoals hier vermeld, kunnen worden aangeduid	Open veld	Minimum set*

N.b. attributen waarbij de scope is gemarkeerd met een asterix (*) zijn nieuw toegevoegd aan de asset-type ten opzichte van CSIR versie 2.x.

CSR 16.3.8 IV-Service asset-type

Dit asset-type is optioneel. Registratie en bewerking van de asset-informatie is niet van toepassing voor de primaire onderhoudspartij van het object.

Het asset-type IV-Service verwijst naar de assets afkomstig uit dienstverlening vanuit informatievoorziening (IV), ook wel kantoorautomatisering of IT. Denk hierbij aan ontsluiting van een object aan de 'backbone'-glasvezelnetwerk en het gebruik van standaard ingekochte producten (bijvoorbeeld 'routeerbare noodstop', 'Audio', 'Video', 'bediening' etc.)
Deze komen tezamen op fysieke locaties en het is voor het assetmanagement van belang om te weten wie verantwoordelijk is. Dit asset-type staat toe dat het apparaat wél geregistreerd wordt in de *CMDB Industriële Automatisering en Cybersecurity* als fysiek onderdeel van het object, met als doel om expliciet vast te leggen dat deze in beheer is bij een IV-service dienstverlener.
ABDL: -

Attribuut	Definitie	Schrijfwijze	Scope
Parent ID	ID van bovenliggend asset-type	Format: <asset-type>:<Entiteit ID>	Optioneel*
Asset ID	Unieke ID/naam van de IV Service exact zoals geregistreerd in de CMDB voor IV-assets.	Open veld (let op, dit ID dient identiek te zijn aan een in TopDesk geregistreerd Asset ID)	Optioneel*
Omschrijving	Omschrijving van de IV Service zoals geregistreerd in de CMDB voor IV-assets.	Open veld	Optioneel*
Opmerking	Opmerkingen over het asset-type, die niet met de attributen zoals hier vermeld, kunnen worden aangeduid	Open veld	Optioneel*

N.b. attributen waarbij de scope is gemarkeerd met een asterix (*) zijn nieuw toegevoegd aan de asset-type ten opzichte van CSIR versie 2.x.

Indien het een apparaat gekoppeld is aan een IV-Service, dan wordt de programmatuur inclusief onderliggende asset-types niet geregistreerd in de *CMDB Industriële Automatisering en Cybersecurity*, maar in de IV-Service CMDB.
Bijvoorbeeld: Een netwerk-router geplaatst en in beheer bij het CIV als IV dienstverlening (IV-Service) wordt als apparaat geregistreerd met een gekoppeld IV-Service asset-type om duidelijk te maken dat het apparaat in beheer is bij het CIV. Koppeling met de technische decompositie in het OMS blijft mogelijk.

CSR 16.3.9 Netwerkcommunicatie asset-type

Het netwerkcommunicatie asset-type bevat alle netwerk configuratie items welke benodigd zijn om een (bovenliggend) gekoppeld asset-type te kunnen laten communiceren met andere assets. Het betreft een 'aanvullende' lijst met attributen die niet zelfstandig zou kunnen bestaan.

Afhankelijk van de bovenliggende asset-type wordt een deel van de attributen gevuld. Bijvoorbeeld, voor een web-applicatie zal enkel een 'communicatie protocol' worden gedefinieerd. Een PLC kent een 'IPv4 adres' met 'Communicatie protocol' voor communicatie met SCADA en soms een 'Bus adres' voor communicatie met een serieel veldbus netwerk (o.a. modbus). Het is dus goed mogelijk dat er meerdere (deels gevulde) entiteiten voor dezelfde bovenliggende programmatuur aangemaakt dienen te worden.
ABDL: -
Let op: Zie paragraaf 16.4 over welke netwerkgegevens geregistreerd dienen te worden.

Attribuut	Definitie	Schrijfwijze	Scope
Parent ID	ID van bovenliggend asset-type	Format: <asset-type>:<Entiteit ID>	Minimum set*
Entiteit ID	Unieke identificatie van de CI record	Uniek ID zoals geregistreerd in de database	Minimum set*
Status werking	Is dit asset-type actief	Actief/Inactief	Minimum set*
Opmerking	Opmerkingen over het asset-type, die niet met de attributen zoals hier vermeld, kunnen worden aangeduid	Open veld	Minimum set*
	Onderstaande attributen zijn specifiek ten behoeve van registratie van verschillende soorten communicatieprotocollen die worden gebruikt om informatie over het netwerk te versturen.		
Communicatie protocol	Transportlaag: TCP, UDP of ISO-on-TCP(rfc1006) en het poortnummer (bv 80, 443, 22 etc.)	Format: <transportlaag> <poortnummer>	Minimum set
	Onderstaande attributen zijn specifiek ten behoeve van registratie van het unieke adres dat een apparaat op internet of in een lokaal netwerk of veldbus identificeert. Deze wordt geconfigureerd in de programmatuur (veelal het besturingssysteem).		
IPv4 adres	Internet protocol v4 adres in de vorm van cijfers	Format: xxx.xxx.xxx.xxx	Minimum set
IPv4 Subnet	Internet protocol v4 subnet in de vorm van cijfers	Format: xxx.xxx.xxx.xxx (xx)	Minimum set
IPv4 Default gateway	Internet protocol v4 adres als gateway in de vorm van cijfers	Format: xxx.xxx.xxx.xxx	Minimum set
IPv6 adres	Internet protocol v6 adres en prefix	Format: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx (/xx)	Minimum set
IPv6 Default gateway	Internet protocol v6 adres als gateway	Format: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx	Minimum set
Bus adres	Netwerkadres anders dan IP (bv Profibus, Modbus etc.)	Open veld	Minimum set**
DNS	Domain name system	Open veld	Standaard set
	Onderstaande attributen zijn specifiek ten behoeve van registratie van netwerksegmentatie middels virtuele netwerken.		
VLAN	Virtueel LAN nummer	Numeriek	Minimum set**
VPN	Gekoppeld (RWS) VPN naam	Open veld	Minimum set**

	Indien netwerkgegevens gekoppeld zijn aan een fysieke poort (bijvoorbeeld op een server), registreer dan het poortnummer welke aan de buitenkant van de fysieke apparaat gevonden kan worden.		
Fysieke poort	Fysieke poortnummer op de switch, router of van de server	Open veld, veelal numeriek	Standaard set

N.b. attributen waarbij de scope is gemarkeerd met een asterix (*) zijn nieuw toegevoegd aan de asset-type en CSIR ten opzichte van CSIR versie 2.x.

N.b. attributen waarbij de scope is gemarkeerd met een dubbele asterix (**) zijn nieuw toegevoegd aan de CMDB, maar zijn logischerwijs wel onderdeel van een vereist IP plan.

CSR 16.3.10 Locatie asset-type

Veel van de velden in het locatie asset-type kunnen of zullen aanwezig zijn in het onderhoudsmanagementsysteem (OMS) of documentbeheersysteem (bijv. Meridian) van waaruit het asset of documentatie wordt beheerd. Indien de benodigde velden allen in het OMS of documentbeheersysteem aanwezig zijn volstaat het veelal om voor overige asset-types te verwijzen naar het OMS middels het veld 'OMS ID' in plaats van de velden op te nemen in een nieuwe database.
ABDL: Locatie
Let op: Zie paragraaf 16.4 over welke locatie gegevens geregistreerd dienen te worden.

Attribuut	Definitie	Schrijfwijze	Scope
Parent ID	ID van bovenliggend asset-type	Format: <asset-type>:<Entiteit ID>	Minimum set
Entiteit ID	Unieke identificatie van de CI record	Uniek ID zoals geregistreerd/gegenereerd in de database	Minimum set
Locatienaam	Fysiek adres (vestiging, objectjectnaam etc) en/of netwerk locatie van het bovenliggende asset-type	Open veld (mogelijk gebruik OMS ID naar OMS)	Minimum set
Overige plaatsbepaling zoals kamernummer	Specificeer zo specifiek mogelijk met bijvoorbeeld ruimtenaam, kamer en kastnummer	Open veld (mogelijk gebruik OMS ID naar OMS)	Standaard set
RD X- coördinaat	Geometrie: Volgens Rijksdriehoek	Open veld (mogelijk gebruik OMS ID naar OMS)	Standaard set
RD Y- coördinaat	Geometrie: Volgens Rijksdriehoek	Open veld (mogelijk gebruik OMS ID naar OMS)	Standaard set
WGS Latitude	Geometrie: World Geodetic System 1984 coördinaten	Open veld (mogelijk gebruik OMS ID naar OMS)	Optioneel (indien geen RD X)
WGS Longitude	Geometrie: World Geodetic System 1984 coördinaten	Open veld (mogelijk gebruik OMS ID naar OMS)	Optioneel (indien geen RD Y)
BAG ID	Indien het een pand betreft geregistreerd in de Basisregistratie Adressen en Gebouwen (BAG). ID zoals in de BAG geregistreerd	Open veld (mogelijk gebruik OMS ID naar OMS)	Optioneel
Rack (kastnummer)	Nummer of naam zoals overeenkomstig met de elektrotechnische tekening of aanwezig op de buitenkant van de kast	Open veld (mogelijk gebruik OMS ID naar OMS)	Optioneel
Rack (kasthoogte)	Benodigde ruimte voor het asset-type in de kast (in cm's of HE etc.)	Open veld (mogelijk gebruik OMS ID naar OMS)	Optioneel
Opmerking	Opmerkingen over het asset-type, die niet met de attributen zoals hier vermeld, kunnen worden aangeduid	Open veld	Optioneel*

N.b. attributen waarbij de scope is gemarkeerd met een asterix (*) zijn nieuw toegevoegd aan de asset-type ten opzichte van CSIR versie 2.x.

CSR 16.3.11 Rollen asset-type

Veel van de velden in het 'Rollen' asset-type kunnen of zullen aanwezig zijn in het onderhoudsmanagementsysteem (OMS) van waaruit het asset wordt beheerd. Indien de benodigde velden allen in het OMS aanwezig zijn volstaat het veelal om voor overige asset-types te verwijzen naar het OMS middels het veld 'OMS ID' in plaats van de velden op te nemen in een nieuwe database.

Iedere rol kan een bepaalde verantwoordelijkheid hebben. Alhoewel de definitie van ieder attribuut een globale verantwoordelijkheid beschrijft, worden de verantwoordelijkheden van iedere rol niet vastgelegd binnen dit asset-type. Het is daardoor mogelijk dat de definitie per asset, beheerobject of regio net iets anders is georganiseerd. Het is aan de beheerder van het object om aan te geven welke persoon de rol draagt.
ABDL: - (verantwoordelijke)
Let op: Zie paragraaf 16.4 over welke rollen geregistreerd dienen te worden.

Attribuut	Definitie	Schrijfwijze	Scope
Parent ID	ID van bovenliggend asset-type	Format: <asset-type>:<Entiteit ID>	Minimum set
Entiteit ID	Unieke identificatie van de CI record	Uniek ID zoals geregistreerd/gegenereerd in de database	Minimum set
Eigenaar	Eindverantwoordelijke	Open veld (mogelijk gebruik OMS ID naar OMS)	Minimum set
Beheerder	Veelal het district, regio of dienstonderdeel RWS, maar kan ook een specifiek persoon of bedrijf zijn	Open veld (mogelijk gebruik OMS ID naar OMS)	Minimum set
Configuratiemanager		Open veld (mogelijk gebruik OMS ID naar OMS)	Minimum set
Gegevenseigenaar	Veelal een technisch adviseur of medewerker informatievoorziening	Open veld (mogelijk gebruik OMS ID naar OMS)	Minimum set
Afdelingshoofd		Open veld (mogelijk gebruik OMS ID naar OMS)	Standaard set
Assetmanager		Open veld (mogelijk gebruik OMS ID naar OMS)	Standaard set
Changemanager		Open veld (mogelijk gebruik OMS ID naar OMS)	Standaard set
Problemmanager		Open veld (mogelijk gebruik OMS ID naar OMS)	Standaard set
Voorkeurscontract	Primaire onderhoudscontract op het bovenliggende asset-type	Open veld (mogelijk gebruik OMS ID naar OMS)	Optioneel
Opmerking	Opmerkingen over het asset-type, die niet met de attributen zoals hier vermeld, kunnen worden aangeduid	Open veld	Optioneel*

N.b. attributen waarbij de scope is gemarkeerd met een asterix (*) zijn nieuw toegevoegd aan de asset-type ten opzichte van CSIR versie 2.x.

CSR 16.4 Gebruik van de Excel Template

Deze paragraaf maakt gebruik van de Excel Template “CMDB IA OT – Informatiebehoefte en presentatie Excel Format”. Hierna te noemen: ‘Excel template’ of ‘template’.

N.b. De Excel template is bedoeld als ‘middel’. Idealiter is er voor alle beoogde gebruikers een ‘CMDB tool’ beschikbaar waarmee de registratie, relaties en beheer van de data overzichtelijk en efficiënt kunnen worden uitgevoerd.

In paragraaf 16.3 wordt uitleg gegeven over hoe te starten met het vullen van de CMDB middels het presentatiemodel. Allereerst dienen werkafspraken gemaakt te worden met de beheerder/ontvanger van de informatie. Zie hiervoor de volgende paragraven.

Tabbladen
De Excel template bestaat uit verschillende tabbladen ‘TP <*naam*>’ waarbij de <*naam*> overeenkomstig is met het asset-type in dit document. In ieder tabblad beginnend met ‘TP’ bevindt zich een tabel met koptekst. De koptekst en omschrijving tooltip komen overeen met attribuutnaam, definitie en schrijfwijze van dit document.

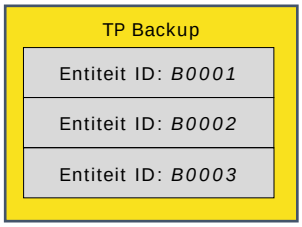
Tabellen
De koptekst en enkele regels daaronder zijn onderdeel van een Excel tabel. Iedere tabel begint met de naam ‘TB_<*naam*>’ waarbij de <*naam*> overeenkomstig is met het asset-type in dit document. Indien het aantal regels uitgebreid dient te worden, voeg dan regels toe aan de tabel zodat de opmaak van de velden gelijk blijft.
Zie paragraaf 16.4.2.3 voor uitgebreidere informatie over de mogelijke invulling van de tabbladen.

CSR 16.4.1 Relaties aanbrengen in de Excel Template

Middels de velden ‘Parent Id’ en ‘Entiteit Id’ kan een relatie aangebracht worden tussen de verschillende asset-types in de verschillende tabbladen.

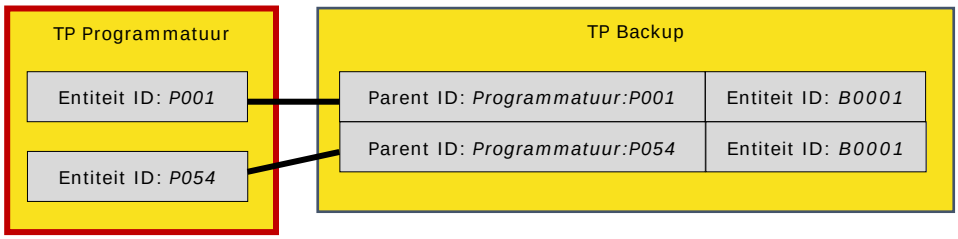
Entiteit ID

Dit betreft de unieke identificatie van de gegevens binnen één tabel. In iedere tabel kan dit genummerd worden van 1 tot n. Indien er nog niets is bedacht vanuit een voorgaande CMDB Excel Template, mag een eigen wijze van nummering worden bedacht. Voor deze unieke identificatie kan ook gebruik worden gemaakt van een unieke identificatie uit de database vanwaar de data is geëxporteerd naar de Excel Template.



Indien een Parent ID wordt gebruikt, zie uitleg hierna, kan het voorkomen dat meerdere unieke assets van een bovenliggend asset-type verwijzen naar hetzelfde gegeven in de onderliggende asset-type. Hierbij zal de Entiteit ID inclusief de daaropvolgende attributen identiek zijn, maar kan door middel van de kolom Parent ID aangegeven worden dat dezelfde data aan meerdere bovenliggende asset-types toebehoord.

Voorbeeld:
Er is tweemaal programmatuur geïnstalleerd waarvan één back-up gemaakt wordt voor beide programmatuur.
In dit geval is de back-up eenmaal aanwezig, maar wordt met dezelfde Entiteit ID en attribuut gegevens twee maal in de tabel ‘TP Backup’ geplaatst.
Vervolgens wordt met twee verschillende Parent ID’s (één per regel) de relatie gelegd naar twee bovenliggende programmatuur asset-types.

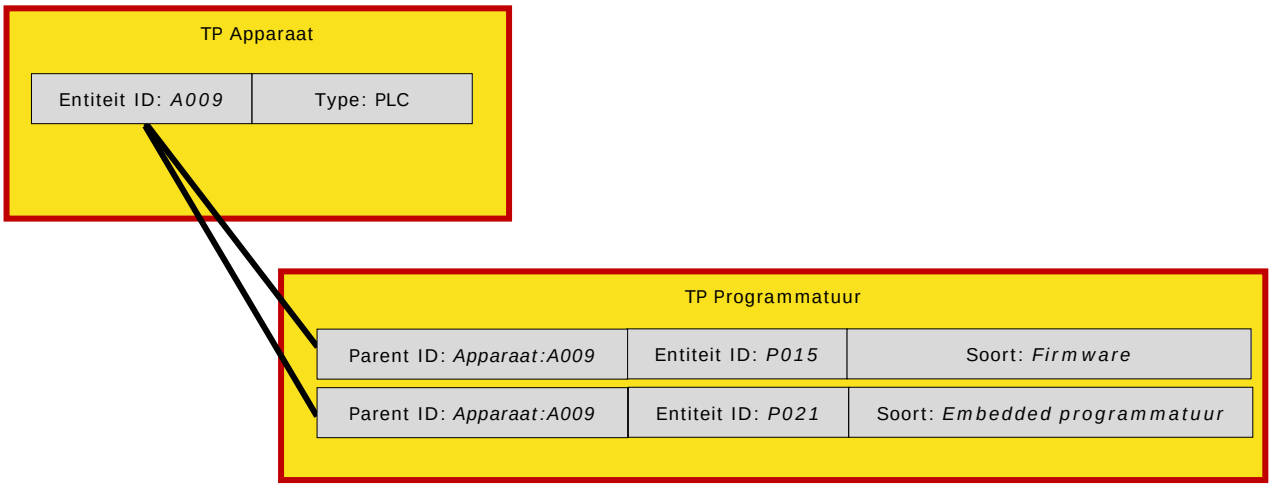


Parent ID

Een Parent ID verwijst naar een bovenliggende ouder binnen de ouder-kind relatie. Het format waarmee de parent ID wordt opgebouwd bestaat uit de asset-type naam (bijvoorbeeld: “Programmatuur”) gevolgd door een dubbele punt (“:”) en de unieke entiteit ID in de bovenliggende asset-type tabel.

Voorbeeld:
In de ‘apparatuur’ asset-type tabel bevindt zich een fysieke PLC met uniek ‘Entiteit Id’=A009. Op deze fysieke PLC is firmware aanwezig en embedded programmatuur. Deze firmware en embedded programmatuur worden geregistreerd in de tabel ‘programmatuur’. Deze krijgen een uniek nummer binnen de tabel ‘programmatuur’, in dit voorbeeld ‘Entiteit Id’=P015 voor de firmware en ‘Entiteit Id’=P021 voor de embedded programmatuur.

Invulling van ‘Parent Id’ en ‘Entiteit Id’ volgens bovenstaande voorbeeld in beide asset-type tabellen:



CSR 16.4.2 Best practice aanpak data uitwisseling

De Excel template is een ‘middel’ om data uit te wisselen via verschillende stakeholders. Deze template bevat alle informatiebehoefte ten aanzien van Industriële Automatisering en Cybersecurity. In overleg met de IA adviseur, IV adviseur en/of assetmanager worden afspraken gemaakt ten aanzien van het gebruik van de Excel template.

CSR 16.4.2.1 Workflow

Een voorstel van te maken afspraken in logische werkvolgorde:

1. Bepaal welke middelen ingezet worden voor data uitwisseling.
   Indien gebruik wordt gemaakt van een bestaande OMS (bijvoorbeeld Ultimo, Infor of Meridian) dan is er een mogelijke overlap aan informatiebehoefte.
   Ditzelfde geldt ook indien gevraagd wordt om specifieke informatie voor bijvoorbeeld ‘DVM’ installaties met specifieke CMDB informatiebehoefte.
   Hanteer hiervoor het volgende ‘waterval’ model voor de, in dit document, beschreven informatiebehoefte:
   - ✓ Probeer zoveel als mogelijk de attributen in het onderhoudsmanagementsysteem (OMS) en bij documenten als META-informatie in het document-beheer-systeem te registreren (zie ook CSR 16.4.4).
     Indien alle beschikbare informatie in het OMS geregistreerd kan worden, dan wordt geen kopie van dezelfde informatie verwacht in de Excel template.
   - ✓ Wat overblijft; probeer zoveel als mogelijk de attributen in een, eventueel, aanwezig CMDB te registreren (bijvoorbeeld een bestaande Excel).
   - ✓ Wat overblijft; registreer de overgebleven attributen in de Excel template behorende bij dit document.

   Omdat een OMS continu in ontwikkeling is, blijkt het onmogelijk om een lijst op te stellen met de gegevens in een OMS overeenkomstig met de informatiebehoefte vanuit dit document.
   Paragraaf CSR 16.4.4 bevat een kort overzicht met de vermoedelijk overeenkomstige informatiebehoefte volgens ‘Ultimo Rijkswaterstaat’. Hier zijn echter geen rechten aan te ontlenen en de tabel dient bij ieder project opnieuw vastgesteld te worden.

2. Bepaal welke asset-types (tabbladen) en kolommen gevuld dienen te worden met data, in de Excel template.
   Onderstaande rollen vanuit de beheerder (informatie ontvangst en oplevering) kunnen hierbij betrokken worden:
   - ✓ Medewerker Informatievoorziening (MIV); deze persoon levert en ontvangt alle informatie over het object inclusief CMDB informatie. Deze persoon zou minimaal betrokken moeten zijn bij het opleveren van de CMDB informatie.
   - ✓ Gegevenseigenaar; dit is veelal een technisch adviseur of assetmanager van het object en is inhoudelijk verantwoordelijk voor de opgeleverde gegevens.
   - ✓ Integraal Beveiligingsspecialis (IBS); deze persoon is in de regio betrokken bij algemene cybersecurity vraagstukken.
   - ✓ IA adviseur; deze medewerker is inhoudelijk betrokken t.a.v. het beheer van de IA installaties vanuit het team assetmanagement.
   - ✓ Assetmanager; deze persoon is algemeen betrokken bij het beheer voor het object vanuit het team assetmanagement.

   Gezamenlijk met één of meerdere personen met bovenstaande rollen wordt bepaald welke gegevens worden uitgewisseld.
   Let daarbij op de minimale informatiebehoefte, versus de standaard informatiebehoefte, versus de al aanwezige/gewenste data vanuit de beheerder. Bij nieuwbouw dient alle data aangeleverd te worden. Ten aanzien van optionele data dient hiervoor overleg met de beheerder te worden gevoerd waarbij de beheerder dient te onderbouwen of- en waarvoor

deze data gebruikt zal worden.

3. Bepaal op welke wijze de koppeling gemaakt wordt tussen bestaande bronnen (o.a. OMS en DMS) en de Excel template.
   Hiervoor zijn meerdere mogelijkheden waarbij het gebruik van de kolom ‘OMS ID’ een logische keuze kan zijn om de verbinding te leggen met een registratie in het OMS.
   Indien, bijvoorbeeld, alle gewenste gegevens in het asset-type ‘Locatie’ al beschikbaar is in een OMS, dan behoeft deze tab niet opnieuw gevuld te worden, maar kan vanuit de Excel template in het asset-type ‘Apparaat’ de verbinding gemaakt worden met de unieke identificatie van het asset in het OMS. Ditzelfde kan ook gelden voor individuele attributen.

   Zorg er altijd voor dat er een unieke relatie ontstaat tussen verschillende bronnen waarbij data tot eenzelfde asset behoort!

4. Bepaal wat er ingevuld moet worden indien data niet voor handen is.
   Indien, bijvoorbeeld, een end-of-service onbekend is dan kan de kolom leeg blijven, maar er kan ook voor worden gekozen om een dummy-datum in te vullen.

5. Indien er nog geen informatie voorhanden is in een Excel template (het betreft nieuwe data en geen wijziging), dan wordt eerst een ‘concept’ opgesteld. Opdrachtnemer gaat voor enkele assets de informatiebehoefte in de Excel template vullen. Dit concept wordt beoordeeld door de IV adviseur in samenspraak met de assetmanager of IA adviseur. Gezamenlijk wordt nogmaals gekeken wat te doen met ontbrekende data.
   Na het opstellen en goedkeuring van het ‘concept’, kan de opdrachtnemer alle kolommen vullen.

CSR 16.4.2.2 Uitwisseling van data

De uit te wisselen data is bedrijfsvertrouwelijk. Data uitwisseling dient volgens CSIR bijlage CSR 1 plaats te vinden.

Daarnaast kunnen specifieke afspraken gemaakt worden met de IV adviseur, IA adviseur en/of assetmanager gezamenlijk met de opdrachtnemer, ten aanzien van het opdelen van de data op basis van ‘need to know’. Globaal kan de CMDB-data in drie ‘informatie-groepen’ opgedeeld worden:

1. Basis informatie
   Inhoud: Algemene informatie zoals merk, model, leverancier, locatie in het netwerk, algemene beschrijving.
   Ten aanzien van de Excel template beperkt het zich tot apparaat-gegevens, locatie en rollen.

2. Specifieke Informatie
   Inhoud: Gedetailleerde technische specificaties zoals servergeheugen, processor, BIOS-versie; bij programmatuur het serienummer, locatie van de softwareopslag, specifieke backup configuraties.
   Ten aanzien van de Excel template wordt de basis aangevuld behoudens de tabbladen met beveiligingsgevoelige informatie.

3. Beveiligingsgevoelige Informatie
   Inhoud: Onderhoudsgegevens zoals IP-adressen, MAC-adressen, netwerkconfiguraties, wachtwoorden of andere beveiligingsgevoelige informatie.
   Ten aanzien van de Excel template betreft het vooral de tabbladen met netwerkcommunicatie en mogelijk de velden ten aanzien van Identity and Access Management (IAM). Wachtwoorden en andere beveiligingsgevoelige informatie behoren niet via de Excel template uitgewisseld te worden.

Let op: wat buiten scope gehouden dient te worden van de Excel template:
-Wachtwoordbeheer – (zie hiervoor de CSIR)
-Accountbeheer, wie heeft toegang tot welk systeem.

CSR 16.4.2.3 Data-vulling

Hieronder volgt, per asset-type, een best-practice ten aanzien van het aanleveren van de data en vulling van de asset-type tabel. Met name de vraag “Welke … moet ik registreren?” wordt hiermee beantwoord.
Voor de inhoudelijke beschrijving van ieder asset-type (de attributen) dient gekeken te worden naar de beschrijving in paragraaf 16.3. Zie paragraaf 16.4.2.4 over hoe om te gaan met registratie van onbekende of ontbrekende attributen.

Asset-type “Apparaat”:
Het asset-type ‘apparaat’ kent een grote overlap met de informatiebehoefte vanuit assetmanagement. Met name de fysieke apparaten ‘buiten’ zullen voor een groot deel ook aanwezig zijn in een bestaand onderhoudsmanagementsysteem. Ditzelfde zal ook gelden voor de documentatie in het documentmanagementsysteem.

1. Ieder apparaat (fysiek en virtueel) dient geregistreerd te worden als:
   a. Apparaat bevat programmatuur/configuratie (cybersecurity) of
   b. Apparaat raakt een faaldefinitie van het object (assetmanagement) of
   c. Apparaat is nodig voor het in-stand-houden ofwel beheren van het object (wijzigingen).
2. Fysieke apparaten kan je aanraken en zien. Virtuele apparaten zijn veelal geconfigureerd op een hypervisor. De informatiebehoefte voor virtuele apparaten is nagenoeg identiek aan de informatiebehoefte voor fysieke apparaten.

Als voorbeeld; een hypervisor (server) kent programmatuur voor het aanmaken van virtuele apparaten.
- Het fysieke apparaat (server) wordt geregistreerd in de tabel ‘apparaat’ en de programmatuur t.b.v. virtualisatie, in de tabel ‘programmatuur’.
- Daarnaast wordt ieder virtueel apparaat geregistreerd in de tabel ‘apparaat’ met eventueel bijbehorende, daarop aanwezige, programmatuur.
- De verbinding of groepering tussen het fysieke apparaat en de virtuele apparaten wordt gelegd met het attribuut ‘cluster’ die uniek en identiek dient te zijn voor deze groep.

Asset-type “Programmatuur”:
Onder programmatuur (en software) wordt bij IA verstaan alle software die benodigd is om IA-systemen te laten functioneren. Dit is belangrijk wanneer we spreken over ‘IA software beheer’. Middels ‘inventarisatie’ tools kan automatisch gescand worden op geïnstalleerde programmatuur. Het is handmatig nagenoeg niet compleet te beheren welke programmatuur met versie, updates en installatiedatum is geïnstalleerd. Deze informatie dient beperkt te worden tot het ‘hoogst-noodzakelijke’.
Als hoogstnoodzakelijk, definiëren we drie doelen waarvoor de CMDB minimaal gevuld dient te worden met programmatuur:

- ✓ Beschikbaarheid; Ten aanzien van beschikbaarheid van de installatie dient datgene wat *bewust* geïnstalleerd wordt geregistreerd te zijn in de CMDB. Onder *bewust* verstaan we de programmatuur die bij naam genoemd wordt bij de start van de installatie.
  Denk hierbij o.a. aan:
  - Microsoft Excel versie *xyz*.
  - Siemens WinCC OA versie *xyz*.
  - Rockwell RSLogix versie *xyz*.

  Automatisch mee-geïnstalleerde afhankelijke programmatuur (dependencies) behoeven niet genoemd te worden in de CMDB.

- ✓ Recovery; Alle stappen die uitgevoerd worden om een uitgevallen functie (bijvoorbeeld ‘bediening’ of ‘omroep’) mogelijk te maken dienen beschreven te worden in een recovery handleiding. Alle programmatuur die benodigd is (waar naar verwezen wordt tijdens het volgen van een recovery handleiding) dient minimaal geregistreerd te worden in de CMDB. Denk hierbij minimaal aan de programmatuur waarvan een *backup* gemaakt wordt. Deze backup kan enkel aan programmatuur hangen in de CMDB.

Denk hierbij o.a. aan:
- Microsoft Windows versie *xyz*.
- Embedded programmatuur PLC *abc* versie *xyz.*

✓ Beheer en Onderhoudbaarheid; Ten aanzien van beheer en onderhoud is het belangrijk om te weten welke programmatuur actief is en de functie van het object afhankelijk van is. Hiervoor is het noodzakelijk om te weten wanneer programmatuur end-of-life is. Of er bijvoorbeeld licenties voor nodig zijn, want die dienen ook geregistreerd te worden in de CMDB. Maar denk ook aan de firmware versie van een PLC. Bij vervanging van de PLC-CPU is de firmware versie van belang om te kunnen bepalen of de programmatuur daadwerkelijk 1 op 1 geladen kan worden.

Asset-type “Database”:
Alle databases welke handmatig zijn aangemaakt dienen geregistreerd te worden in de CMDB.
Denk hierbij o.a. aan:
- Zelf gemaakte SQL databases voor registratie van gegevens.
- CSV export via een automatisch script.

Niet geregistreerd hoeft te worden:
- Automatisch gemaakte SCADA alarmlog database.
- Historische datalog (geconfigureerd via SCADA) voor eventlogging.

Asset-type “Datashare”:
Alle datashares waar data geplaatst wordt of is waarbij een persoon of geautomatiseerd script/programmatuur gebruik van kan maken ten behoeve van een willekeurige functie dienen geregistreerd te worden.
Denk hierbij o.a. aan:
- Een gedeelde locatie waar software of back-ups beschikbaar zijn.
- Een gedeelde locatie waar CSV exports worden opgeslagen voor gebruik door derden.

Asset-type “Licentie”:
Alle licenties benodigd om de functie van het object volledig uit te kunnen voeren dienen geregistreerd te worden.

Asset-type “Back-up”:
Alle gemaakte back-ups in het kader van backup & recovery dienen geregistreerd te worden.

Asset-type “Document”:
Alle soorten documentatie, benoemd in dit document dienen, geregistreerd te worden met de voorgeschreven attributen als ‘meta-data’.

Asset-type “LFV”:
Het invullen van de ‘LFV’ gaat enkel in overleg met de asset beheerder.

Asset-type “Netwerkcommunicatie”:
Alle toegewezen IP-adressen, inclusief gateway/subnet/vlan, dienen minimaal geregistreerd te worden in de CMDB onder ‘netwerkcommunicatie’. Ook wanneer deze toegewezen zijn aan een apparaat maar (nog) niet in gebruik zijn. Dit geldt ook voor bus-adressen (oa Modbus).

Ten aanzien van de gebruikte communicatieprotocollen zijn deze van belang voor alle geconfigureerde zaken die afwijken van het standaard communicatieprotocol.
Niet geregistreerd hoeft bijvoorbeeld te worden:
- OPC UA (discovery), deze gebruikt standaard poort 4840.
- MS SQL Server, deze gebruikt standaard poort TCP1433.

Wel geregistreerd dient bijvoorbeeld te worden:
- Wanneer voor MS SQL Server een afwijkende communicatiepoort is geconfigureerd.
- Wanneer er een web-service actief is anders dan poort 80 of 8080.

Asset-type “Locatie”:
Alle fysieke apparaten dienen een ‘locatie’ te hebben.

Asset-type “Rollen”:
Alle apparaten dienen een verwijzing te hebben naar ‘rollen’.
Rollen t.b.v. programmatuur (bijv. ‘functioneel beheerder’ en/of ‘technisch beheerder’) dienen geregistreerd te worden bij de asset. Eventueel kan de relatie met de programmatuur verduidelijkt worden in het veld ‘opmerkingen’.

CSR 16.4.2.4 Onbekende of ontbrekende attributen

Voor het kunnen beheren van de CMDB data is het van belang om te weten of data ‘ontbreekt’ of welke data ‘niet van toepassing’ is. Hiervoor hanteren we in de communicatie middels de Excel Template, onderstaande standaard waarden welke toegepast worden per ontbrekend attribuut:

Attribuut data	Beschrijving
-	(streepje) Het attribuut kan op dit moment nog niet gevuld worden omdat de gegevens niet beschikbaar zijn. In de toekomst kan dit attribuut wel gevuld worden zodra de informatie bekend is gemaakt. Denk hierbij aan de ‘End-of-Service’ datum of een ‘OMS ID’.
nb	(Afkorting ‘Niet bekend’) Het attribuut zal wel van toepassing zijn, maar op dit moment kan het attribuut niet geregistreerd worden. Denk hierbij aan de scope-beperking van de opdrachtnemer of het achterhalen van de attribuut data is te ingrijpend voor de functie van het object.
nvt	(Afkorting ‘Niet van toepassing’) Het attribuut kan niet gevuld worden en zal in de toekomst voor het asset-type ook niet gebruikt gaan worden.
<leeg>	(Veld leeg laten of ‘spatie’) Attributen gemarkeerd als ‘(optioneel)’ mogen leeg blijven of voorzien worden van een streepje ‘-‘. Denk hierbij aan een optioneel opmerking of een aanschafprijs attribuut.

CSR 16.4.3 Voorbeeld uitwerking
Hieronder volgt een voorbeeld uitwerking van een eenvoudige installatie.

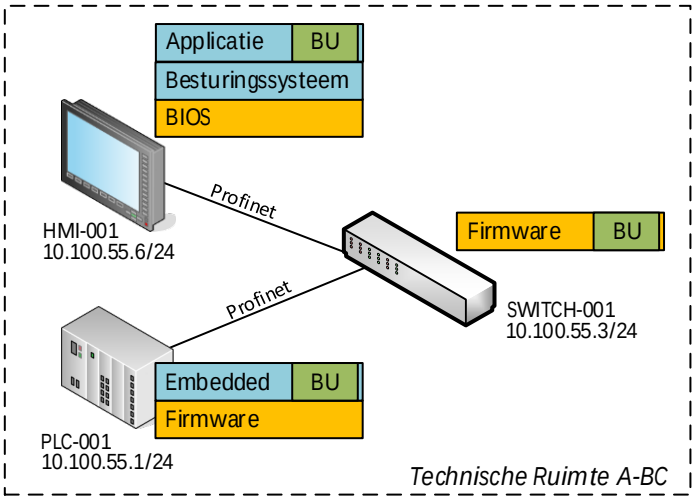
Het voorbeeld bevat een (niet tot in detail uitgewerkt) praktijkvoorbeeld.
In dit geval betreft het registratie van:

- De locatie (Locatie)
- De apparatuur (Apparaat)
- De firmware/bios, besturingssysteem en software/applicatie (Programmatuur)
- De back-up van enkele programmatuur (Back-up)
- De netwerk IP adres gegevens (Netwerkcommunicatie)

De installatie, geplaatst in een technische ruimte, bestaat uit de volgende fysieke apparaten:

- Object PLC welke de besturing en bewaking realiseert van het object,
- HMI welke de (lokale) bediening mogelijk maakt van het object,
- Netwerk switch welke communicatie tussen de PLC, HMI en bediening op afstand realiseert.

Onderstaande figuur geeft weer welke apparatuur, programmatuur en back-ups aanwezig zijn en geregistreerd dienen te worden.
Deze voorbeeld casus is uitgewerkt als ‘dummy’ in de Excel template. Waar nodig, zijn de attributen met fictieve informatie gevuld.



Figuur: Eenvoudige illustratie van de voorbeeld uitwerking

CSR 16.4.4 AM informatieregistratie vs CMDB informatiebehoefte

Zonder hieraan rechten te kunnen ontlenen, geven onderstaande tabellen aan welke CMDB attributen in het huidige Ultimo OMS en Meridian DMS beschikbaar zijn en waarbij deze overeenkomen met de CMDB informatiebehoefte. Deze lijst is aan verandering onderhevig afhankelijk van de versie-ontwikkeling van het OMS en DMS.

Het betreft de volgende asset-types die mogelijke overlap hebben met het OMS, Ultimo en DMS, Meridian:

- Apparaat (voorlopig enkel fysieke apparaten en geen virtuele apparaten)
- Locatie
- Rollen (enkel/hooguit de minimum set)
- Document (geen Escrow)

CMDB Asset-type	CMDB Attribuut	Ultimo locatie	Ultimo veld	Opmerking
Apparaat	OMS ID	Bouwdeel 'header'	Bouwdeel *(nummer)*	Gelijk houden in beide!
Apparaat	Omschrijving	Bouwdeel 'header'	Bouwdeel *(tekst)*	Gelijk houden in beide!
Apparaat	Producent/Merk	Bouwdeel tab 'Algemeen II'	Merk	
Apparaat	Type	Bouwdeel tab 'Algemeen II'	Type	
Apparaat	Serienummer	Bouwdeel tab 'Algemeen II'	Serienummer	
Apparaat	Leverancier	Bouwdeel tab 'Algemeen I'	Leverancier	
Apparaat	Aanschafdatum	Bouwdeel tab 'Algemeen II'	Bouwjaar	Veelal is jaartal voldoende (zoals Ultimo)
Apparaat	Installatiedatum	Bouwdeel tab 'Algemeen II'	Installatiedatum	
Apparaat	End-of-Life datum	Bouwdeel tab 'Algemeen II'	Theoretisch vervangmoment	Dit wordt berekend met het veld 'Theoretische levensduur'. Het theoretisch vervangmoment dient binnen de End-of-Service datum te vallen.
Apparaat	End-of-Service datum	Bouwdeel tab	Theoretisch vervangmoment	Dit wordt berekend met het veld

CMDB Asset-type	CMDB Attribuut	Ultimo locatie	Ultimo veld	Opmerking
		'Algemeen II'		'Theoretische levensduur'. Voeg in het veld 'Bouwdeel informatie' toe dat de rest-levensduur wordt bepaald/ingekort door de End-of-Service datum van het bouwdeel.
Apparaat	Opmerking	Bouwdeel tab 'Algemeen II'	Bouwdeel informatie	Dit veld kan voor meer opmerkingen gebruikt worden
Locatie	OMS ID	Bouwdeel 'header'	Bouwdeel *(nummer)*	Gelijk houden in beide!
Locatie	Locatienaam	Bouwdeel tab 'Algemeen I'	Systeemdeel, Object, Locatie	Combinatie van velden is mogelijk
Locatie	Overige plaatsbepaling zoals kamernummer	Bouwdeel tab 'Algemeen I'	Object, Locatie, Ruimte, Magazijn	Combinatie van velden is mogelijk
Locatie	RD X / RD Y	Bouwdeel tab 'Algemeen I'	Coördinaten RD X / RD Y	
Locatie	WGS Latitude / WGS Longitude	Bouwdeel tab 'Algemeen I'	Coördinaten RD X / RD Y	Enkel mogelijk indien de WGS locatie wordt omgezet in RD locatie!
Locatie	BAG ID	-		Eventueel kan afgesproken worden de BAG ID in het veld 'Bouwdeel informatie' te plaatsen: "BAG ID = *[xyz]*".
Locatie	Rack (Kastnummer)	Bouwdeel tab 'Algemeen II'	Kastnummer	
Locatie	Rack (Kasthoogte)	Bouwdeel tab 'Algemeen II'	Hoogte	
Locatie	Opmerking	Bouwdeel tab 'Algemeen II'	Bouwdeel informatie	Dit veld kan voor meer opmerkingen gebruikt worden
Rollen	OMS ID	Bouwdeel 'header'	Bouwdeel *(nummer)*	Gelijk houden in beide!
Rollen	Eigenaar	Bouwdeel tab	Eigenaar	

CMDB Asset-type	CMDB Attribuut	Ultimo locatie	Ultimo veld	Opmerking
		'Algemeen I'		
Rollen	Beheerder	Bouwdeel tab 'Algemeen I'	Beheerder	
Rollen	Configuratiemanager	Bouwdeel tab 'Algemeen I'	Onderhouder	Let op! Vulling van 'configuratiemanager' als 'onderhouder' in Ultimo dient vastgesteld te worden vooraf aan de levering van de CMDB data. Hier is geen eenduidige 1 op 1 relatie vooraf vast te stellen.
Rollen	Gegevenseigenaar	Bouwdeel tab 'Algemeen II'	Discipline	Let op! Vulling van 'gegevenseigenaar' als 'discipline' in Ultimo dient vastgesteld te worden vooraf aan de levering van de CMDB data. Hier is geen eenduidige 1 op 1 relatie vooraf vast te stellen.
Rollen	Voorkeurscontract	Bouwdeel tab 'Algemeen I'	Voorkeurscontract	
Rollen	Opmerking	Bouwdeel tab 'Algemeen II'	Bouwdeel informatie	Dit veld kan voor meer opmerkingen gebruikt worden

CMDB Asset-type	CMDB Attribuut	Meridian locatie	Meridian veld	Opmerking
Document	Documentnaam	Eigenschappen/Properties	RegistratieNr / Omschrijving	Het 'registratieNr' wordt automatisch gegenereerd en dit is de systeem-documentnaam. De 'Omschrijving' zal handmatig ingevuld moeten worden met de (originele)naam van het document.
Document	Soort document	Eigenschappen/Properties	Documentsoort1 / 2 / 3	Het vereiste 'documentsoort' om overeen te komen met het CMDB attribuut 'Soort document' zal op 1 van de drie nivo's te vinden zijn.
Document	Datum laatste wijziging	Revisions	Wijzigingsdatum	
Document	Aanleiding wijziging	Revisions	Wijziging	
Document	Gewijzigd door	Revisions	Modified by	
Document	Locatie		-	Als Meridian standaard is aangewezen, dan vervalt dit veld.
Document	Opmerking	Eigenschappen/Properties	Commentaar	

Bijlage CSR 17 Beveiligingshuisregels

CSR 17.1 Doelstelling

Aanvallen van buitenaf, malware en andere security incidenten kunnen ervoor zorgen dat er schade ontstaat aan een object of de industriële automatisering die het object bestuurt. Opdrachtnemer dient daarom huisregels te hebben voor het werken binnen en met IA-omgevingen. Deze huisregels helpen bij het op een verantwoorde en cyberveilige manier te werken. Net als bij de persoonlijke veiligheid geldt: we werken veilig of we werken niet.

CSR 17.2 Best practices

De beveiligingshuisregels dienen kenbaar te worden gemaakt aan alle vaste medewerkers op het object en te worden verstrekt aan alle bezoekers aan het object. Hierbij dienen duidelijk naam en telefoonnummer van de objectbeheerder en het telefoonnummer voor storingsmeldingen te worden vermeld.

De beveiliging van bedienbare objecten, verkeersposten en bediencentrales is een verantwoordelijkheid van ons allemaal. Van beheerder, monteur tot bedienaar: samen helpen we misbruik en fouten te voorkomen.

De beveiligingshuisregels bevatten ten minste het volgende:

a. Toegang tot deze locatie is alleen toegestaan voor wie zich heeft aangemeld bij de objectbeheerder;
b. Meld het vermoeden van een beveiligingsincident net zoals andere storingen. Geef bij de melding aan dat het (mogelijk) om een beveiligingsincident gaat. Voorbeelden zijn virusbesmetting, plotseling en onverklaarbaar verlies van zicht op of controle over het object, een verloren USB-stick/laptop, het object komt plotseling in beweging zonder dat hiervoor opdracht is gegeven door de bedienaar;
c. Loopt er iemand op het object die je niet kent? Ga na of deze persoon op het object hoort te zijn en of deze persoon toegang mag hebben tot de IA apparatuur;
d. Wijzig systemen alleen met toestemming van de objectbeheerder. Meld je bij werkzaamheden aan en af bij de objecteigenaar. Zorg voor een werkvergunning als deze nodig is voor de werkzaamheden;
e. Het is voor gebruikers niet toegestaan zelf software te installeren;
f. Leen passen en sleutels niet uit zonder toestemming van de objectbeheerder. Persoonlijke accounts en wachtwoorden deel je nooit met anderen, ook niet met collega's;
g. Voorkom dat informatie in verkeerde handen kan vallen. Bij twijfel over het delen van informatie, raadpleeg de objectbeheerder vóórdat informatie wordt gedeeld;
h. Sla wachtwoorden beveiligd en niet zichtbaar voor anderen op. Gebruik hiervoor een elektronische wachtwoordkluis;
i. Mobiele apparatuur mag niet onbeheerd worden achtergelaten;
j. Sluit bij onderhoudswerkzaamheden alleen USB-sticks of apparaten aan die op malware zijn gescand. Scan de aangesloten apparatuur ook achteraf nogmaals op malware. Sluit nooit persoonlijke apparatuur zoals telefoons aan op de IA-omgeving;
k. Sluit (internet)verbindingen (wifi, 4G, 5G, Bluetooth, etc) af op apparatuur die wordt aangesloten op de IA-omgeving, vóórdat de apparatuur gekoppeld wordt. Sluit geen draadloze netwerken aan op de IA-omgeving;
l. Creëer geen eigen netwerken en koppelingen. Alleen een RWS-netwerk mag gebruikt worden voor externe verbindingen;
m. Log systemen uit na gebruik op en ruim apparatuur op (netwerkkabels, USB-sticks, externe harde schijven, etc);
n. Haal na gebruik de sleutel uit het slot of de schakelaar. Berg sleutels veilig op;
o. Sluit deuren en ramen af en doe ze op slot. Doe serverkasten en werkruimtes op slot als je er niet bezig bent en altijd als je weg gaat;
p. Spreek elkaar aan op het niet naleven van deze regels.

Bijlage CSR 18 Back-up en recovery

CSR 18.1 Doelstelling

Door apparatuur die kapot gaat, een security incident, of andere oorzaak, is het mogelijk dat een back-up moet worden teruggezet. Het is dan van belang dat er een actuele, werkende back-up is. Een goede back-up strategie zorgt ervoor dat het back-up proces voorspoedig verloopt met een minimale impact op de operationele status van het object.

CSR 18.2 Best practices

Een goede back-up strategie voorziet tenminste in het volgende:

a. Bepaal van welke systemen op het object back-ups gemaakt dienen te worden;
b. Zorg dat de benodigde materialen aanwezig zijn;
c. Maak voor elk systeem een duidelijk stappenplan voor het maken van de back-ups, toegepast op de specifieke situatie;
d. Maak voor elk systeem een duidelijk stappenplan voor het terugzetten van de back-ups, toegepast op de specifieke situatie;
e. Maak back-ups van elk systeem;
f. Controleer of de gemaakte back-ups de informatie bevatten die nodig is voor een succesvolle restore en of deze correct functioneren;
g. Sla de back-ups op, zowel on-site als off-site;
h. Bij wijzigingen aan een systeem, maak een nieuwe back-up;
i. Controleer de back-up's jaarlijks middels een recovery test.

Benodigde materialen

Verschillende materialen kunnen benodigd zijn voor het maken en controleren van back-ups. Voorbeelden hiervan zijn:

a. Sleutel voor het openen van de serverkast / besturingskast;
b. Versleutelde harde schijf;
c. Back-up software;
d. Toetsenbord en muis;
e. Externe DVD-ROM drive en DVD-ROM's;
f. Inloggegevens van de systemen waarvan een back-up gemaakt wordt;
g. Werkvergunning.

Bijlage CSR 19 Intellectueel eigendom

CSR 19.1 Doelstelling

RWS maakt gebruik van bedrijf kritische Programmatuur ter aansturing of ondersteuning van de maatschappelijk vitale processen. Daarmee ontstaat afhankelijkheid van de leveranciers, die deze Programmatuur (op maat) ontwikkelden en/of moeten onderhouden. Het staken van de bedrijfsactiviteiten of het failliet gaan van de leverancier introduceert serieuze risico's voor de continuïteit van de maatschappelijk vitale processen van RWS. Om deze continuïteitsrisico's te mitigeren moet RWS in de contracten goede afspraken maken over de Intellectuele Eigendomsrechten van Maatwerk Programmatuur en/of een Escrow overeenkomst aangaan voor Standaardprogrammatuur waarvan de intellectuele eigendomsrechten bij Opdrachtnemer of derden liggen.

Intellectueel Eigendom

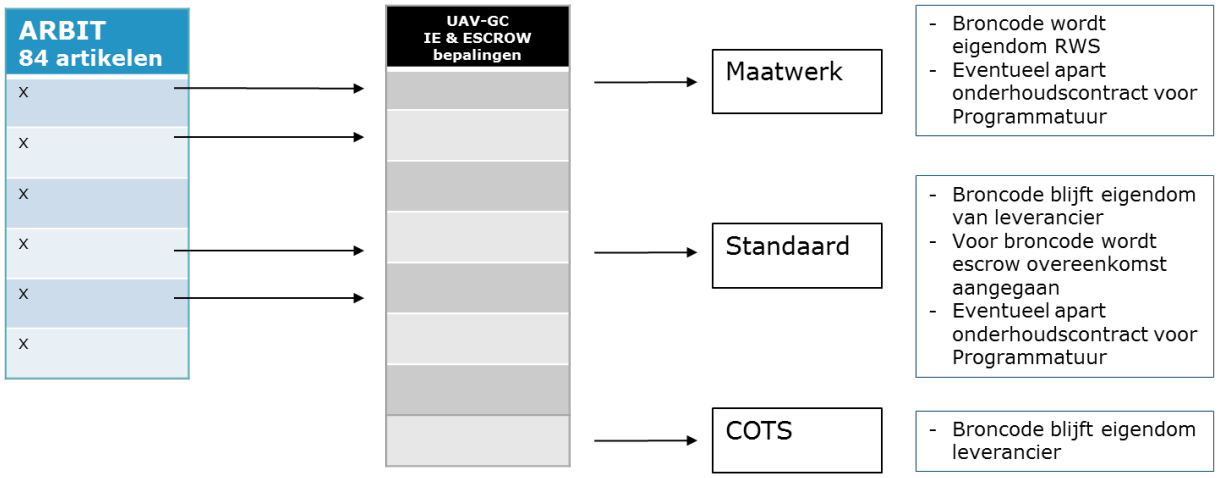
Intellectueel Eigendomsrechten zijn exclusieve rechten van rechthebbenden op een voortbrengsel van de menselijke geest. Een voorbeeld daarvan is het auteursrecht, waar Programmatuur onder valt. IE-rechten stellen de eigenaar in staat het werk (Programmatuur) te exploiteren.

Inkoopvoorwaarden

RWS maakt gebruik van de Algemene Rijksinkoopvoorwaarden bij IT-overeenkomsten (ARBIT). De ARBIT bestaat uit algemene- en bijzondere bepalingen die betrekking hebben op alle IT-overeenkomsten die de Opdrachtgever aangaat en bevat 84 artikelen die de verhouding tussen de overheid als Opdrachtgever en ICT-bedrijven als leverancier vastleggen. Een aantal van deze artikelen gaat over het Intellectueel Eigendom van Programmatuur en beschrijft wanneer een Escrow overeenkomst moet worden aangegaan tussen Opdrachtgever en Opdrachtnemer.

Echter voor de uitvoering van werken en van technische installatiewerken maakt RWS gebruik van de Uniforme Administratieve Voorwaarden Geïntegreerde Contractvormen (UAV-GC). Deze voorwaarden zijn een combinatie van inkoop- en leveringsvoorwaarden. *D*e UAV-GC bevat onvoldoende bepalingen voor Intellectueel Eigendom en Escrow van Programmatuur om de continuïteit van de primaire en ondersteunende systemen binnen de Infrastructuur van RWS te waarborgen in geval van staken, overname of failliet gaan van een leverancier. RWS heeft dan ook een "Bijlage bijzondere bepalingen IA gerelateerde Programmatuur" ontwikkeld om in deze leemte van de UAV-GC te voorzien. Hierbij is gebruik gemaakt van de artikelen uit de ARBIT-2018 die het Intellectueel Eigendom en Escrow tussen Opdrachtgever en Opdrachtnemer regelen. Waar mogelijk is de tekst van de artikelen en de definities van de begrippen uit de ARBIT integraal aangehouden. Om inconsistenties tussen de ARBIT en UAV-GC bepalingen en begrippen te voorkomen zijn enkele artikelen en begrippen aangepast en/of toegevoegd.

In de volgende afbeelding wordt de mapping van de relevante artikelen uit de ARBIT-2018 naar toepassing binnen de UAV-GC weergegeven. Ook wordt op hoofdlijnen aangegeven in welke situatie er een overdracht van de broncode plaatsvindt van de Opdrachtnemer naar Opdrachtgever of dat er een Escrow overeenkomst moet worden aangegaan.



CSR 19.2 Bijzondere bepalingen Industriële Automatisering gerelateerde Programmatuur

Artikel 1 Begripsbepalingen Industriële Automatisering gerelateerde Programmatuur

1. Deze bijzondere bepalingen gelden alleen voor Programmatuur gerelateerd aan Industriële Automatisering.
2. Aan de volgende in deze bijzondere bepalingen met een hoofdletter gebezigde woorden wordt, aanvullend op de gedefinieerde begrippen in paragraaf 1 UAV-GC, de bijbehorende betekenis toegekend:
    a. Broncode: De Programmatuur en het geheel van programma-instructies in de oorspronkelijke programmeertaal met inbegrip van de daarbij behorende Documentatie in een zodanige vorm dat een programmeur die beschikt over kennis en ervaring van de gebruikte programmeerwijze en techniek, daarmee de Programmatuur kan wijzigen.

    b. Commercial Off-The-Shelf (COTS): De programmatuur welke commercieel ter beschikking wordt gesteld (geleased, gelicentieerd of verkocht) aan de markt, welke geen speciale aanpassing of onderhoud vereist gedurende de levensduur. Het intellectueel eigendom ligt bij de producent.

    c. Documentatie: Iedere beschrijving van Broncode, Objectcode, het Product en de eigenschappen daarvan bestemd voor de installatie, implementatie, het gebruik, beheer en/of het onderhoud daarvan alsmede de beschrijving van alle hulpmiddelen zoals systeemvereisten voor de ontwikkelomgeving met bijbehorende configuratie en instellingen en de stappen om van Broncode tot Objectcode te komen.

    d. Escrow: Het deponeren van (een kopie van) de Broncode van Standaardprogrammatuur waarvan het intellectueel eigendom bij de Opdrachtnemer ligt en waarin aanpassingen zijn gedaan specifiek ten behoeve van Opdrachtgever bij een onafhankelijke derde opdat Opdrachtgever deze, bij het in vervulling gaan van een of meer in de Escrow overeenkomst bepaalde voorwaarden, eigenmachtig kan (laten) gebruiken voor het herstellen van fouten en anderszins onderhouden, verder ontwikkelen en beheren van de Standaardprogrammatuur.

    e. Gebrek: Een gebrek conform paragraaf 4.1 UAV-GC dat in het kader van deze bijlage mede omvat iedere storing en/of mankement als gevolg waarvan de Prestatie niet geschikt is voor het overeengekomen gebruik.

f. Gebruiksrecht: Het recht op grond waarvan de Opdrachtgever bevoegd is tot het installeren en gebruiken van Standaardprogrammatuur overeenkomstig het overeengekomen gebruik conform de bepalingen van deze Overeenkomst met inbegrip van alle daarvoor redelijkerwijs noodzakelijke al dan niet tijdelijke verveelvoudigingen.

g. Industriële Automatisering (IA): De ICS/SCADA systemen en de ICT gerelateerde systemen en onderdelen (hardware en software), waarbij functioneel interactie plaats vindt met de fysieke omgeving of gebruikers (bijvoorbeeld een brug, onderstation, DRIP, etc.). Het voorgaande omvat mede het verkrijgen van informatie over de fysieke omgeving (inwinnen) en het beïnvloeden van de fysieke omgeving (bedienen en besturen).

h. Installatiekopie: Een gegevensdrager met daarop de Standaardprogrammatuur waarvoor het Gebruiksrecht wordt verleend.

i. Maatwerkprogrammatuur: Specifiek ten behoeve van de Opdrachtgever te ontwikkelen of ontwikkelde Programmatuur. Het intellectueel eigendom ligt bij de Opdrachtgever.

j. Materialen: Voor installatie, implementatie, gebruik en/of beheer en onderhoud van het Product benodigde hulpmiddelen, zoals de ontwikkelomgeving inclusief de hardware en software waaronder conversiesoftware, kabels, smartcards en fysieke gegevensdragers waarop Programmatuur wordt geleverd.

k. Objectcode: Vertaling van de Broncode in een direct door een computer leesbare en uitvoerbare code.

l. Patch: Als tijdelijk bedoelde correctie van Programmatuur.

m. Product: de Broncode, de Objectcode, de Programmatuur, de Documentatie en bijbehorende Materialen, inclusief alle aanpassingen van deze productonderdelen.

n. Programmatuur: De door Opdrachtnemer op te leveren set programmaregels zoals die, op directe of indirecte wijze, door een apparaat kan worden gebruikt om een bepaald, nader omschreven, resultaat tot stand te brengen. Programmatuur kan worden onderscheiden in Standaard- en Maatwerkprogrammatuur.

o. Standaardprogrammatuur: Voor algemeen gebruik ontwikkelde Programmatuur van de Opdrachtnemer dan wel derde(n) die niet exclusief aan de Opdrachtgever beschikbaar wordt gesteld en welke door Opdrachtnemer (specifiek) ten behoeve van het gebruik door Opdrachtgever zullen worden aangepast. Het intellectueel eigendom ligt bij de Opdrachtnemer dan wel derde(n).

Artikel 2 Intellectuele eigendomsrechten

1. Alle intellectuele eigendomsrechten die ten aanzien van het Product waar en wanneer ook kunnen worden uitgeoefend, berusten bij:

   a. De Opdrachtgever voor zover het betreft (onderdelen van) het Product die specifiek voor de Opdrachtgever zijn of worden ontworpen of vervaardigd en/of onder leiding of toezicht van de Opdrachtgever dan wel aan de hand van diens instructies of ontwerpen zijn gerealiseerd. Voor zover nodig worden deze rechten op grond van de Overeenkomst door de Opdrachtnemer aan de Opdrachtgever overgedragen welke overdracht reeds nu voor alsdan door de Opdrachtgever wordt aanvaard;

   b. De Opdrachtnemer of een derde in alle overige gevallen. Opdrachtnemer verleent in dat geval aan de Opdrachtgever een nader bij de Overeenkomst te bepalen niet exclusief recht tot gebruik van (onderdelen van) het Product dat in ieder geval toereikend is voor nakoming van het in de Overeenkomst(en) bepaalde.

2. Door ondertekening van de Overeenkomst worden de in lid 1 sub a bedoelde rechten aan de Opdrachtgever overgedragen. Voor zover voor de overdracht van die rechten op enig moment een nadere akte is vereist, stellen de Opdrachtgever en de Opdrachtnemer deze akte op.

Opdrachtnemer machtigt voor zover nodig Opdrachtgever hierbij tevens onherroepelijk om de overdracht van deze intellectuele eigendomsrechten in de desbetreffende registers in of over te (doen) schrijven.

3. Bij verschil van mening tussen partijen over intellectuele eigendomsrechten op (onderdelen van) het Product wordt er, behoudens tegenbewijs, vanuit gegaan dat die rechten bij de Opdrachtgever berusten. De Opdrachtgever mag ongeacht de uitkomst van dat geschil voortgaan met het overeengekomen gebruik.

4. De Opdrachtnemer heeft een inspanningsverplichting, voor zover nodig, om mede namens de door hem ingezette (zelfstandige) hulppersonen, afstand te doen van alle eventueel aan hem toekomende zogenoemde persoonlijkheidsrechten als bedoeld in artikel 25 lid 1, sub a t/m c Auteurswet, in de mate waarin die regelgeving zodanige afstand toelaat. De Opdrachtnemer garandeert de Opdrachtgever bevoegd te zijn om mede namens zijn (zelfstandige) hulppersonen afstand te doen.

5. De Opdrachtnemer vrijwaart de Opdrachtgever tegen aanspraken van derden terzake van een (gestelde) inbreuk op intellectuele eigendomsrechten van die derden, zulks met inbegrip van persoonlijkheidsrechten als bedoeld in artikel 25 lid 1, sub a t/m c Auteurswet, vergelijkbare aanspraken met betrekking tot kennis, ongeoorloofde mededinging en dergelijke daaronder begrepen. De Opdrachtnemer neemt op eerste verzoek van de Opdrachtgever de verdediging op zich in iedere procedure die in verband met (onderdelen van) de Programmatuur tegen de Opdrachtgever mocht worden ingesteld wegens inbreuk op de intellectuele eigendomsrechten van een derde. De Opdrachtgever zal de Opdrachtnemer in verband daarmee onverwijld van een dergelijke actie in kennis stellen en aan de Opdrachtnemer de noodzakelijke volmachten en hulp verstrekken. De Opdrachtnemer vrijwaart de Opdrachtgever tevens tegen alle schade en kosten waartoe die in een dergelijke procedure mocht worden veroordeeld alsook tegen de kosten van die procedure zelf waaronder, maar niet beperkt tot, de kosten die verband houden met het inwinnen van juridisch advies in verband daarmee.

6. De Opdrachtnemer zal in geval van een gestelde inbreuk op het intellectuele eigendomsrecht van een derde, op zijn kosten alle maatregelen treffen die kunnen bijdragen tot voorkoming van stagnatie van de bedrijfsvoering van de Opdrachtgever en tot beperking van de door de Opdrachtgever als gevolg daarvan te maken kosten en/of te lijden schade.

7. Onverminderd het bepaalde in lid 5 en lid 6 kan Opdrachtgever, indien derden hem terzake van schending van intellectuele eigendomsrechten in rechte betrekken, de Overeenkomst buiten rechte geheel of gedeeltelijk ontbinden.

Artikel 3 Gebruiksrecht

1. De Opdrachtnemer verleent aan de Opdrachtgever een Gebruiksrecht op de Standaardprogrammatuur voor een periode van 25 jaar na oplevering van het Werk. Het Gebruiksrecht omvat geen overdracht door de Opdrachtnemer aan de Opdrachtgever van octrooi-, auteurs- of merkenrechten op de betreffende Standaardprogrammatuur.

2. In het Gebruiksrecht is, zonder dat Opdrachtgever daarvoor enige additionele vergoeding verschuldigd is, in ieder geval begrepen:

   a. Het recht om alle voor de Opdrachtgever toegankelijke functionaliteiten van de Standaardprogrammatuur te gebruiken ook als die niet in de Documentatie staan vermeld;

   b. Het recht om kopieën van de Standaardprogrammatuur te vervaardigen, op te slaan, regelmatig te testen en ‘hot standby’ te houden, voor het geval van een calamiteit;

   c. Het recht om de Standaardprogrammatuur voor testdoeleinden te gebruiken;

d. Het recht om de Standaardprogrammatuur zonder enige beperking of begrenzing met betrekking tot plek, apparatuur of anderszins te gebruiken.

3. De Opdrachtgever mag kopieën van de Standaardprogrammatuur vervaardigen en in gebruik nemen zo vaak hij dat voor zijn bedrijfsvoering nodig oordeelt. Als hij daartoe overgaat en om die reden een additionele vergoeding aan de Opdrachtnemer verschuldigd is, deelt hij dat de Opdrachtnemer met bekwame spoed mee.

4. De Opdrachtgever verwijdert geen aanduidingen van eigendoms- en/of auteursrechten bij het verveelvoudigen van Standaardprogrammatuur.

5. Tot het moment van oplevering van het Werk verkrijgt de Opdrachtgever van de Opdrachtnemer een niet-exclusief recht tot het gebruik van de Standaardprogrammatuur voor installatie- en testdoeleinden. Het risico van dit Gebruiksrecht ligt bij de Opdrachtgever.

6. Indien de Opdrachtnemer gebreken in de Standaardprogrammatuur alleen herstelt door middel van het uitbrengen van Patches, heeft de Opdrachtgever gedurende de garantietermijn van artikel 5, ook al is hij met de Opdrachtnemer geen onderhoud overeengekomen, recht op de kosteloze ontvangst daarvan.

Artikel 4 Omzetting in andere gebruiksrechten

1. Indien de Opdrachtnemer het aan de Opdrachtgever verleende Gebruiksrecht op enig moment wil omzetten in een ander gebruiksrecht ten aanzien van de Standaardprogrammatuur treedt hij daarover, alsmede over de daarbij te hanteren omwisselverhouding, vooraf in overleg met de Opdrachtgever. Aan een dergelijke omzetting zijn voor de Opdrachtgever geen nadelige gevolgen van welke aard ook, verbonden.

2. Indien partijen bij het overleg bedoeld in lid 1 geen overeenstemming bereiken, mag de Opdrachtgever zijn Gebruiksrecht onverkort blijven uitoefenen.

Artikel 5 Garanties

1. De Opdrachtnemer garandeert dat hij voor zijn rekening voor de duur van 12 maanden na de datum van oplevering van het Werk, gebreken in het Product van Maatwerkprogrammatuur herstelt. Indien de Opdrachtgever een beroep wil doen op deze garantie, stelt hij de Opdrachtnemer daarvan schriftelijk en in spoedgevallen telefonisch op de hoogte. De Opdrachtnemer herstelt gebreken onverwijld rekening houdend met de ernst en de aard daarvan. Herstel vindt plaats in overleg met de Opdrachtgever. Na herstel dient Opdrachtnemer het aangepaste Product van Maatwerkprogrammatuur op te leveren aan Opdrachtgever. Het aangepaste Product van Standaardprogrammatuur waarin aanpassingen specifiek ten behoeve van Opdrachtgever zijn gedaan dient conform artikel 7 in depot te worden afgegeven.
2. De in lid 1 bedoelde garantie geldt niet voor zover de Opdrachtnemer aantoont dat een gebrek is ontstaan als gevolg van een, zonder zijn toestemming, door Opdrachtgever of een door deze ingeschakelde derde in door hem geleverde delen van de Programmatuur aangebrachte wijziging. De garantie geldt evenmin indien een gebrek aantoonbaar het gevolg is van onjuist, onzorgvuldig of ondeskundig gebruik van door hem geleverde onderdelen van Programmatuur door de Opdrachtgever.

Artikel 5a Eisen aan het Product

1. De Maatwerkprogrammatuur bevat geen technische voorzieningen, functies of andere vreemde elementen die op enig moment, al dan niet tijdelijk, aan het overeengekomen gebruik in de weg (kunnen) staan.

2. Indien Opdrachtnemer niet de rechthebbende van de Standaardprogrammatuur is, is hij door rechthebbende gemachtigd om namens deze Gebruiksrechten aan derden te verschaffen. De Opdrachtnemer verstrekt de Opdrachtgever op verzoek een kopie van die machtiging.

3. Opdrachtnemer zal desgevraagd onderhoud plegen op de door hem geleverde Maatwerkprogrammatuur door middel van een nog overeen te komen onderhoudscontract.

Artikel 6 Verstrekken Installatiekopie

1. De Opdrachtnemer verstrekt de Opdrachtgever een Installatiekopie van de geïnstalleerde versie van de Standaardprogrammatuur waarin aanpassingen zijn gedaan specifiek ten behoeve van de Opdrachtgever bij oplevering van het Werk of ingebruikneming van onderdelen van het Werk. De Opdrachtnemer dient van de Installatiekopie van de Standaardprogrammatuur een hash waarde te genereren met gebruik van hash algoritme SHA-256.

Artikel 7 Escrow

1. COTS Programmatuur valt buiten de scope van Escrow.

2. De Opdrachtnemer voorziet voor de duur van 25 jaar na oplevering van het werk in Escrow voor Standaardprogrammatuur waarvan het intellectueel eigendom bij de Opdrachtnemer ligt en waarin aanpassingen specifiek ten behoeve van de Opdrachtgever zijn gedaan.

3. Van Standaardprogrammatuur waarin aanpassingen zijn gedaan specifiek ten behoeve van de Opdrachtgever dient het Product gedeponeerd te worden bij de Escrow agent doch uiterlijk bij oplevering van het Werk of ingebruikneming van onderdelen van het Werk. Dit wordt bepaald door de Opdrachtgever.

4. De Opdrachtgever is gerechtigd de in te zetten Escrow agent te kiezen.

5. De in te zetten Escrow agent heeft expertise om het gedeponeerde Product te controleren op aanwezigheid, volledigheid en bruikbaarheid. Het Product dient hiertoe binnen de onafhankelijke omgeving van de Escrow agent gecompileerd en getest te worden. Ontbrekende of niet werkende onderdelen van het Product worden door de Opdrachtnemer gecorrigeerd en alsnog aangeleverd.

6. Escrow omvat alle niet openbaargemaakte informatie die de Opdrachtgever redelijkerwijs nodig heeft voor foutherstel, onderhoud, verder ontwikkelen en beheer van de Standaardprogrammatuur zodat hij daarvan het overeengekomen gebruik kan blijven maken. Escrow voldoet aan hetgeen dienaangaande ten tijde van het afsluiten daarvan op de Nederlandse markt gebruikelijk is.

7. De Escrow agent en de Escrow overeenkomst voorzien ten minste in het volgende:

   - Deponering van Materialen
   - Deponering van de Installatiekopie bij oplevering van het Werk of ingebruikneming van onderdelen van het Werk
   - Deponering van de hash waarde
   - Verificatie van de gedeponeerde Materialen
   - Verplichtingen van Escrow agent
   - Geheimhouding
   - Dat op de Intellectuele Eigendomsrechten geen pandrecht of beslag rust
   - Afgifte van het gedeponeerde
   - Garanties
   - Aansprakelijkheid

- Duur

8. De Opdrachtnemer levert Opdrachtgever nu voor alsdan, onder voorwaarde dat het gedeponeerde Product door de Escrow agent wordt vrijgegeven aan de Opdrachtgever conform de nog te sluiten Escrow overeenkomst, een gebruiksrecht op het Product om het eigenhandig en naar eigen inzicht te (laten) gebruiken, onderhouden, door ontwikkelen en beheren.

Artikel 8 Verbeterde en Nieuwe versies Standaardprogrammatuur

1. De Opdrachtnemer zorgt voor een consistent versiebeleid gedurende de periode van 25 jaar na oplevering van het Werk. Daarbij geldt als uitgangspunt dat Verbeterde en Nieuwe versies tijdig beschikbaar komen bij gebreken.

2. Tussentijdse wijzigingen in Programmatuur maken zoveel mogelijk onderdeel uit van Verbeterde en Nieuwe versies.

3. De Opdrachtnemer stelt de Opdrachtgever op verzoek kosteloos een exemplaar van een Nieuwe versie ter beschikking voor test- en evaluatiedoeleinden.

4. Indien is overeengekomen dat de Opdrachtnemer de Programmatuur installeert, geldt deze verplichting tevens voor Nieuwe versies die de Opdrachtgever in gebruik wil nemen.

5. Indien de Opdrachtnemer er voor kiest om in plaats van een Nieuwe versie andere Programmatuur uit te brengen en te stoppen met Verbeterde en Nieuwe versies van de bij de Opdrachtgever in gebruik zijnde Programmatuur, kan de Opdrachtgever aanspraak maken op een Gebruiksrecht op die nieuwe Programmatuur tegen de in de Overeenkomst vastgelegde voorwaarden voor een Nieuwe versie.

Artikel 9 Levering Maatwerkprogrammatuur

1. De Opdrachtnemer dient bij oplevering of ingebruikneming van onderdelen van het Werk van Maatwerkprogrammatuur het Product te leveren.

2. De Opdrachtnemer dient bij oplevering of ingebruikneming van onderdelen van het Werk een kopie te verstrekken van de geïnstalleerde versie van het Product van de Maatwerkprogrammatuur. Van de geïnstalleerde versie van het Product van de Maatwerkprogrammatuur dient een hash waarde te worden gegenereerd met gebruik van hash algoritme SHA-256 en meegeleverd te worden aan Opdrachtgever.

3. De Opdrachtgever heeft het recht om het geleverde Product van Maatwerkprogrammatuur zelf of door een derde partij te (laten) beoordelen op aanwezigheid, volledigheid en bruikbaarheid.

Bijlage CSR 20 Camera’s en omgang met camerabeelden van de verkeersregistratiesystemen

CSR 20.1 Doelstelling

Binnen de verkeersregistratiesystemen van Rijkswaterstaat worden tegenwoordig veel videocamera's ingezet. Het betreft bijvoorbeeld camera's bij tunnels, wisselstroken, spitsstroken, sluizen en bruggen. Reden voor het gebruik van videocamera's kan zijn het bevorderen van veiligheid van het verkeer, maar ook het op afstand regelen van waterstaatswerken, zoals bruggen. Dergelijke videocamera's zijn meestal gekoppeld aan systemen waarmee beelden kunnen worden vastgelegd.

Deze beelden kunnen persoonsgegevens bevatten. Een voorbeeld van een persoonsgegeven is een videobeeld indien daarop een persoon zichtbaar is of gegevens staan die herleidbaar zijn tot een natuurlijk persoon. Persoonsgegevens moeten conform de AVG beveiligd worden.

Medewerkers van de Opdrachtnemer (die beheer- en onderhoudswerkzaamheden verrichten aan camera’s en systemen die camerabeelden opslaan, verwerken of distribueren) dienen bewust te zijn van de privacy aspecten wanneer ze in contact komen met camera’s en systemen waarin camerabeelden worden opgeslagen, verwerkt of gedistribueerd en de hieronder beschreven instructies in acht nemen bij het verrichten van hun werkzaamheden. De verwerking van beelden en alle handelingen van medewerkers daaromtrent, dienen in lijn met de AVG plaats te vinden.

CSR 20.2 Best practice

Voor het beveiligingsbewust omgaan met camera’s en systemen waarin camerabeelden worden opgeslagen gelden de volgende instructies:

a. Alleen geautoriseerde medewerkers van de Opdrachtnemer mogen beheer- en onderhoudswerkzaamheden uitvoeren aan camera’s en systemen die camerabeelden opslaan;
b. De eventueel benodigde en verkregen accounts en wachtwoorden zijn strikt voor persoonlijk gebruik en mogen niet met anderen worden gedeeld. Hieronder vallen de accounts en wachtwoorden en toegangsmiddelen tot ruimten en de toegang tot de systemen binnen de ruimten;
c. Zonder uitdrukkelijke toestemming van de Opdrachtgever worden camerabeelden niet vernietigd, verwijderd of verstrekt aan derden of gebruikt voor persoonlijke of bedrijfsdoeleinden;
d. Indien bestanden met camerabeelden tijdelijk opgeslagen moeten worden of een kopie gemaakt moet worden voor onderzoeksdoeleinden is zorgvuldige omgang vereist. Er dient hierbij altijd een beveiligingsmaatregel actief te zijn zodat alleen een geautoriseerde medewerker toegang kan verkrijgen tot het bestand met beelden met in achtneming van de vigerende wachtwoord policy. Voorbeeld is dat bestanden op een beveiligde usb-stick of laptop met encryptie van de harde schijf worden opgeslagen en ontsluiting via een wachtwoord plaatsvindt. Standaard dient hierbij AES-256 versleuteling gebruikt te worden;
e. Na afronding van de werkzaamheden dient controle plaats te vinden dat er geen onnodige kopieën van bestanden met camerabeelden op eigen apparatuur of media en/of back-ups achterblijft;
f. Indien onregelmatigheden worden geconstateerd rondom de inzet, werking en opslag van camerabeelden dient dit direct als beveiligingsincident bij de Opdrachtgever gemeld te worden.

Bijlage CSR 21 Uniform aanleveren van incidentrapportages

Cybersecurityincidenten dienen te worden gerapporteerd. Daarnaast dient maandelijks een overzicht te worden gestuurd van alle incidenten. De rapportagestructuur is te vinden in de hiernavolgende paragrafen.

CSR 21.1 Formulier voor rapportage van een cybersecurityincident

Dit formulier dient zo volledig mogelijk te worden ingevuld. Na invulling dit formulier versturen naar: EMAILADRES@rws.nl

ALGEMENE INFORMATIE	
Datum rapport:	dd-mm-jjjj
Objectnaam en locatie:	
Naam rapporteur:	
Functie rapporteur:	
Organisatie rapporteur:	
Telefoonnummer:	

Rapporteert hiermee het volgende cybersecurityincident:

ALGEMENE INFORMATIE INCIDENT	
Soort incident[6]:	
Incident is opgemerkt op:	[jjjjmmdd/uu:mm]
Incident opgemerkt door:	[indien ander dan rapporteur]
Is het object nog operationeel:	Ja/Nee
Opschaling incident response team nodig:	Ja/Nee

DETAIL INFORMATIE INCIDENT	
Beschrijving van het incident[7]:	
Analyse van het incident:	
Is de dreiging ingesloten:	Ja/Nee
Hoe is de dreiging ingesloten:	
Is de dreiging bestreden:	Ja/Nee
Hoe is de dreiging bestreden:	
Is herstel nodig:	Ja/Nee
Welk herstel is nodig:	

[6] Voorbeelden van incidenten zijn: malware, (D)DoS, verlies van controle over proces/bediening, verlies van zicht op proces/bediening, verlies van toegang tot systemen, hack, ongeoorloofd verschaffen van toegang, ongeoorloofde wijziging van configuratie/instellingen/rechten, verwijderen/wijzigen van logfiles.

[7] Een korte, duidelijke beschrijving van het incident, verwijzing naar overige beschikbare documentatie (b.v. logfiles, communicatie met leverancier en RWS) betreffende het incident.

CSR 21.2 Formulier voor periodieke rapportage van cybersecurityincidenten

Dit formulier dient aan het begin van elke maand zo volledig mogelijk te worden ingevuld. Na invulling dit formulier versturen naar: EMAILADRES@rws.nl

Datum rapport:	dd-mm-jjjj
Objectnaam en locatie:	
Rapporteur:	[naam, functie en bedrijf van degene die het rapport opmaakt]
Periode:	[maand waarop deze rapportage betrekking heeft]

De volgende cybersecurityincidenten (inclusief hun afhandeling) hebben plaatsgevonden in de hiervoor genoemde periode:

No	Datum/tijd incident: [jjjjmmdd/uu:mm]	Soort incident[8]:	Afgehandeld (J/N):	Datum/tijd afgehandeld:	Uitleg/opmerkingen m.b.t. incident en afhandeling[9]:
1					
2					
3					
4					
5					

[8] Voorbeelden van incidenten zijn: malware, (D)DoS, verlies van controle over proces/bediening, verlies van zicht op proces/bediening, verlies van toegang tot systemen, hack, ongeoorloofd verschaffen van toegang, ongeoorloofde wijziging van configuratie/instellingen/rechten, verwijderen/wijzigen van logfiles.

[9] Een korte, duidelijke beschrijving van het incident, incident afhandelingsnummer/verwijzing naar overige beschikbare documentatie (b.v. logfiles, communicatie met leverancier en RWS) betreffende het incident, en hoe het incident is opgelost.

Bijlage CSR 22 Virtualisatie

CSR 22.1 Doelstelling

Virtualisatie wordt steeds vaker toegepast binnen de IA-omgeving. Vaak gebeurt dit om de beschikbaarheid van verouderde toepassingen of systemen te verhogen. Het is van belang dat virtualisatie op een cyberveilige wijze wordt ingezet en dat toepassing ervan geen nieuwe kwetsbaarheden en dreigingen introduceert.

CSR 22.2 Best Practice

Indien virtualisatie wordt toegepast gelden de volgende minimale best practices:

a. Voorafgaand aan de inzet van virtualisatie wordt een risicoanalyse uitgevoerd om de risico's van zowel virtualisatie, als het niet virtualiseren in kaart te brengen;
b. Bij toepassing van virtualisatie dient de zonescheiding in stand te blijven;
c. Security functies draaien op fysiek gescheiden virtualisatieplatformen;
d. Safety functies draaien op fysiek gescheiden virtualisatieplatformen;
e. Systeem hardening wordt toegepast op de virtualisatieomgeving, waarbij:
    i. Alleen de noodzakelijke Operating System (OS) componenten en services zijn geactiveerd;
    ii. Verbindingen met onnodige fysieke apparaten vanuit Virtual Machines (VM's) zijn verboden;
    iii. Filesharing tussen host en gast OS is gedeactiveerd;
    iv. Het gebruik van resources door individuele VM's is gelimiteerd;
    v. Zowel gast als host OS's net als de fysieke systemen regelmatig worden gepatcht;
    vi. Gewerkt wordt met minimale privileges;
f. Administrators kunnen uitsluitend gebruik maken van een persoonlijk account voor beheertaken;
g. Zowel het host OS als de gast OS's worden centraal gelogd;
h. Productie en testomgevingen voor VM's zijn gescheiden;
i. Bij toepassing van virtualisatie voor de IA dienen algemene best practices m.b.t. virtualisatie voor IV te worden gevolgd, voor zover deze de belangen van IA niet schaden.

Bijlage CSR 23 Verwijdering en vernietiging van informatie en apparatuur

CSR 23.1 Doelstelling

Indien apparatuur uit de IA omgeving met opslagmedia wordt verwijderd of hergebruikt, moet er op toegezien worden dat er geen gevoelige gegevens of in licentie gegeven software op de opslagmedia achterblijft. Denk hierbij bijvoorbeeld aan gegevensdragers zoals harde schijven, maar ook aan PLC's of IoT apparatuur. Het is van belang dat alle informatie die aanwezig is op apparatuur op zorgvuldige wijze wordt verwijderd wanneer een apparaat uit de IA omgeving wordt gehaald en afgevoerd of hergebruikt. Daarnaast dient vertrouwelijke informatie in de IA omgeving die niet meer nodig is vernietigd te worden.

CSR 23.2 Best Practice

Bij de best practices wordt er onderscheid gemaakt tussen apparatuur die wordt hergebruikt en apparatuur die wordt vernietigd enerzijds en fysieke documenten anderzijds. De volgende minimale best practices zijn van toepassing:

CSR 23.2.1 Verwijdering gegevens bij hergebruik apparatuur

Indien apparatuur wordt hergebruikt is het van belang de op het apparaat aanwezige informatie te verwijderen. Hierbij geldt het volgende:

a. Vertrouwelijke informatie wordt tenminste 3 maal volledig overschreven met verschillende bitpatronen, waaronder 2 vaste patronen en één random patroon;
b. Niet vertrouwelijke informatie wordt tenminste 1 maal volledig overschreven met een random bitpatroon;
c. Er wordt gecontroleerd of de gegevens onherstelbaar zijn verwijderd;
d. Indien volledig overschrijven van de informatie niet mogelijk is, dient de gegevensdrager te worden vernietigd.

CSR 23.2.2 Verwijdering gegevens bij vernietiging apparatuur

Indien apparatuur niet wordt hergebruikt is het van belang de op het apparaat aanwezige informatie te verwijderen. Hierbij geldt het volgende:

a. De informatie wordt middels een degausser verwijderd door een hiertoe gecertificeerd bedrijf, of;
b. Het apparaat wordt versnipperd door een hiertoe gecertificeerd bedrijf.

CSR 23.2.3 Verwijdering van fysieke informatie (documenten)

Verwijdering van fysieke documenten met daarop vertrouwelijke informatie vindt plaats op een veilige manier, bijvoorbeeld door verbranding of versnippering. Bij versnippering wordt er gebruik gemaakt van apparatuur waarbij de mate van versnippering (snippergrootte) in overeenstemming is met het vertrouwelijkheidsniveau van de informatie.

Bijlage A Begrippenlijst

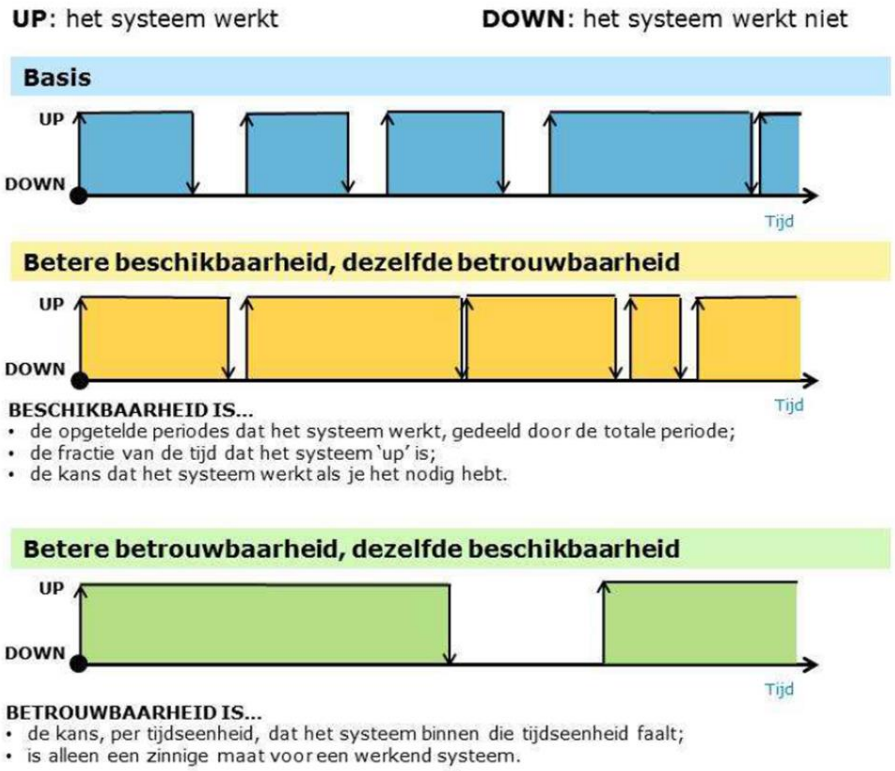
Bedrijfsmiddel
Apparatuur met informatie verwerkende en of opslag capaciteit, software die waarde vertegenwoordigt voor de organisatie en producten waarmee fysieke en of logische toegang tot ruimten en informatiesystemen verkregen kan worden.

Beheerobject
Afgebakende eenheid die bestaat uit een samenhangend geheel van elementen met één of meer autonome functies, bijvoorbeeld een tunnel, sluis, brug, kering, verkeerscentrale etc.

Beschikbaarheid (IA)
De fractie van de tijd dat een systeem werkt, of “up” is. Ofwel de opgetelde periodes (tijd) dat een systeem werkt, gedeeld door de totale periode (tijd).

Betrouwbaarheid (IA)
De kans, per tijdseenheid, dat een systeem binnen die tijdseenheid faalt.

Afbeelding: visualisatie onderscheid beschikbaarheid en betrouwbaarheid



Cybersecurity
Cybersecurity is het voorkomen van gevaar of schade veroorzaakt door verstoring, uitval of misbruik van ICT en Industriële Automatisering.

Cybersecurity weerstandsniveau
Het vermogen om weerstand te bieden tegen aanvallen die bedoeld zijn om zich met geweld of manipulatie toegang fysiek dan wel digitaal te verschaffen tot ruimten en tot de informatievoorziening.

Explain

Een plausibel gemotiveerde tijdelijke afwijking ten aanzien van de eisen en maatregelen uit de BIO of de Cybersecurity Implementatierichtlijn Objecten waarvan het risico als gevolg van de afwijking geaccepteerd is.

Informatievoorziening (IV)
Het geheel aan hulpmiddelen (waaronder ICT en IA), gegevensverzamelingen en organisatorische inrichtingen, dat dient tot het verstrekken van informatie.

Industriële Automatisering (IA)
Industriële Automatisering omvat de ICS/SCADA systemen en de ICT gerelateerde systemen en onderdelen (hardware en software), waarbij functioneel interactie plaats vindt met de fysieke omgeving of gebruikers (bijvoorbeeld een brug, onderstation, DRIP, etc.). Dit omvat mede het verkrijgen van informatie over de fysieke omgeving (inwinnen) en het beïnvloeden van de fysieke omgeving (bedienen en besturen). PA en OT zijn synoniemen voor IA.

Informatie- en Communicatietechnologie (ICT)
Informatie- en Communicatietechnologie omvat een samenhangend geheel van informatiesystemen, hardware en software, operating systemen van servers, de onderliggende technische datanetwerkinfrastructuur met datanetwerken en bijbehorende datanetwerkcomponenten, dataopslag in rekencentrum, computer- en technische ruimten met als doel het mogelijk maken of ondersteunen van de processen.

Industrial Control Systems (ICS)
Industrial Control Systems zijn systemen die toegerust zijn voor de bediening en besturing van de RWS Infrastructuur waarbij ook gebruik wordt gemaakt van SCADA systemen.

IoT
Het Internet-of-Things is een netwerk van slimme apparaten, sensoren en andere objecten die (vaak verbonden met het internet) gegevens verzamelen over hun omgeving, deze kunnen uitwisselen en op basis daarvan (semi-) autonome beslissingen of acties nemen die van invloed zijn op hun omgeving.

Kwetsbaarheid
Een kwetsbaarheid is een eigenschap die een aanvaller de mogelijkheid biedt een cyberaanval uit te voeren of een eigenschap die kan leiden tot uitval. Dit kan zich voordoen in een digitale dienst, proces of systeem, maar ook in de samenleving als geheel of in een specifieke organisatie.

Risico
De kans dat de dreiging optreedt en het verlies (of impact) realiteit wordt.

Risicoanalyse
Een methode die informatie oplevert, waarmee het management in staat wordt gesteld te beslissen welke risico's, of weke combinaties van risico's, een te grote potentiële schade vormen en met welke maatregelen deze risico's teruggedrongen kunnen worden.

RWS Infrastructuur
RWS infrastructuur staat voor de netwerkinfrastructuur (het areaal) van RWS: de wegen, vaarwegen en watersystemen.

Supervisory Control And Data Acquisition (SCADA)
SCADA systemen verzamelen, verwerken en visualiseren meet- en regelsignalen.

Vitale processen
Bepaalde processen zijn zo essentieel voor de Nederlandse samenleving dat uitval of verstoring tot ernstige maatschappelijke ontwrichting leidt en een bedreiging vormt voor de nationale veiligheid. Deze processen vormen de Nederlandse vitale infrastructuur.

Bijlage B Cybersecurity Dossier / Cybersecurity Beveiligingsplan

De template voor het Cybersecurity Dossier / Cybersecurity Beveiligingsplan wordt op verzoek door het door het Security Centre van CIV beschikbaar gesteld.

Bijlage C Best practice voor risico inschatting bij CSIR afwijkingen

Het is van belang dat een juiste risico inschatting en afweging kan worden gemaakt indien er afwijkingen zijn aan de CSIR. Deze bijlage biedt hiervoor een best practice.

RWS hanteert de formule risico = kans x impact voor het bepalen van eventuele risico's.
De kans is de waarschijnlijk dat de dreiging zich zal manifesteren en dat de kwetsbaarheid wordt benut door het ontbreken van Baseline Beveiliging IA controls of maatregelen uit de CSIR.

Voor de bepaling van het risico dienen de volgende stappen gevolgd te worden. In de eerste stap wordt de kanswaarde aan de hand van onderstaande tabel bepaald.

De kans score kan bepaald worden aan de hand van de dreiging en bijbehorende kwetsbaarheid of er kan simpelweg aansluiting gezocht worden bij de kans scores zoals opgenomen en toegepast binnen de specifieke dreigingsanalyse voor RWS.

Stap 1: De kans score
De kans score of waarde wordt uitgedrukt in een vijfpuntschaal.

De kans of waarschijnlijkheid dat de dreiging zich zal manifesteren in de komende periode		Omschrijving kans en daarmee het benutten van de kwetsbaarheid
1	**Verwaarloosbaar** *t > 5 jaar*	De kans en daarmee het falen van de functie van het object wordt niet binnen 5 jaar verwacht;
2	**Klein** (*3 jaar < t ≤ 5 jaar*)	De kans en daarmee het falen van de functie van het object wordt tussen 3 jaar en 5 jaar na nu verwacht;
3	**Middelmatig** (*2 jaar < t ≤ 3 jaar)*	De kans en daarmee het falen van de functie van het object wordt tussen 2 jaar en 3 jaar na nu verwacht;
4	**Groot** (1 jaar < *t ≤ 2 jaar*)	De kans en daarmee het falen van de functie van het object wordt tussen 1 jaar en 2 jaar na nu verwacht;
5	**Zeker** (*t ≤ 1 jaar)*	De kans en daarmee het falen van de functie van het object wordt tussen nu en 1 jaar verwacht;

De manifestatie van de dreiging en benutting van de kwetsbaarheid zal leiden tot een impact voor RWS die uitgedrukt kan worden in een gevolgschade en is daarmee de tweede stap in het bepalen van het cybersecurity risico.

Stap 2: Gevolgschade / Impact
Bij het manifest worden van de dreiging en kwetsbaarheid zullen als gevolg van het niet of afwijkend invullen van de Baseline beveiliging IA controls en of CSIR maatregelen security (Se) maatregelen ongewenste uitwerkingen op de RAMSSHEEP aspecten van IA systemen verwacht kunnen. Ontbrekende maatregelen zullen in eerste instantie leiden tot ongewenste negatieve uitwerkingen op de betrouwbaarheid (R), availability (A), maintainability (M) en safety (veiligheid). De negatieve uitwerking op de aspecten R, A, M en S van IA systemen zullen vervolgens ook tot negatieve effecten op de overige aspecten leiden. De gevolgschade wordt conform de RWS handleiding Prestatiegestuurde Risicoanalyse (PRA) uitgedrukt in een viertal gevolgklassen.

Betrouwbaarheid' (R):
Availability (Beschikbaarheid) (A):
Maintainability (Onderhoudbaarheid) (M):
Safety (veiligheid) (S):
Security (Beveiliging) (Se);
Health (Gezondheid) (H):
Environment (Omgeving en Milieu) (E):
Economics (Levensduurkosten) (€):
Politics (Politiek) (P):

	Gevolgklasse			
	Verwaarloosbaar (1)	Beperkt (2)	Groot (3)	Ernstig (4)
R	Het niet (binnen het geplande jaar) uitvoeren van de (onderhouds) maatregel voor cybersecurity leidt tot een niet compliancy registratie en rapportage en heeft negatieve invloed op de betrouwbaarheid van het betreffend object maar heeft een verwaarloosbare invloed op de hoofdfunctie.	Het niet (binnen het geplande jaar) uitvoeren van de (onderhouds) maatregel voor cybersecurity leidt tot een niet compliancy registratie en rapportage en heeft negatieve invloed op de betrouwbaarheid van het betreffende object en heeft een minimale negatieve invloed op de hoofdfunctie.	Het niet (binnen het geplande jaar) uitvoeren van de (onderhouds) maatregel voor cybersecurity leidt tot een niet compliancy registratie en rapportage en heeft negatieve invloed op de betrouwbaarheid van het betreffend object en heeft ernstige negatieve invloed op de hoofdfunctie.	Het niet (binnen het geplande jaar) uitvoeren van de (onderhouds) maatregel voor cybersecurity leidt tot een niet compliancy registratie en rapportage en heeft negatieve invloed op de betrouwbaarheid van het betreffend object en heeft catastrofale negatieve invloed op de hoofdfunctie.
A	Het niet (binnen het geplande jaar) uitvoeren van de (onderhouds) maatregel voor cybersecurity leidt tot een niet compliancy registratie en rapportage en heeft negatieve invloed op de beschikbaarheid van het betreffend object maar heeft een verwaarloosbare invloed op de hoofdfunctie.	Het niet (binnen het geplande jaar) uitvoeren van de (onderhouds) maatregel voor cybersecurity leidt tot een niet compliancy registratie en rapportage en heeft negatieve invloed op de beschikbaarheid van het betreffend object maar heeft een minimale invloed op de hoofdfunctie.	Het niet (binnen het geplande jaar) uitvoeren van de (onderhouds) maatregel voor cybersecurity leidt tot een niet compliancy registratie en rapportage en heeft negatieve invloed op de beschikbaarheid van het betreffend object en heeft ernstige negatieve invloed op de hoofdfunctie.	Het niet (binnen het geplande jaar) uitvoeren van de (onderhouds) maatregel voor cybersecurity leidt tot een niet compliancy registratie en rapportage en heeft negatieve invloed op de beschikbaarheid van het betreffend object en heeft catastrofale negatieve invloed op de hoofdfunctie.
M	Het niet (binnen het geplande jaar) uitvoeren van de (onderhouds) maatregel voor cybersecurity leidt tot een niet compliancy registratie en rapportage en maakt dat onderhoud in een later stadium verwaarloosbaar moelijker uitgevoerd kan worden binnen de randvoorwaarden van gebruik.	Het niet (binnen het geplande jaar) uitvoeren van de (onderhouds) maatregel voor cybersecurity leidt tot een niet compliancy registratie en rapportage en maakt dat onderhoud in een later stadium minimaal moeilijker uitgevoerd kan worden binnen de randvoorwaarden van het gebruik.	Het niet (binnen het geplande jaar) uitvoeren van de (onderhouds) maatregel voor cybersecurity leidt tot een niet compliancy registratie en rapportage en maakt dat onderhoud in een later stadium niet uitgevoerd kan worden binnen de randvoorwaarden van gebruik, hetgeen ernstige negatieve invloed heeft op de prestaties van de netwerkschakel.	Het niet (binnen het geplande jaar) uitvoeren van de (onderhouds) maatregel voor cybersecurity leidt tot een niet compliancy registratie en rapportage en maakt dat onderhoud in een later stadium niet uitgevoerd kan worden binnen de randvoorwaarden van gebruik, hetgeen catastrofale negatieve invloed heeft op de prestaties van de netwerkschakel.
S	Het niet (binnen het geplande jaar) uitvoeren van de (onderhouds) maatregel voor cybersecurity leidt tot een niet compliancy registratie en rapportage en heeft een verwaarloosbare invloed op gebruiksveiligheid van het object, maar dit blijft	Het niet (binnen het geplande jaar) uitvoeren van de (onderhouds) maatregel voor cybersecurity leidt tot een niet compliancy registratie en rapportage en leidt tot een situatie die de geaccepteerde grenzen voor gebruiksveiligheid benaderd en leidt daardoor	Het niet (binnen het geplande jaar) uitvoeren van de (onderhouds) maatregel voor cybersecurity leidt tot een niet compliancy registratie en rapportage en leidt tot het niet voldoen aan gestelde eisen ten aanzien van gebruiksveiligheid wat daardoor leidt tot een	Het niet (binnen het geplande jaar) uitvoeren van de (onderhouds) maatregel voor cybersecurity leidt tot een niet compliancy registratie en rapportage en heeft een catastrofaal negatief effect op de gebruiksveiligheid wat leidt tot extra dodelijk gevaar bij normaal gebruik.

	Gevolgklasse			
	Verwaarloosbaar (1)	Beperkt (2)	Groot (3)	Ernstig (4)
	binnen geaccepteerde grenzen.	tot een minimaal aantal extra ongelukken met tijdelijke gezondheidsschade of letsel zonder verzuim.	ernstige toename van het aantal ongelukken met blijvend letsel of met blijvende gezondheidsschade.	
Se	Het niet (binnen het geplande jaar) uitvoeren van de (onderhouds) maatregel voor cybersecurity leidt tot een niet compliancy registratie en rapportage en heeft negatieve invloed op de fysieke en of logische toegangsbeveiliging van het betreffende object maar heeft een minimale invloed op de hoofdfunctie.	Het niet (binnen het geplande jaar) uitvoeren van de (onderhouds) maatregel voor cybersecurity leidt tot een niet compliancy registratie en rapportage en heeft negatieve invloed op de fysieke en of logische toegangsbeveiliging van het betreffende object en heeft een minimale negatieve invloed op de hoofdfunctie.	Het niet (binnen het geplande jaar) uitvoeren van de (onderhouds) maatregel voor cybersecurity leidt tot een niet compliancy registratie en rapportage en heeft negatieve invloed op de fysieke en of logische toegangsbeveiliging van het betreffend object die tot security incidenten leiden en heeft hiernaast ernstige negatieve invloed op de hoofdfunctie.	Het niet (binnen het geplande jaar) uitvoeren van de (onderhouds) maatregel voor cybersecurity leidt tot een niet compliancy registratie en rapportage en heeft negatieve invloed op de fysieke en of logische toegangsbeveiliging van het betreffende object die tot security incidenten leiden en heeft hiernaast catastrofale negatieve invloed op de hoofdfunctie en of de prestaties van de netwerkschakel.
H	Het niet uitvoeren van de onderhoudsmaatregel heeft een verwaarloosbare negatieve invloed op de gezondheid.	Het niet uitvoeren van de onderhoudsmaatregel heeft een minimale negatieve invloed op de gezondheid.	Het niet uitvoeren van de onderhoudsmaatregel heeft een ernstige negatieve invloed op de gezondheid.	Het niet uitvoeren van de onderhoudsmaatregel heeft een catastrofale negatieve invloed op de gezondheid en veroorzaakt overlijden.
E	Het niet uitvoeren van de maatregelen heeft een verwaarloosbaar negatief effect op het gebruik.	Het niet uitvoeren van de maatregel heeft een beperkt negatief effect op het gebruik en beperkt zich tot consequenties voor het lokale netwerk.	Het niet uitvoeren van de maatregel heeft een ernstig negatief effect op het gebruik en heeft consequenties voor het regionale netwerk.	Het niet uitvoeren van de maatregel heeft een catastrofaal negatief effect op het gebruik en heeft consequenties voor het landelijke netwerk.
€	Uitstel geeft < 50 k Euro aan extra onderhoud/claims/inspecties.	Uitstel geeft < 500 k Euro aan extra onderhoud/claims/inspecties.	Uitstel geeft < 1000 k Euro aan extra onderhoud/claims/inspecties.	Uitstel geeft > 1000 k Euro aan extra onderhoud/claims/inspecties.
P	Het niet (binnen het geplande jaar) uitvoeren van de (onderhouds) maatregel voor cybersecurity leidt tot een niet compliancy registratie en rapportage en heeft verder geen politieke consequenties.	Het niet (binnen het geplande jaar) uitvoeren van de (onderhouds) maatregel voor cybersecurity leidt tot een niet compliancy registratie en rapportage en is mogelijk aanleiding voor verscherpte controles door toezichthouders.	Het niet (binnen het geplande jaar) uitvoeren van de (onderhouds) maatregel voor cybersecurity leidt tot een niet compliancy registratie en rapportage en is mogelijk aanleiding voor negatieve media berichtgeving die tot kamer vragen kunnen leiden.	Het niet (binnen het geplande jaar) uitvoeren van de (onderhouds) maatregel voor cybersecurity leidt tot een niet compliancy registratie en rapportage en de positie van DG, de Minister of Staatssecretaris staat ter discussie.

In de derde stap wordt de risicoscore afgebeeld in de risicomatrix of heat map waarbij op de ene as de impact/gevolgschade wordt uitgedrukt en op de andere as de kans (waarschijnlijkheid) dat de dreiging en kwetsbaarheid manifest wordt.

Stap 3: Risicomatrix en risicoscore
De risicomatrix is hieronder weergegeven. De risicoscore wordt eenvoudig bepaald door kans- en gevolgscore met elkaar te vermenigvuldigen. De hoogte van dit getal geeft aan hoe noodzakelijk een beheersmaatregel is. Hierin worden drie niveaus onderscheiden: het rode, oranje of groene gebied.

1. Onacceptabel — Risicoscore 15 t/m 20
Er moeten direct beheersmaatregelen worden getroffen om het risico te beheersen.

2. Ongewenst — Risicoscore 5 t/m 12
Er moet ofwel een beheersmaatregel worden getroffen om het risico te beheersen ofwel worden aangetoond waarom dit niet haalbaar/noodzakelijk is

3. Acceptabel — Risicoscore 1 t/m 4
Er hoeft geen maatregel te worden getroffen om het risico te beheersen. Bij falen van de functie van het object worden de gebruikelijke acties ondernomen voor (functie-)herstel.

		Impact			
		Verwaarloosbaar (1)	Beperkt (2)	Groot (3)	Ernstig (4)
Kans	Verwaarloosbaar (1)	Acceptabel (1)	Acceptabel (2)	Acceptabel (3)	Acceptabel (4)
	Klein (2)	Acceptabel (2)	Acceptabel (4)	Ongewenst (6)	Ongewenst (8)
	Gemiddeld (3)	Acceptabel (3)	Ongewenst (6)	Ongewenst (9)	Ongewenst (12)
	Groot (4)	Acceptabel (4)	Ongewenst (8)	Ongewenst (12)	Onacceptabel (16)
	Zeker (5)	Ongewenst (5)	Ongewenst (10)	Onacceptabel (15)	Onacceptabel (20)

Bijlage T Procedure Werkvergunningen

Bijlage T Procedure Werkvergunningen

Bijlage bij Vraagspecificatie Proces

D&C Vervanging Verlichting Schipholtunnel
Zaaknummer: 31212908

Rijkswaterstaat
Ministerie van Infrastructuur en Milieu

Procedure Werkvergunningen

Tunnels WNN/MN

Datum 27 maart 2020
Status Definitief
Versie 1.0

Rol	Naam	Functie en organisatie	Paraaf	Datum
Opsteller en Beheerder document (vrijgegeven)	E. de Haan	Objectbeheerder TTI *RWS tunnelbeheer organisatie WNN/MN*		13-02-2020
Proceseigenaar (voor akkoord)	E.F.A. Blomjous	Assetmanager *RWS tunnelbeheer organisatie WNN, mede namens RWS tunnelbeheer organisatie MN*		27-3-2020
	R. Külman	Afdelingshoofd District		27-3-2020

Colofon

Uitgegeven door	Rijkswaterstaat West Nederland District West-Noord tunnelbeheer organisatie
Contact	tunnelbeheer-WNN/MN@rws.nl
Hoofdproces	Assetmanagement
Proceseigenaar	Elsbeth Blomjous *Assetmanager*
Beheerder document	Edwin de Haan *Objectbeheerder TTI*
Opgesteld door	tunnelbeheer organisatie

Versiebeheer

Versie	Aanpassingen	Auteur	Afgestemd met	Datum
1.0	Versie van WNZ omgezet naar versie 1.0 WNN/MN	EH	EB	24-09-2019

Dit document behoort tot het Veiligheidsbeheerplan tunnels WNN/MN versie 1.0 d.d. 24 september 2019.

Inhoud

1 Inleiding 5
1.1 Doel en doelgroep 5
1.2 Toepassingsbereik 5
1.3 Definities 6
1.4 Lijst met afkortingen 7
1.5 Overzicht contactgegevens 7

2 Soorten vergunningen 8
2.1 Toegangsvergunning 8
2.2 Werkvergunning **Fout! Bladwijzer niet gedefinieerd.**

3 Procedure Werkvergunningen 10
3.1 Aanvraag Werkvergunning 10
3.2 Behandeling en beoordelen van de Werkvergunning 12
3.3 Verstrekking Werkvergunning 12

4 Aanvang, uitvoeren en beëindigen werkzaamheden 14
4.1 Aanvang werkzaamheden 14
4.2 Uitvoeren werkzaamheden 14
4.3 Beëindigen werkzaamheden 14

Bijlage A Flowchart procedure Werkvergunningen 15

Bijlage B Instructie en achtergrond voor het invullen van de Werkvergunning 16
B.1 Tabblad Aanvraag – Aanvraaggegevens en type 16
B.2 Tabblad Aanvraag – Keuzelijsten 16
B.3 Tabblad Risico's 17
B.4 Tabblad Maatregelen 18

Bijlage C Aanwezigheid Registratieformulier 19

Bijlage D Toelichting Taak Risico Analyse 21
D.1 Doel Taak Risico Analyse 21
D.2 Werkwijze opstellen TRA 23
D.3 TRA Checklist 25
D.4 TRA Formulier 26

1 Inleiding

Dit document beschrijft het proces rond het verstrekken van een Werkvergunning voor instandhouding/onderhoudswerkzaamheden voor de tunnels van WNN/MN.

1.1 Doel en doelgroep

Het doel van het Werkvergunningenstelsel is de borging van een veilige uitvoering van werkzaamheden in en om de tunnels van WNN/MN.

Het Werkvergunningenstelsel is bedoeld voor iedere partij die werkzaamheden verricht binnen de beheergrenzen van de tunnels van WNN/MN, of om andere redenen in het bedien- of dienstgebouw aanwezig is.

Binnen en buiten de beheergrenzen van de tunnels van WNN/MN. is het ook verplicht om naast het hebben van een Werkvergunning goedkeuring van de te nemen verkeersmaatregelen te hebben. Aanvraag van deze verkeersmaatregelen lopen via het verkeersloket (SPIN).

https://spin.rijkswaterstaat.nl/spin/

Bij calamiteiten dient de aannemer indien er verkeersmaatregelen zijn toegepast dit achteraf in SPIN te melden.

1.2 Toepassingsbereik

Een Werkvergunning heeft het volgende toepassingsbereik:

> Een **Werkvergunning** is vereist voor alle werkzaamheden binnen de beheergrenzen van de tunnels van WNN/MN.. Een **toegangsvergunning** is vereist voor alle personen in en om de tunnels van WNN/MN in relatie tot tunnelbezoek / werkzaamheden.

Dit document is onderdeel van het Rijkswaterstaat Instandhoudingsplan Tunnels WNN/MN. Daarnaast heeft het raakvlak met de volgende documenten:

- **Veiligheidsbeheerplan Tunnels WNN/MN (Rijkswaterstaat)**
  - Instandhoudingsplan
    - Instructie Veilig Werken
    - Sleutelplan
    - *Werkvergunningenstelsel (dit document)*
    - Bedrijfsnoodplan Gebouwen Tunnels WNN/MN
- **Overige documenten (Rijkswaterstaat)**
  - Integraal Veiligheidsplan
- **Overige documenten (Opdrachtnemer)**
  - Project Management Plan
    - Integraal Veiligheidsplan

Het ondersteunende systeem voor het Werkvergunningenstelsel is in het Beheer Management Systeem (Ultimo) geregeld, in de module “Werkvergunningen” (zie Instandhoudingsplan). Zowel opdrachtnemer als opdrachtgever hebben toegang tot deze module.

> ***Zie https://rijkswaterstaat.ultimo.net***

1.3 Definities

Aanvrager	De persoon die de vergunning aanvraagt
Bezoekersregistratie	Registratie waarbij een bezoeker onder begeleiding van een vergunninghouder bezoek brengt aan de tunnel en/of toegang heeft tot de tunnelruimten.
Gebruiker	De verkeersdeelnemer die gebruik maakt van de tunnels van WNN/MN.
Houder	De persoon die in het bezit dient te zijn van de Werkvergunning.
IPM-team	Integraal Project Management team bestaande uit de vijf rollen t.w. Projectmanager, Manager Projectbeheersing, Contractmanager, Technisch Manager en Omgevingsmanager.
Risico ruimte	Elke begrensde en van de omgeving afgesloten ruimte waar een of meer van de volgende beperkende omstandigheden op van toepassing zijn: • Moeilijk toegankelijk en/of te verlaten. • Niet vrij van brandbaar en/of toxisch product. • Mogelijk zuurstof tekort. • Slecht te ventileren. • Moeilijk contact met de omgeving. • Aanwezigheid van midden- of hoogspanningsinstallaties.
TRA	Taak Risico Analyse – een specifieke (aanvullende) risico-inventarisatie met beheersmaatregelen die betrekking hebben op (specifieke) werkzaamheden.
Tunnelbeheer organisatie	Operationeel tunnelbeheerder is het Afdelingshoofd van RWS WNN/MN. Tunnelbeheerorganisatie(TBO) is bevoegd om namens het Afdelingshoofd de rol van operationeel tunnelbeheerder in BMS (Ultimo) uit te voeren.
Tunnelsysteem	Alles wat een onderdeel vormt van het beheersgebied van de tunnels van WNN/MN en betrekking heeft op gebouwen, terreinen, dienstwegen, installaties etc.
Verstrekker	De persoon welke toestemming verleent tot het uitvoeren van werkzaamheden door ondertekening van de Werkvergunning.
Wegverkeersleider	De persoon die vanuit de Verkeerscentrale verantwoordelijk is voor de bediening en de bewaking van de tunnels van WNN/MN.
Werkplan	De omschrijving van de werkzaamheden waarvoor een Werkvergunning noodzakelijk is.

1.4 Lijst met afkortingen

Dit document bevat de volgende afkortingen:
- ARBO: Arbeidsomstandighedenwet
- BMS: Beheer Management Systeem
- CBP: Calamiteitenbestrijdingsplan
- DVM: Dynamisch Verkeers Management
- IPM-team: Integraal Project Management team
- RI&E: Risico Inventarisatie en Evaluatie
- SPIN: Systeem voor Planning en Informatie Nederland
- TRA: Taak Risico Analyse
- TTI: Tunnel Technische Installaties
- V&G- plan: Veiligheids- en Gezondheidsplan
- VODK: Vast Onderhoud DVM Keten
- Warvw: Wet aanvullende regels veiligheid wegtunnels
- WVL: Wegverkeersleider

De volgende afkortingen staan voor (dienstonderdelen van) Rijkswaterstaat.
- RWS: Rijkswaterstaat
- TBO: Tunnelbeheer Organisatie
- PPO: Programma's, Projecten en Onderhoud
- VCWNN: Verkeerscentrale West Nederland Noord
- VCMN: Verkeerscentrale Midden Nederland
- VWM: Verkeer en Water Management

1.5 Overzicht contactgegevens

Verkeerscentrale West Nederland Noord
Onderdeel van: RWS Verkeer & Water Management
Locatie: Amsterdamseweg 25, 1981 LE Velsen-Zuid
Telefoon: 088-7985700
Bereikbaar: 24/7

Verkeerscentrale Midden Nederland
Onderdeel van: RWS Verkeer & Water Management
Locatie: Papendorpseweg 101, 3528 BJ Utrecht
Telefoon: 088-7986910
Bereikbaar: 24/7

Tunnel Beheerorganisatie (Tunnelbeheerder)
Onderdeel van: RWS Dienst West Nederland – District Noord en Zuid
Email: tunnelbeheer-WNN@rws.nl
Telefoon: 088- 088 7973925
Bereikbaar: tijdens kantooruren (ma-vr 8:00 – 16:30).

Opdrachtnemer (ON)

2 Soorten vergunningen

Er wordt hierin onderscheid gemaakt in een procedure Toegangsvergunning en een procedure Werkvergunningen.

2.1 Toegangsvergunning

De toegangsvergunning wordt op twee manieren geborgd:

- Toegangspas of toegangstag; voor personen die regelmatig legitieme werkzaamheden moeten verrichten in en/of om het tunnelcomplex.
- Bezoekersregistratieformulier; voor personen die werkzaamheden komen verrichten in en/of om het tunnelcomplex of op bezoek komt.

Elke persoon die in de tunnel aanwezig is dient zich conform één van beide wijzen te registeren. Hiermee is voor de unit Tunnel Beheer duidelijk wie toegang heeft tot de tunnel of de tunnelgebouwen

Het 'Bezoekers Registratie Formulier' (zie Bijlage C) dient beschikbaar te worden gesteld en te worden beheerd in de Bedieningsgebouwen.

Een toegangspas zal toegang verschaffen tot specifieke ruimtes die beveiligd zijn met een paslezer, afhankelijk van de persoonlijke toegangsrechten. Voor het aanvragen en beheersregels van een toegangspas wordt verwezen naar het Sleutelplan.

De Verstrekker is er verantwoordelijk voor dat te allen tijde duidelijk inzichtelijk is wie er in het tunnelcomplex aanwezig is en welke werkzaamheden er plaatsvinden.

Bezoekersregistratie
Als voorwaarde voor toegang tot de tunnel de tunnelruimten en toegangshekken van toegangswegen van de hulpdiensten geld het lezen van door de "**Instructie Veilig Werken**". Dit wordt vastgelegd en afgetekend op het Bezoekers registratieformulier (zie Bijlage C) bij de Bedieningsgebouwen.

Hiermee verklaart en bevestigt de Werkvergunninghouder dat hij en zijn eventuele bezoekers onder zijn begeleiding "Instructie Veilig Werken" hebben gelezen en begrepen.

Iedereen die zelfstandig en niet onder begeleiding van een vergunninghouder aanwezig is in de tunnel dient een Werkvergunning te hebben.

2.2 Werkvergunning

Een Werkvergunning is bedoeld om risico's behorende bij alle onderhoudswerkzaamheden zoveel mogelijk te beperken. Deze risico's zijn al deels geborgd in de object Risico Inventarisatie en Evaluatie (object RI&E). Dit is een onderdeel van het Veiligheid en Gezondheidsplan (V&G plan). Bij het opstellen van de Werkvergunning dient de aanvrager de RI&E aan te vullen met een Taak Risico Analyse (TRA). Deze is met name bedoeld voor risico volle werkzaamheden (b.v. hoog- en laagspanning) of in risico volle ruimten (b.v. pompkelders).

In essentie beschrijft de Werkvergunning de werkzaamheden, de omstandigheden, de risico's t.a.v. de werksituatie, de maatregelen die genomen worden om de risico's te minimaliseren en de bij de werkzaamheden betrokken partijen.

Er wordt onderscheid gemaakt in twee soorten Werkvergunningen:

Een **langlopende Werkvergunning** is opgedeeld in twee typen:

- Preventieve onderhoudswerkzaamheden (vast onderhoud).
- Repeterende werkzaamheden met een laag risico.

Langlopende Werkvergunningen hebben een doorlooptijd van de duur van het contract. Voor storingen is een bijzondere vorm van de langlopende Werkvergunning van toepassing. Omdat het niet praktisch is om bij storingen een Werkvergunning procedure te doorlopen, moet de persoon daarom zelfstandig situaties kunnen beoordelen op geldende risico's.

Een voorbeeld van repeterende werkzaamheden met een laag risico zijn schoonmaakwerkzaamheden of het bijvullen van kantineartikelen.

Een **kortlopende Werkvergunning** is verplicht voor alle overige werkzaamheden. De geldigheidsduur van deze vergunning zal per situatie worden bepaald en wordt gedefinieerd met een duidelijke begin- en einddatum. De kortlopende Werkvergunning is bedoeld voor (bijvoorbeeld) grootschalige werkzaamheden, of (eenmalige) werkzaamheden met een hoog risico.

Naast een actieve Werkvergunning blijft te allen tijde de bezoekersinstructie gelden.

NB. De tijdsduur van de vergunning kan bij de vergunningsaanvraag in Ultimo worden aangegeven.

3 Procedure Werkvergunningen

Dit hoofdstuk beschrijft de werkwijze van de aanvraag, behandeling, beoordeling, en verstrekking van de Werkvergunning. De rollen Aanvrager, Verstrekker en Houder kunnen naar de onderhoudsaannemer gedelegeerd, waarbij de functiescheiding moet worden gewaarborgd door beide partijen (aannemer en RWS). Het functioneel beheer (proceseigenaarschap t.a.v. Werkvergunningen) blijft echter bij de unit Tunnel Beheer. De toetsing op een juiste uitvoering van de procedure Werkvergunningen zal door Rijkswaterstaat worden gewaarborgd.

De aanvraag, beoordeling, uitgifte en registratie van de procedure Werkvergunningen zal gefaciliteerd en geborgd worden in de BMS applicatie Ultimo Werkvergunningen. Alle betrokken rollen bij de procedure Werkvergunningen dienen de informatie te verwerken in de applicatie Ultimo Werkvergunningen. Naast de workflow van de procedure Werkvergunningen zijn ook alle van toepassing zijn documenten in de Werkvergunningen module ondergebracht.

De procedure Werkvergunningen is in een flowchart weergegeven in Bijlage A. Bijlage B bevat een invulinstructie.

Het ondersteunende systeem voor de procedure Werkvergunningen is het Beheer Management Systeem (Ultimo), waarin een module "Werkvergunningen" is opgenomen: https://rijkswaterstaat.ultimo.net

3.1 Aanvraag Werkvergunning

- Voor werkzaamheden die vallen onder het eerder genoemde toepassingsgebied dient de Aanvrager een Werkvergunning in bij de Verstrekker.

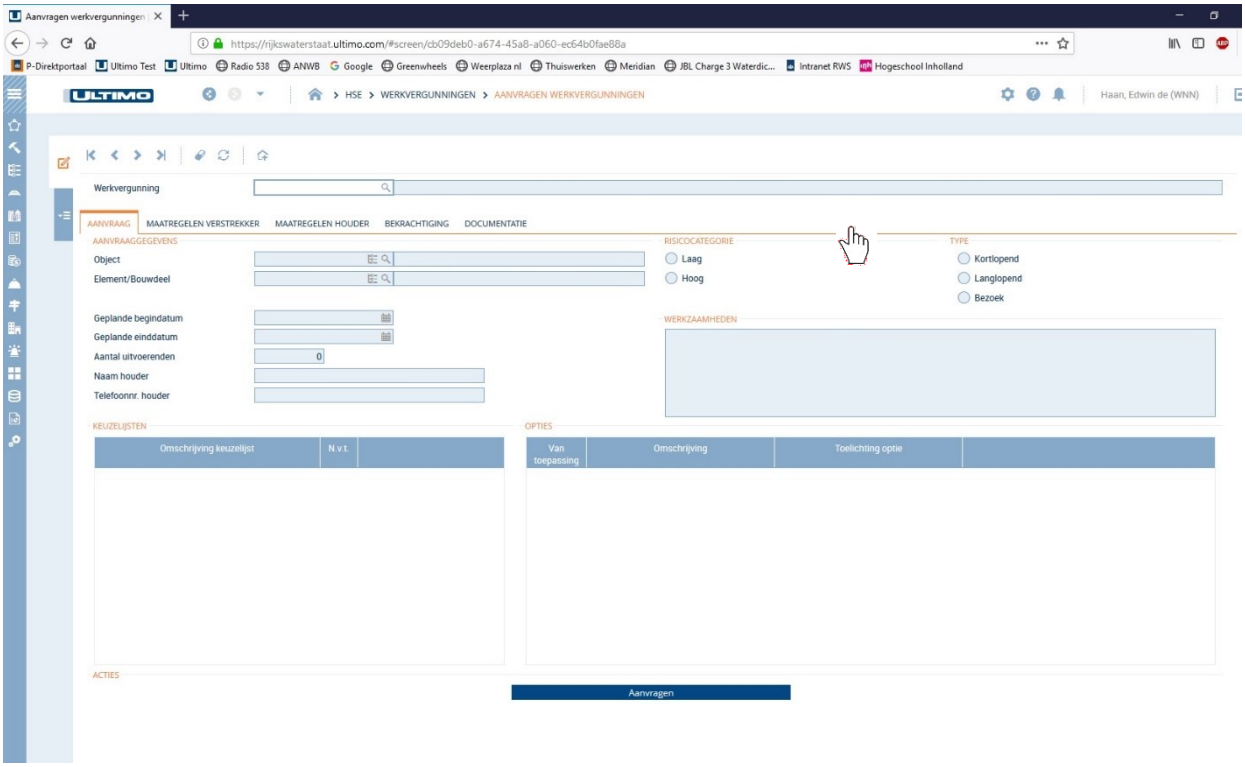
  Dit dient minimaal:

  2 weken – Voor kortlopende werkzaamheden voor uitvoering te worden ingediend.

  6 weken – Voor langlopende werkzaamheden voor uitvoering te worden ingediend.

- *(voor)overleg*
  Voor verduidelijking van de aanvraag of voor de afstemming van de Werkvergunning kan de aanvrager contact opnemen met de unit Tunnel Beheer en andere de betrokken partijen, of betrokken partijen uitnodigen, om de Werkvergunning in een vooroverleg af te stemmen.

- *Werkvergunning sturen*
  Werkvergunningsaanvragen dienen voor uitvoering ter goedkeuring te worden ingediend bij de Verstrekker. Deze aanvraag dient te worden ingevoerd in het BMS, middels het scherm zoals in Figuur 1 is aangegeven.
  - Het is van belang dat bij de aanvraag alle relevante tabbladen (Aanvraag, Risico's en Maatregelen) ingevuld worden.
  - Indien de aanvrager geen toegang tot Ultimo heeft kan de aanvraag ook met behulp van de unit Tunnel Beheer en/of de opdrachtnemer gedaan worden. De aanvrager dient echter wel zelf actief te worden betrokken bij het invullen!
  - De aanvrager dient zijn aanvraag via het tabblad Bekrachtiging te bekrachtigen, zie Figuur 2.



Figuur 1: Aanvraag werkvergunning in Ultimo. De tabbladen Aanvraag, Risico's en Maatregelen dienen hierbij volledig ingevuld te worden.



Figuur 2: Digitaal bekrachtigen van de aanvraag in Ultimo.

- *Aanvraag Verkeersmaatregelen*
  Verkeersmaatregelen voor de tunnel dienen teven voorafgaande aan de werkzaamheden bij het verkeersloket te worden aangevraagd.
  - https://spin.rijkswaterstaat.nl/spin/

  Voor de afhandeling van storingen dienen de verkeersmaatregelen te zijn vastgelegd in de langlopende Werkvergunning. Verkeersmaatregelen kunnen hiervoor achteraf in het SPIN worden vastgelegd (zie Instandhoudingsplan).

3.2 Behandeling en beoordelen van de Werkvergunning

- *Beoordelen aanvraag*
  De Werkvergunning wordt door de Verstrekker o.a. getoetst en beoordeeld:
  - Correcte weergave van werkzaamheden
  - Volledigheid en een correcte inschatting van veiligheidsrisico's.
  - Beoordeling impact op tunnelbeschikbaarheid

Mogelijk dient de Werkvergunning te worden aangevuld met additionele maatregelen en/of aanwijzingen. In bepaalde gevallen is een Taak Risico Analyse (TRA) en/of aanvullende vergunning een vereiste (dit wordt per werksituatie bepaald). Zie bijlage D voor meer informatie over de TRA.

Voor het accorderen van de Werkvergunning gaan Houder en Verstrekker met elkaar in gesprek om de werksituatie, de ingeschatte risico's en de genomen maatregelen door te nemen.

Slechts enkele personen hebben de bevoegdheid tot het beoordelen (en bekrachtigen/verstrekken) van een Werkvergunning. Namens Rijkswaterstaat zijn dit de Objectbeheerder TTI. De Objectbeheerder TTI kunnen in overleg met de opdrachtnemer bevoegdheden tot verstrekking aan hem toekennen.

3.3 Verstrekking Werkvergunning

In geval de verstrekker akkoord is met de werkzaamheden en (aanvullende) beheersmaatregelen dan accordeert hij digitaal de Werkvergunning.

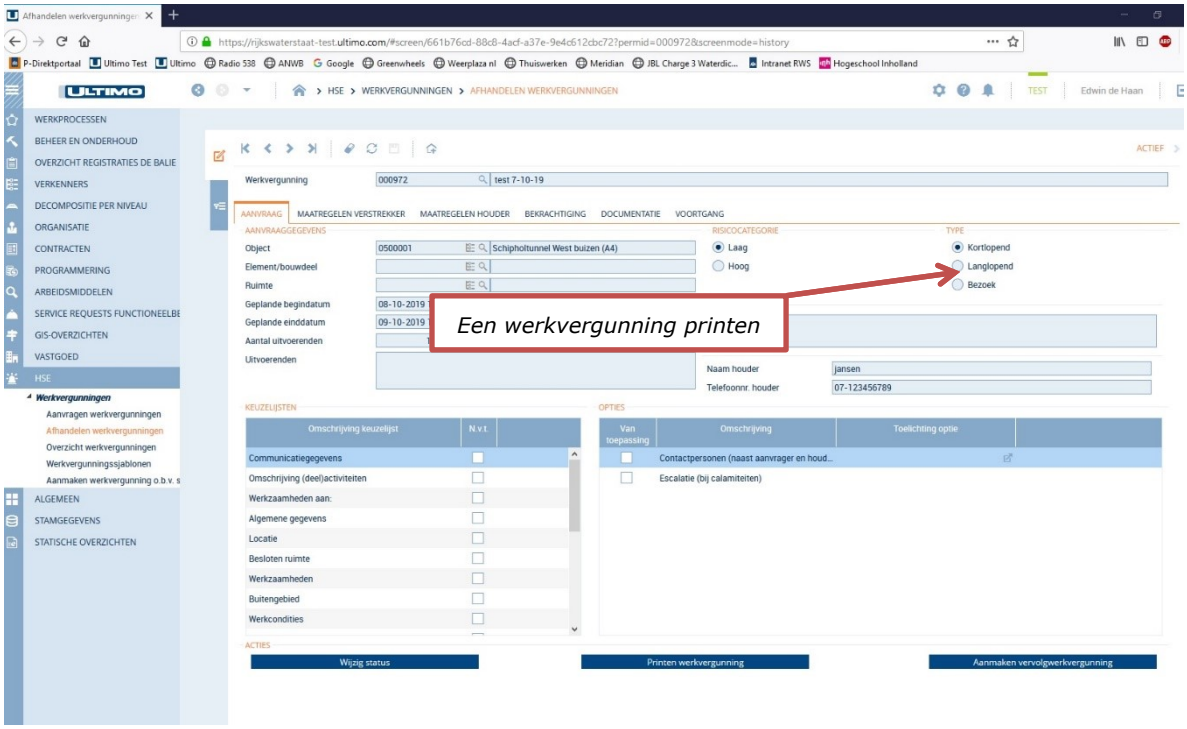
Het verstrekken van een vergunning (bekrachtigen) vindt in Ultimo plaats op een soortgelijke manier als in Figuur 2. Bij bekrachtiging dient de Verstrekker onderstaande verklaring af te leggen.



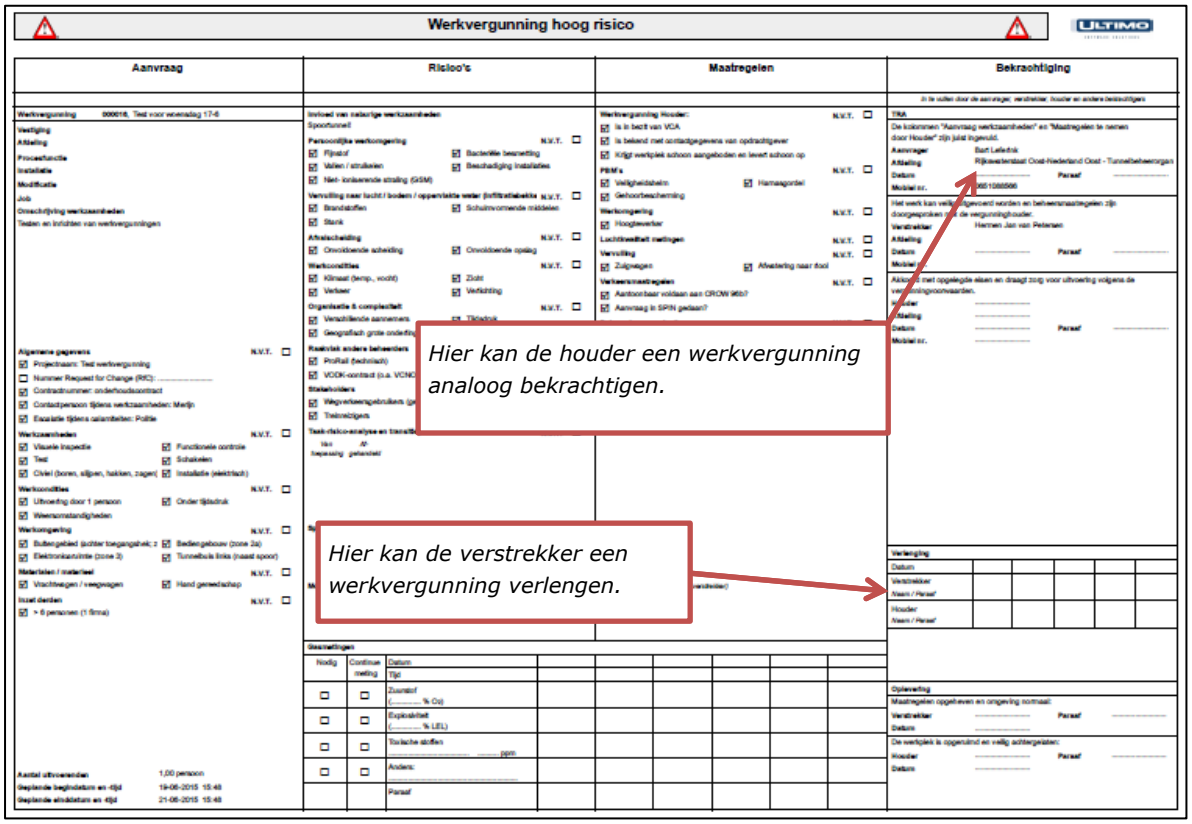
Vervolgens geeft de verstrekker een bericht aan de Aanvrager dat de Werkvergunning akkoord is. De Houder dient te bevestigen dat hij/zij conform de vastgestelde afspraken zal werken. Dit dient bevestigd te worden door ofwel 1) een digitale handtekening; of 2) een analoge handtekening. Dit digitaal bekrachtigen gaat eveneens op soortgelijke wijze als in Figuur 2. Analoog bekrachtigen kan middels een handtekening op de uitgeprinte Werkvergunning (zie Figuur 3 en 4).

De Houder dient een uitgeprinte versie van de Werkvergunning bij zich te houden ten tijde van de werkzaamheden. Hierna kan op afgesproken data en tijdstip begonnen worden met de werkzaamheden.

Verlenging van de Werkvergunning (alleen voor de kortlopende)
Dit voorkomt onnodig werk om een nieuwe Werkvergunning aan te vragen. Een Werkvergunning kan verlengd worden wanneer de gedefinieerde situatie onveranderd is. De Houder kan de Werkvergunning in overleg na afloopdatum laten verlengen bij de Verstrekker. Dit kan alleen analoog (op papier), zie Figuur 4. De Houder en Verstrekker bepalen samen of de gestelde situatie onveranderd is.



Figuur 3: Het printen van een werkvergunning



Figuur 4: Het analoog bekrachtigen van een werkvergunning

4 Aanvang, uitvoeren en beëindigen werkzaamheden

Deze paragraaf geeft het starten, uitvoeren en beëindigen van de werkzaamheden weer. In het geval van een storingsafhandeling dient de procedure Storingsmanagement te worden gevolgd (zie Instandhoudingsplan).

4.1 Aanvang werkzaamheden

Bij aanvang van de werkzaamheden meldt de aannemer de start van de werkzaamheden bij de Verstrekker.

- De vergunninghouder is te allen tijde verantwoordelijk voor een veilige werkplek en heeft een coördinatieplicht met betrekking tot veilig werken bij inzet van onderaannemers.

- Personen die geen toegangspas hebben (zoals contractors) worden bij het betreden van de ruimtes ofwel begeleid door de onderhoudaannemer, ofwel via de voorwaarden die in de Werkvergunning worden vastgelegd. De identiteit van de persoon wordt echter altijd geregistreerd in de bezoekersregistratie.

4.2 Uitvoeren werkzaamheden

Personen werkzaam in en/of om het tunnelcomplex in het bezit te zijn van:

1 Geldige Werkvergunning
2 Geldig legitimatiebewijs
3 Begeleider met toegangspas (wanneer van toepassing)

4.3 Beëindigen werkzaamheden

Na afloop van de werkzaamheden verifieert (voert zelf een functietest uit) de aannemer de betreffende systemen op juist functioneren, in samenspraak met de Verkeerscentrale. Indien noodzakelijk.

De Werkvergunning vervalt wanneer één of meerdere van onderstaande zaken van toepassing zijn:

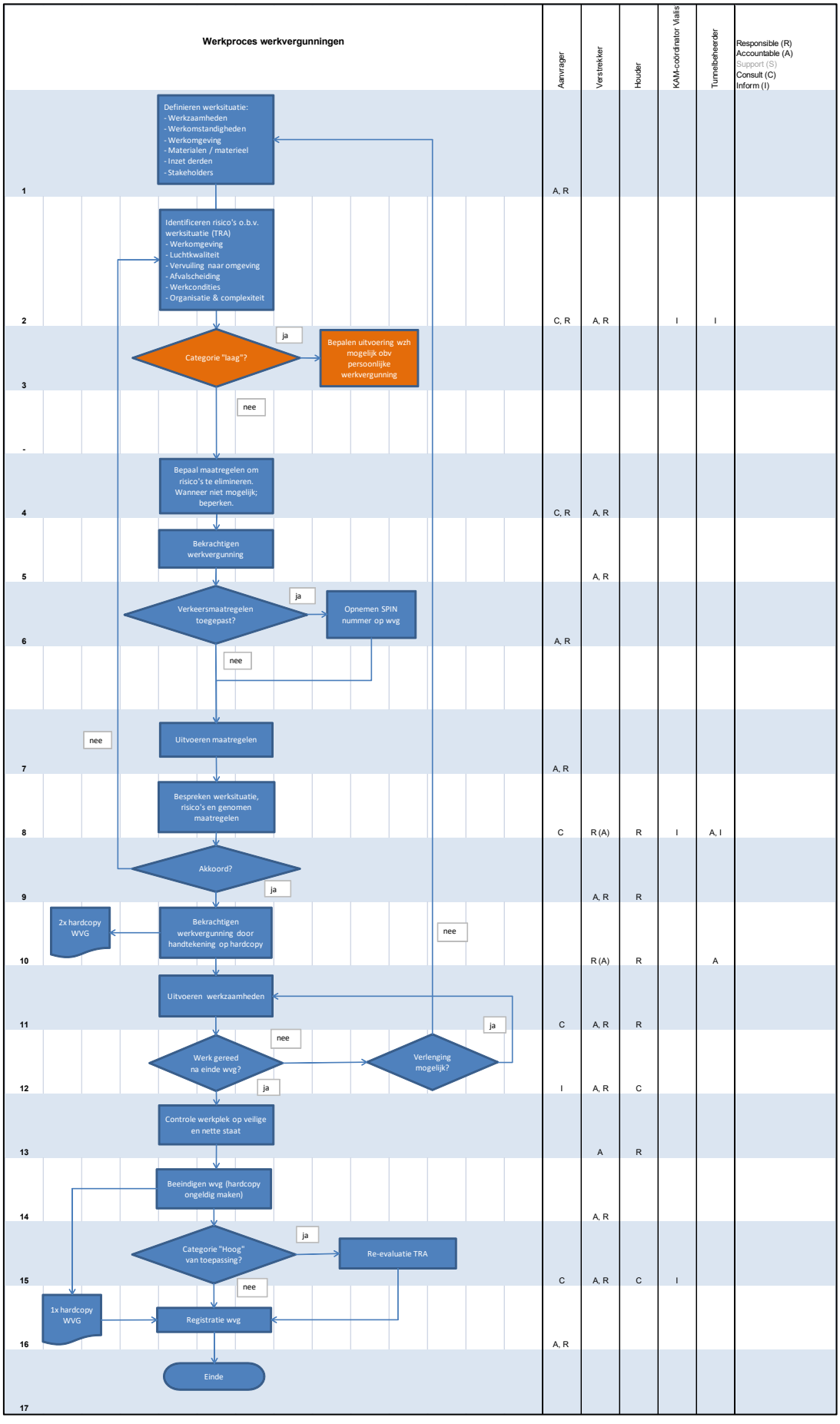
- Huidige datum overschrijdt de vastgelegde datum op de Werkvergunning.
- De werksituatie is veranderd ten opzichte van de vastgelegde situatie in de Werkvergunning
- Een incident en/of calamiteit
- Een directe ‘order tot onderbreking werkzaamheden’ door een Weginspecteur of een Officier van Dienst van RWS

In geval van incidenten en calamiteiten vervalt de vergunning. De aannemer en Verkeerscentrale informeren elkaar over het incident en/of calamiteit. De verkeerscentrale geeft de aannemer zo nodig instructies over ontruiming en/of herstel van het normaal bedrijf van de systemen (zie ook het V&G-plan voor nadere toelichting, zoals het terugschakelen van de bediening).

De Tunnel Beheer organisatie of Officier van Dienst kan met een ‘order tot onderbreking werkzaamheden’ de werkzaamheden stil leggen. Alle personen dienen de instructies van unit Tunnel Beheer of de Officier van Dienst onmiddellijk op te volgen en werkzaamheden te staken wanneer dat wordt geëist.

Bij het verlaten van de tunnel dient de Houder zich af te melden bij de Verstrekker.

Bijlage A Flowchart procedure Werkvergunningen



Bijlage B Instructie en achtergrond voor het invullen van de Werkvergunning

Hieronder worden enkele invulvelden van de Werkvergunning nader toegelicht.

B.1 Tabblad Aanvraag – Aanvraaggegevens en type

In het kader van de geldigheid dienen onder andere de volgende gegevens te worden vermeld:

Type

Kortlopende Werkvergunning met specifieke benoemende doorlooptijd; Langlopende Werkvergunning algemeen met doorlooptijd van maximaal 1 jaar.

Geplande begin- en einddatum

Hierin verschillen de Werkvergunningen qua inhoud. De looptijd van de langlopende Werkvergunning is maximaal één jaar.
De looptijd van een korte Werkvergunning is specifiek op de Werkvergunning aangegeven (bijvoorbeeld één periode vaak weekend of avond/nacht).

Aantal uitvoerenden

Het aantal werknemers dient vermeld te staan. Bovendien dient de op de werkplek aanwezige contactpersoon de Nederlandse taal goed te beheersen.

Werkzaamheden

Geef een duidelijke omschrijving van de (deel)werkzaamheden. In de omschrijving mag verwezen worden naar het werkplan en/of het Veiligheid- en Gezondheidsplan (V&G plan) van de aanvrager. Deze moet dan wel als bijlage meegezonden worden met de aanvraag. Dit kan via het tabblad "Documentatie".

B.2 Tabblad Aanvraag – Keuzelijsten

Hieronder worden enkele invulvelden van de keuzelijst "Algemene gegevens" (Tabblad Aanvraag) nader toegelicht.

Algemene gegevens - Projectnaam

Dit is de naam van het project waar de werkzaamheden onder vallen, bijvoorbeeld "Nachtsluiting maart 2016".

Algemene gegevens - Contract/projectnummer en/of RfC nummer

Dit is het contract/projectnummer waaronder de hoofdaannemer met Rijkswaterstaat afspraken heeft gemaakt.
Het RfC nummer is het nummer van de change waarvoor de Werkvergunning wordt aangevraagd.

Algemene gegevens - Contactpersonen

Wie zijn de contactpersonen voor het opstellen van de Werkvergunning, en wie zijn de contactpersonen bij het uitvoeren van de werkzaamheden?

Algemene gegevens - Escalatie

Welke personen moeten worden geraadpleegd in geval van calamiteiten?

Materialen / materieel

Het aantal voertuigen dient vermeld te staan, evenals het type voertuigen dat gebruikt wordt.

Werkomgeving

Geef aan in welke ruimten de werkzaamheden plaatsvinden. Geef daarbij ook de ruimten aan waarvoor toegang moet worden verleend om daar te komen. In de tunnel zijn verschillende ruimten. Hier is een onderscheid gemaakt in besloten ruimte, technische (elektro) ruimte, bijzondere ruimte en overige ruimte. Voor het werken in deze ruimtes gelden aparte regels, waar de aanvrager zich aan moet houden. Bij de verstrekking of voorbespreking van de vergunning zal per ruimte worden aangegeven welke typering van toepassing is. Alle besloten ruimtes zijn van pictogrammen voorzien.

B.3 Tabblad Risico's

Hieronder worden enkele invulvelden van het tabblad Risico's nader toegelicht.

Risico's - Taak Risico Analyse

De Taak Risico Analyse (TRA) wordt uitgevoerd om vroegtijdig de risico's op te sporen en op te heffen dan wel te verminderen middels beheersmaatregelen van complexe en/of risicovolle werkzaamheden. Het dient om werkzaamheden goed voor te bereiden, efficiënter uit te voeren en om incidenten te voorkomen. In een TRA dient rekening te houden met de (veiligheid van) omgeving, weggebruikers en onderhoudsmedewerkers.

TRA's worden opgesteld voor werkzaamheden waarvan de risico's en te nemen maatregelen (1) niet zijn opgenomen in de Risico Inventarisatie en Evaluatie (RI&E) van de onderhoudfase van de wegtunnel Tunnels WNN/MN; (2) niet zijn onderkend in een Veiligheids- en Gezondheidsplan (V&G); of (3) indien de werkzaamheden in bijzondere mate complex en/of risicovol zijn.

Bij het opstellen van een TRA worden de volgende stappen gevolgd. Het vooroverleg kan ondersteuning bieden bij het invullen van de stappen.

1. *De werkzaamheden worden opgesplitst in taakstappen.*

2. *De taakstappen worden op risico's beoordeeld. Deze risico's worden bepaald door de aard van het werk, de werkcondities, de complexiteit en, in het geval zich toch verstoringen voordoen, de ernst en de gevolgen hiervan.*

3. *Vervolgens moet worden bekeken of de risico's van bepaalde taakstappen voldoende beheerst zijn middels werkinstructies en/of procedures.*

4. *Is dit niet het geval, dan moet een risicobepaling plaatsvinden (bijvoorbeeld door een classificatie te maken van ' laag' en 'hoog'). De risico's ten aanzien van een veilige doorstroming van het verkeer vormen een belangrijk onderdeel van de risicobepaling.*

5. *Tot slot dienen er bij de hoog geclassificeerde risico's passende beheersmaatregelen opgesteld te worden.*

Risico's - Transitieplan

De impactanalyse op de verkeerscentrale vloeit voort uit het transitieplan. In dit onderdeel moet expliciet duidelijk worden gemaakt wat de gevolgen van de werkzaamheden zijn voor afzonderlijke onderdelen van de verkeerscentrale.

1 *Verkeersgeleiding*
Deze sectie beschrijft de impact van de werkzaamheden op de operationele uitwerking van systemen in de verkeerscentrale, objecten en langs de weg en de uitvoering van de bedientaken in de verkeerscentrale.

Voorwaarde voor het in gebruik nemen van nieuwe en of aangepaste functionaliteit is dat de (coördinerend) wegverkeersleider op de hoogte is van de nieuwe en/of gewijzigde bediening voordat deze operationeel gemaakt kan worden. De opdrachtnemer is verantwoordelijk voor het plannen, coördineren en uitvoeren van instructies, opleidingen, trainingen en/of oefenen. Ook de inzet van weginspecteurs tijdens de uitvoering van de werkzaamheden dient beschreven te worden.

2 *Operationeel verkeer*
Deze sectie beschrijft de wegaanpassingen inclusief de noodzakelijke verkeersmaatregelen (afkruisen, teksten op drip's, tekstkarren, afzettingen etc.) en de wijzigingen in de verkeerskundige configuratie / werking van de systemen.

Indien de inzet van operationeel verkeerskundigen noodzakelijk is, bijvoorbeeld voor het toetsen van documenten of het uitvoeren van testen, dient dit hier te worden beschreven.

3 *Object- en technisch beheer*
Deze sectie beschrijft de impact van de werkzaamheden op het beheer en onderhoud van objecten en/of Dynamisch Verkeersmanagement (DVM). Het serviceniveau en de storingsprocedure tijdens de uitvoering van de werkzaamheden moet duidelijk zijn. De opdrachtnemer moet zelf afspraken maken met de object of VODK (Vast Onderhoud DVM-Keten) contractant als ondersteuning bij de uitvoering gewenst is (of zelfs noodzakelijk in geval van risico's met grote gevolgen voor doorstroming en veiligheid).

B.4 Tabblad Maatregelen

Hieronder worden enkele invulvelden van het tabblad Maatregelen nader toegelicht.

Maatregelen - Verkeersmaatregelen

Inrichting van verkeersmaatregelen, bediening en omleidingen tijdens onderhoud dient te zijn gewaarborgd. De wijze hiervan hangt af van het soort maatregel, waarover in het vooroverleg afstemming plaatsvindt.

Verkeersmaatregelen dienen separaat te worden aangevraagd via het SPIN. Bij de inrichting van de verkeersmaatregelen dienen te allen tijde de richtlijnen uit CROW Publicatie 96b te worden gehanteerd.

Maatregelen – Werkvergunning Houder

In het kader van veilig werken dient elke medewerker die aanwezig is in de tunnels van WNN/MN *zich te houden aan de gestelde maatregelen.Hiervoor dienen Vergunningverstrekker en Werkvergunninghouder beide getekend te hebben. Voor praktische uitvoering kan in de Werkvergunning geregeld worden dat de hoofdaannemer zorg draagt dat elke onderaannemer de eigen instructie 'Veilig Werken' bijgewoond/gelezen en ondertekend heeft. Bij uitgifte van de Werkvergunning kan al worden getekend voor de borging van veilig werken.*

Bijlage C Aanwezigheid Registratieformulier

Datum	Tijd		Naam	Firma	Zone						Nummer Werkvergunning	Instructie gelezen?*
	Aankomst	Vertrek			1	2	2a	3	Li	Re		

Zone 1 = Buitengebied; **Zone 2** = Bediengebouw; **Zone 2a** = Dienstgebouw; **Zone 3** = Dienstgebouw elektronicaruimte. Zie Bedrijfsnoodplan Tunnels WNN/MN.

Li = Tunnelbuis links; **Re** = Tunnelbuis rechts ***** = Instructie Veilig Werken wegtunnel Tunnels WNN/MN

Procedure Werkvergunningen Tunnels WNN/MN

Bijlage D Toelichting Taak Risico Analyse

D.1 Doel Taak Risico Analyse

De Taak Risico Analyse (TRA) wordt uitgevoerd om vroegtijdig de risico's op te sporen en op te heffen dan wel te verminderen middels beheersmaatregelen van complexe en/of risicovolle werkzaamheden. Het dient om werkzaamheden goed voor te bereiden, efficiënter uit te voeren en om incidenten te voorkomen.

TRA's worden opgesteld voor werkzaamheden waarvan de risico's en te nemen maatregelen

- niet zijn opgenomen in de Risico Inventarisatie en Evaluatie (RI&E) van de exploitatiefase (definitieve gebruik) van de wegtunnel Tunnels WNN/MN;
- niet zijn onderkend in een Veiligheids- en Gezondheidsplan (V&G);
- of indien de werkzaamheden in bijzondere mate complex en/of risicovol zijn.

Om te voorkomen dat er werkzaamheden worden uitgevoerd welke onaanvaardbare risico's met zich meebrengen dient er een TRA te worden opgesteld. Met alle betrokkenen dienen de werkzaamheden stapsgewijs te worden doorlopen, om zo op gestructureerde wijze de risico's te onderkennen en de beheersmaatregelen vast te stellen. Vooral bij het uitbesteden van werkzaamheden aan derden is het van belang dat alle veiligheid, gezondheid, welzijn en milieu aspecten en risico's in een vroegtijdig stadium worden onderkend. Hiermee kunnen extra inspanningen, vertragingen en incidenten of gevaarlijke situaties op het moment van uitvoering worden voorkomen.

Het niet toepassen van deze procedure kan tot gevolg hebben dat op gebied van veiligheid, beschikbaarheid, milieu, gezondheid en kosten, de risico's van uit te voeren werkzaamheden niet tijdig onderkend worden (met incidenten als mogelijk gevolg).

Bij de keuze en de analyse van de risicovolle taak moet niet alleen gedacht worden aan de standaard werkzaamheden maar vooral ook aan werkzaamheden bij het opheffen van storingen, reiniging, onderhoud en dergelijke. De TRA dient rekening te houden met de omgeving, weggebruikers en onderhoudsmedewerkers.

De TRA wordt schriftelijk vastgelegd en schenkt aandacht aan de volgende 5 gebieden:

1. De werkzaamheden
2. De werkplek
3. De werkplekomgeving
4. De werkcondities
5. De werkcomplexiteit

De werkzaamheden zelf
Hier gaat het om de aard van de werkzaamheden die zullen moeten worden uitgevoerd. Daarbij valt te denken aan:
- industrieel schoonmaken;
- graafwerkzaamheden (met name op de tunnel en rond de tunnel toeritten);
- werken met elektriciteit;
- kort-cyclisch werk of is het werk fysiek belastend.

De werkplek
Daarbij kunnen we denken aan:
- werken in besloten ruimten;
- werken op hoogte;
- toegankelijkheid van de werkplek;
- welke bewegingsruimte hebben we tijdens de uitvoering van het werk.

De werkplekomgeving
Met betrekking tot de werkplekomgeving kunnen we ons de volgende vragen stellen:
- Hoe ziet de werkomgeving er uit?
- Wordt er boven-onder-voor-achter of naast ons tegelijkertijd ander werk uitgevoerd?
- Hebben we te maken met verkeer en wat voor soort verkeer houdt zich bij de
- werkplekomgeving op?
- Is er sprake van materiaalopslag?

De werkcondities
Onder welke omstandigheden worden de werkzaamheden uitgevoerd, dit levert de volgende vragen op:
- Hoe is het tijdens de uitvoer van de werkzaamheden met het weer gesteld?
- Met welke producten hebben we te maken?
- Hoe is het in de directe omgeving gesteld met bijvoorbeeld verlichting, geluid, temperatuur en lucht?

De werkcomplexiteit
Met betrekking tot de complexiteit stellen we de volgende vragen:
- Met welke aantallen mensen wordt het werk uitgevoerd?
- Zijn dat medewerkers van een of meerdere aannemers?
- In hoeveel tijd moet het werk worden geklaard?
- Is het een bestaand of een nieuw project dat moet worden uitgevoerd?
- Wat zijn de taakfactoren en welke persoonlijke factoren spelen een rol?

D.2 Werkwijze opstellen TRA

Een eerder opgestelde TRA kan dienen als basis voor een nieuw op te stellen, het is echter niet de bedoeling dat deze gekopieerd wordt. Wanneer er identieke werkzaamheden frequent worden uitgevoerd kan men overwegen hiervoor een werkinstructie te maken.

Wanneer er een TRA benodigd is, dient men eerst de uit te voeren werkzaamheden op te splitsen in taakstappen (1). De taakstappen worden elk op risico's beoordeeld (2). Deze risico's worden bepaald door de aard van het werk, de werkcondities, de complexiteit en, in het geval zich toch verstoringen voordoen, de ernst en de gevolgen hiervan.

Vervolgens moet worden bekeken of de risico's van bepaalde taakstappen voldoende beheerst zijn middels werkinstructies en/of procedures (3). Is dit niet het geval, dan moet een risicobepaling plaatsvinden (bijvoorbeeld door een classificatie te maken van 'laag' en 'hoog') (4). De risico's ten aanzien van een veilige doorstroming van het verkeer vormen een belangrijk onderdeel van de risicobepaling.
Ter ondersteuning van de risicobepaling kan het bijgevoegde 'TRA checklist' worden gebruikt (zie Bijlage D.3). Tot slot dienen er bij de hoog geclassificeerde risico's passende beheersmaatregelen opgesteld te worden (5). Zie hiervoor het 'TRA Formulier' (Bijlage D.4).

Algemene aandachtspunten

- Beoordelaar en de aanvrager dienen overleg te voeren tijdens of na het opstellen van de TRA.
- Wanneer een Werkvergunning met TRA wordt uitgegeven dient de beoordelaar voldoende te communiceren met de vergunninghouder.

Het opstellen (invullen) van een TRA (zie 'TRA Formulier')

- Algemene gegevens aan de bovenzijde van het formulier invullen.
- In de linker kolom de taakstappen met betrekking tot het werk of meerdere werkzaamheden invullen.
- Vermeld vervolgens in de middelste kolom per taakstap alle risico's. Het onderlinge overleg tussen de aanvrager en de verstrekker leidt tot een gezamenlijk inzicht over de risico's, dit zijn alle zaken die een negatieve invloed kunnen hebben op o.a.:
  - De veiligheid van personen (ook de gebruiker) en installaties.
  - De gezondheid en/of het welzijn van ieder individu (ook de gebruiker).
  - Het milieu (ook de omgeving).
  - De betrouwbaarheid van de installaties (lees veiligheid en beschikbaarheid).
  - Imago (wederzijds begrip tussen RWS en de omgeving).
- Tot slot worden in de rechterkolom de maatregelen vermeld die genomen dienen te worden om de genoemde risico's te beheersen. Blijkt een risico niet afdoende beheersbaar te zijn, dan moet worden overwogen een andere methodiek of techniek toe te passen. Hierbij behoort het uitstellen van bepaalde werkzaamheden naar een geschikter moment tot de mogelijkheden.

Communicatie naar betrokkenen

- Voorafgaande aan de uitvoering van de werkzaamheden waarbij een TRA van toepassing is dient er een kick-off meeting met alle leidinggevenden te worden gehouden. Het doel hiervan is een totaal overzicht te geven van de risico's, beheersmaatregelen en interacties tijdens het werk.
- Een startwerkmeeting (toolbox) door de vergunninghouder(s) van de Werkvergunning(en) met het uitvoerend personeel om de taakstappen, risico's en beheersmaatregelen door te spreken. In voorkomende gevallen neemt de verstrekker deel aan deze bespreking.

Uitvoering van werkzaamheden

- Indien er tijdens de uitvoering van werkzaamheden blijkt dat er zich een afwijking van het werkplan voordoet, stop dan direct het werk (onveilig = stoppen) en maak met de betrokkenen (tenminste aanvrager/vergunninghouder en verstrekker) een nieuwe inschatting van de risico's en bepaal daarbij de benodigde beheersmaatregelen.

D.3 TRA Checklist

Soort risico	Risico		
	Kans	*Gevolg*	*Beoordeling*
Werkomgeving			
Brand			
Explosie			
Fijnstof			
Bacteriële besmetting			
Vergiftiging			
Vallen/struikelen			
Raken bewegende delen			
Beschadiging installaties			
Elektrocutie			
Niet-ioniserende straling (gsm)			
Trillingen			
Verstikking			
Buitenlucht			
Naar buitenlucht vrijkomen van:			
- Stof			
- Stank			
- Koolwaterstoffen			
- Lawaai			
Oppervlaktewater			
Lozingen op riool naar oppervlaktewater:			
- Vervuild water kelders			
- HD reinigingswater			
- Spoelwater			
- Brandstof/olie/spills			
- Schuimvormend middel			
Bodem			
Schade aan:			
- Folie constructie			
- Kabels en leidingen			
Verontreiniging van bodem:			
- Brandstof / olie / spills			
- HD-reinigingswater			
- Spoelwater			
- Schuimvormend middel			
Afval			
- Onvoldoende scheiding			
- Onvoldoende opslag			
- Onvoldoende verpakking			
Werkcondities			
- Fysiek zwaar werk			
- Weersinvloeden			
- Klimaat (temperatuur, vocht)			
- Zicht			
- Bewegingsruimte			
- Verkeer			
- Verlichting			
- Geluidsniveau			
- Risico’s vanuit de omgeving			
Complexiteit			
- Aantal mensen tegelijkertijd			
- Verschillende aannemers			
- Veranderende condities			
- Tijdsdruk			
- Ander werk (boven, naast, onder)			
- Parallel werk in de spoortunnel			

D.4 TRA Formulier

(mede) Opstellers: _____ **_____** **Aanvrager: _____** **Verstrekker: _____** **Houder: _____**		**Werkomschrijving: _____** **_____** **W.A. nr.: _____** **Datum: _____**	**Paraaf akkoord: _____** **_____** **Aanvrager: _____** **Verstrekker: _____** **Houder: _____**
Taakstap of activiteit		**Risico/Gevaar/Blootstelling**	**Beheersmaatregelen**
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
16			
17			
18			
19			

Bijlage U Leidraad Naamgeving en Codering RWS Tunnelsysteem

Rijkswaterstaat
Ministerie van Infrastructuur en Waterstaat

Bijlage U Leidraad Naamgeving en Codering RWS Tunnelsysteem

Bijlage bij Vraagspecificatie Proces

D&C Vervanging Verlichting Schipholtunnel
Zaaknummer: 31212908

Rijkswaterstaat
Ministerie van Infrastructuur en Waterstaat

RWS INFORMATIE

Leidraad Naamgeving en Codering

Datum	27 januari 2023
Status	Definitief
Release	1.2 SP2 B4



Rijkswaterstaat
Ministerie van Infrastructuur en Waterstaat

Rijkswaterstaat
Ministerie van Infrastructuur en Waterstaat

RWS INFORMATIE

Leidraad Naamgeving en Codering

RWS Tunnelsysteem

Datum	27 januari 2023
Status	Definitief
Release	1.2 SP2 B4

Colofon

Uitgegeven door	Rijkswaterstaat | GPO
Opgesteld door	Afdeling Installaties en Bediening, Tunnelstandaard Beheer
Gecontroleerd door	Tunnelstandaard Beheer, Interne kwaliteitscontrole
Controle kwaliteitsborging	Landelijke Regisseur Veiligheid
Goedgekeurd door	Hoofd afdeling Installaties en Bediening
Manager Team LTS	Fred Bouwmeester (fred.bouwmeester@rws.nl)
Lead Architect LTS	Hans Dijkema (hans.dijkema@rws.nl)
Releasenummer	1.2 SP2 B4
Documentnummer	CON00-1600467164-484
Kader type	RWS kader
Versienummer	1.0
Classificatie	RWS Informatie
Datum	27 januari 2023
Status	Definitief

Versie historie

Datum	Versie	Toelichting	Vrijgegeven met
27 januari 2023	1.0	Definitieve versie. Afgestemd met o.a. het LTB, regio's LTS, PPO, GPO, VWM, CIV, STV, AIRBIM en diverse projecten.	Release 1.2 SP2 B4

Release notes

Wijzigingen in versie 1.0 – initiële versie

Dit betreft de eerste definitieve release van deze leidraad. De aanleiding, probleemstelling en afstemming tbv van deze leidraad zijn opgenomen in de goedgekeurde wijzigingsvoorstellen:

- WV#1609 – Opzetten uniforme codering tunnelsysteem
- WV#2404 – Nummering Noodtelefoons definiëren
- WV#1002 – Nummering HPK in de tunnel

Managementsamenvatting

Het RWS Tunnelsysteem omvat het tunnelobject inclusief het geheel van bedrijfsservices, processen, organisatie en informatie. Het tunnelobject omvat het systeem van tunnel technische installaties (Systeem TTI) en de tunnel. De tunnel betreft de civiele constructie van het kunstwerk.

Dit document beschrijft de naamgeving en codering voor het systeem TTI van het RWS Tunnelsysteem. Het geeft een systematiek voor het coderen van de diverse onderdelen van de tunnel technische installaties.

Een unieke, consistente en herkenbare naamgeving en codering draagt bij aan eenduidige communicatie tussen:

1) weggebruikers, wegverkeersleiders, weginspecteurs en hulpverleningsdiensten over de afhandeling van incidenten en calamiteiten;
2) wegverkeersleiders en beheerder over het herstel van storingen en het doorvoeren van wijzigingen;
3) Beheerder, onderhoudsaansturing (PPO), Missie Kritieke Ondersteuning (MKO) en onderhoudsaannemer over locaties, systemen, componenten, kabels en leidingen in geval van inspecties, testen, storingen of falen t.a.v. Systeem TTI.

Een uniforme naamgeving en codering is rand voorwaardelijk voor standaardisatie van de areaalgegevens als basis voor een landelijke programmering en voor de monitoring van en rapportage over de status (werking) en toestand (toestands- en instandhoudingsinspecties) van de tunnelobjecten.

Voor de naamgeving en codering van de diverse onderdelen van de tunnel technische installaties wordt uitgegaan van een generieke decompositie op basis van [SATO] en [NEN2767].

Volgens de NEN is de tunnel een beheerobject dat is opgebouwd uit elementen. De elementen komen overeen met de technische installaties en de delen van de civiele constructie. De elementen zelf zijn ook opgebouwd uit verschillende onderdelen of apparaten, de bouwdelen. De NEN kent ook componenten die onderliggend zijn aan de bouwdelen. Deze leidraad beperkt zich tot de naamgeving en codering van de tunnel technische installaties tot het niveau van bouwdelen.

Uitgangspunt is dat de codering van een bouwdeel informatie geeft over de installatie waartoe het bouwdeel behoort en de locatie van het bouwdeel in de civiele constructie van de tunnel.

De codering van de bouwdelen bestaat uit de volgende blokken:

- Object, de codering van de civiele constructie;
- Locatie, de locatie van het bouwdeel in de civiele constructie;
- Installatie, de installatie waartoe het bouwdeel behoort;
- Onderdeel, de codering en volgnummer van het bouwdeel.

In de afzonderlijke hoofdstukken wordt de naamgeving en codering van deze aspecten beschreven alsmede de toepassing ervan in de beheer management systemen en de tunnelapplicatie.

Dit document maakt deel uit van het kader Tunnelstandaard. De Tunnelstandaard wordt beheerd door GPO-IB Veiligheid & Kwaliteit, CD, VWM en LTB. Hierbij is GPO-IB Veiligheid & Kwaliteit verantwoordelijk voor de borging van de integraliteit van de Tunnelstandaard. De Leidraad Naamgeving en Codering wordt conform het kwaliteitssysteem LTS beheerd door LTB.

Inhoud

1 Inleiding 10

1.1 Identificatie 10
1.2 Doel 10
1.3 Definitie RWS Tunnelsysteem 10
1.4 Structuur en leeswijzer 10
1.5 Documentbeheer 11
1.6 Afstemming 11
1.7 Aanwijzingen voor het lezen 11

2 Referenties 13

2.1 Externe referenties 13
2.2 Interne referentie 13

3 Locatie in de tunnel 15

3.1 Tunnel 15
3.2 Tunnelbuis 15
3.3 Dwarsverbinding 17
3.4 Dienstgebouw 18
3.5 Vloeistofkelder 18
3.6 Terrein 19

4 Locatie op de weg 21

4.1 Weg 21
4.2 Baan 22
4.3 Strook 24
4.4 Codering van de locatie op de weg 26

5 Tunnel technische installaties 27

5.1 Decompositie 27
5.2 Naamgeving en codering 27
5.3 Nummering 27
5.4 Codering van de bouwdelen 29

6 Kabels en Leidingen 30

6.1 Codering 30
6.2 Nummering 30
6.3 Registratie 30
6.4 Labels 31

7 Toepassing in Beheer management systeem 32

7.1 Categorieën 32
7.2 Tunnel technische installaties 32
7.3 Bouwdelen 32
7.4 Voorbeelden 33

8 Toepassing in tunnelapplicatie 34

8.1 Tunnelapplicatie (GUI) 34
8.2 Aanraakpaneel 37
8.3 Videobeelden 38
8.4 Voorbeelden 39

Bijlage A. Rijkstunnels 40

Bijlage B. Generieke decompositie 41

Bijlage C. Tunnel technische installaties 46

Bijlage D. Onderdelen van de tunnel technische installaties 48

1 Inleiding

1.1 Identificatie

Dit document is geïdentificeerd als CON00-1600467164-484, Leidraad Naamgeving en Codering, versie 1.0, d.d. 27 januari 2023. Dit document is onderdeel van release 1.2 SP2 B4 van de landelijke tunnelstandaard (LTS).

1.2 Doel

Dit document beschrijft de naamgeving en codering voor het RWS Tunnelsysteem. Het geeft een systematiek voor het coderen van de diverse onderdelen van de tunnel technische installaties.

Een unieke, consistente en herkenbare naamgeving en codering draagt bij aan eenduidige communicatie tussen

1) weggebruikers, wegverkeersleiders, weginspecteurs en hulpverleningsdiensten over de afhandeling van incidenten en calamiteiten;
2) wegverkeersleiders en beheerder over het herstel van storingen en het doorvoeren van wijzigingen;
3) Beheerder, onderhoudsaansturing (PPO), Missie Kritieke Ondersteuning (MKO) en onderhoudsaannemer over locaties, systemen, componenten, kabels en leidingen in geval van inspecties, testen, storingen of falen t.a.v. Systeem TTI.

Een uniforme naamgeving en codering is rand voorwaardelijk voor standaardisatie van de areaalgegevens als basis voor een landelijke programmering en voor de monitoring van en rapportage over de status (werking) en toestand (toestands- en instandhoudingsinspecties) van de tunnelobjecten.

1.3 Definitie RWS Tunnelsysteem

Een tunnel is een omsloten, van de omgeving afgeschermd wegdeel in de doorgaande wegen, met als doel het kruisen van andere infrastructuur, vaak waterwegen, en/of het verhogen van de leefbaarheid van de omgeving. Een tunnel is integraal onderdeel van het hoofdwegennet.

In de systeemdefinitie RWS Tunnelsysteem (ref. [Sysdef]) wordt onderscheid gemaakt tussen RWS Tunnelsysteem, tunnelobject en tunnel.

De tunnel betreft de civiele constructie van het kunstwerk. Het tunnelobject omvat de tunnel en het systeem van tunnel technische installaties (Systeem TTI). Het RWS Tunnelsysteem omvat het tunnelobject inclusief het geheel van bedrijfsservices, processen, organisatie en informatie.

De tunnelobjecten worden als onderdeel van één geïntegreerde bediening op afstand bediend met behulp van de werkplekken op diverse bedienlocaties. De tunnelobjecten worden doorgaans bediend met behulp van de werkplekken in de verkeerscentrales maar kunnen ook lokaal worden bediend met behulp van de werkplek in de tunnel zelf. De werkplekken in de verkeerscentrales en in de tunnels zijn onderdeel van het generieke RWS bediensysteem in het bediendomein.

De weg die door de tunnel leidt, maakt deel uit van het hoofdwegennet. De weg door de tunnel en de DVM systemen, ook aangeduid als de verkeerstechnische installaties (VTI), horen niet tot de scope tot het RWS Tunnelsysteem, maar hebben wel raakvlakken met het RWS Tunnelsysteem. De codering van de onderdelen van de VTI vallen buiten de scope van dit document.

1.4 Structuur en leeswijzer

Dit document maakt onderdeel uit van de RWS Landelijke Tunnelstandaard die uit meerdere documenten bestaat. De Leeswijzer Tunnelstandaard (ref. [Leeswijzer]) geeft een toelichting op de verschillende documenten van de Tunnelstandaard alsook op de samenhang tussen deze documenten. Ook geeft de Leeswijzer de achtergrond, de aanpak en de doelgroep van de Tunnelstandaard.

Dit document is als volgt opgezet:

- Hoofdstuk 2 met de gerefereerde documenten;
- Hoofdstuk 3 met de naamgeving en codering van de locatie in de tunnel;
- Hoofdstuk 4 met de naamgeving en codering van de locatie op de weg;
- Hoofdstuk 5 met de naamgeving en codering van de tunnel technische installaties;
- Hoofdstuk 6 met de naamgeving en codering van de kabels en leidingen;
- Hoofdstuk 7 met de toepassing in het beheer management systeem;
- Hoofdstuk 8 met de toepassing in de tunnelapplicatie;
- Bijlage A met een overzicht van de Rijkstunnels in Nederland;
- Bijlage B met de door Landelijk Tunnelbeheer vastgestelde generieke decompositie;
- Bijlage C met de standaard naamgeving en codering van de tunnel technische installaties;
- Bijlage D met de standaard naamgeving en codering van de onderdelen van de installaties.

1.5 Documentbeheer

Dit document maakt deel uit van de RWS Landelijke Tunnelstandaard die momenteel integraal beheerd wordt door GPO- IB Veiligheid & Kwaliteit (ref. [Leeswijzer]).Dit document is tot stand gekomen volgens de ingerichte beheerprocessen van de LTS. In deze beheerprocessen spelen de stakeholders een belangrijke rol. Deze stakeholders zijn de vertegenwoordigers uit de betrokken RWS onderdelen (o.a. de Regio's, VWM, PPO, CIV en CD). Hierbij worden de regio's vertegenwoordigd door Landelijk Tunnelbeheer (LTB).

1.6 Afstemming

De inhoud van dit document is afgestemd met:

- Landelijk Tunnelbeheer t.b.v. assetmanagement;
- Steunpunt Tunnelveiligheid t.b.v. veiligheidsdocumentatie;
- PPO t.b.v. directe samenwerking met de marktpartijen voor uitvoering onderhoud;
- VWM t.b.v. wegverkeersleiders en weginspecteurs voor uitvoering verkeersmanagement;
- Regio WNZ, WNN, NON, ZN en MN t.b.v. configuratiemanagers en assetmanagers;
- Diverse projecten t.b.v. toepassing in de praktijk;
- Marktpartijen t.b.v. toepassing in de praktijk.

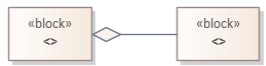
1.7 Aanwijzingen voor het lezen

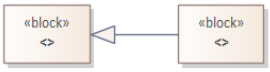
In de uitwerking van de naamgeving en codering van de tunnel technische installaties wordt gebruik gemaakt van modellen en notaties.

Voor het inzichtelijk maken van de structuur en samenhang van de civiele constructie van de tunnel en de weg wordt gebruik gemaakt van Block Definition Diagrams (BDD). Daarin worden de delen van een tunnel en een weg als blokken weergegeven inclusief de onderlinge relaties.

	Met een block wordt een systeem of een onderdeel van een systeem beschreven met de daarbij behorende coderings-methode. De blocks worden in samenhang gebracht door onderstaande relaties en regels die verderop in dit document worden beschreven.

Voor de uitwerking van de naamgeving en codering worden de volgende relaties gebruikt.

	Aggregatie; het linker blok (het geheel) is samengesteld uit de blokken rechts van de lijnen (de onderdelen).
	Compositie; het linker blok (het geheel) is samengesteld uit de blokken rechts van de lijnen (de onderdelen). Compositie is een bijzondere vorm van aggregatie waarbij de onderdelen niet kunnen bestaan zonder het geheel.

	Specialisatie; het rechter blok is afgeleid van het linker blok waarbij de eigenschappen van het linker blok ook van toepassing zijn op het rechter blok en het rechter blok eigenschappen kan toevoegen of herdefiniëren.

De coderingen van de onderdelen van de civiele constructie, van de weg en van de installaties is beschreven in Backus Naur Form (BNF). Daarbij worden de volgende symbolen gehanteerd.

< ... >	is een aanduiding die een deel van de codering representeert
=	betekent STAAT GELIJK AAN
+	betekent GEVOLGD DOOR
|	betekent OF
[...]	betekent OPTIONEEL
(...)	betekent GROEPERING
“ ... ”	betekent LETTERLIJK
<sp>	betekent spatie
<pt>	betekent punt
<+>	betekent een “+” teken
<->	betekent een “-” teken

2 Referenties

2.1 Externe referenties

Om de referenties herkenbaar te maken in de tekst worden referenties opgeschreven als ref. [afkorting document].

Referentie	Document
[SATO]	Specifieke aspecten tunnelontwerp deel 7 Tunnelinstallaties, 2005
[NEN2767]	Norm voor Conditiemeting gebouwen en infrastructuur
[BPS]	Beschrijvende Plaatsaanduiding Systematiek, DWW-2005-039, augustus 2005
[BPK]	Nota Plaatsaanduiding in knooppunten en aansluitingen, nr. 82-05, 3e versie, juni 2006
[LTS]	Referentielijst Landelijke Tunnel Standaard, versie 1.2 SP2B4

Referenties LTS producten
Voor een overzicht van alle LTS producten wordt verwezen naar de LTS Referentielijst (ref. [LTS]).

2.2 Interne referentie

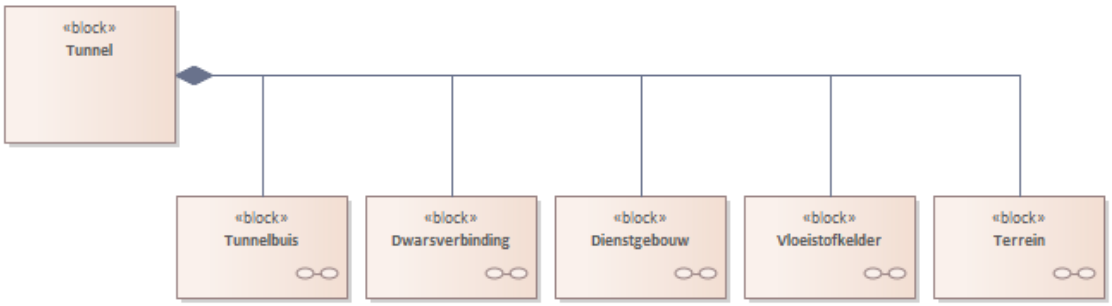
Afkorting	LTS productnaam
[A&D]	Afkortingen en definities tunnelstandaard
[Alarmteksten]	Alarmteksten (Bijlage BOMMI)
[BB2012]	Bouwbesluit 2012 Zie: http://wetten.overheid.nl/
[BehProcLTS]	Beheerprocessen tunnelstandaard
[BehJurKaders]	Beheer juridische kaders
[BOMMI]	Basisontwerp MMI RWS Tunnelsysteem
[BOTTI]	Basisontwerp TTI RWS Tunnelsysteem
[BSMMI]	Basisspecificatie MMI RWS Tunnelsysteem
[BSTTI]	Basisspecificatie TTI RWS Tunnelsysteem
[FormQRA]	Format rapportage QRA
[FormQRAdoc]	Format rapportage QRA invuldocument
[GPE]	Generieke proceseisen realisatie TTI
[Handreiking PRA]	Handreiking Prestatiegestuurde Risico Analyses, versie 1.0.0, september 2016, Rijkswaterstaat Steunpunt ProBo. Zie: https://www.leidraadse.nl
[KaderVC]	Kaders Integratie Tunnelbediening in de VC
[KaderWV]	B&O Kader Werkvergunning
[LDR-CBP]	Leidraad calamiteitenbestrijding in tunnels
[LDR-IR&E]	Leidraad incidentregistratie en –evaluatie van significante voorvallen
[LDR-ISTH]	Leidraad instandhouding tunnels
[LDR-KM]	Leidraad kwaliteitsmanagement tunnels
[Leeswijzer]	Leeswijzer tunnelstandaard

[LDR-OpenVerg]	Leidraad openstellingsvergunning
[LDR-OTO]	Leidraad opleiden, trainen en oefenen
[LDR-Tunnelorg]	Leidraad tunnelbeheerorganisatie
[LRTT]	Leidraad review toepassing tunnelstandaard
[LDR-VeiligDoc]	Leidraad Veiligheidsdocumentatie Zie: http://wetten.overheid.nl/
[LDR-Vergun]	Leidraad vergunningen tunnels
[LDR V&V]	Leidraad Verificatie en Validatie Tunnelstandaard
[LDR-Werkz]	Leidraad werkzaamheden in tunnels
[LR-NC]	Leidraad Naamgeving en Codering
[LTT-BS]	Leidraad toepassing tunnelstandaard in bestaande tunnels
[LTTT]	Leidraad toetsing toepassing tunnelstandaard
[LTTT-Vragen]	Leidraad toetsing toepassing tunnelstandaard vragenlijst (Bijlage A)
[OpBehProces]	Operationele tunnelbeheerprocessen
[QA-LTS]	Kwaliteitsborging tunnelstandaard
[RARVW]	Regeling aanvullende regels veiligheid wegtunnels (Rarvw). Zie: http://wetten.overheid.nl/
[RS-NwWetg]	Richtsnoer nieuwe wetgeving
[SysDef]	Systeemdefinitie RWS Tunnelsysteem
[SysOntw]	Systeemontwerp RWS Tunnelsysteem
[SysSpec]	Systeemspecificatie RWS Tunnelsysteem
[UPP]	Bedrijfsprocessen (UPP) RWS Tunnelsysteem
[Trac_RARVW]	Tracering RARVW (Bijlage BSTTI)
[UPP-HTML]	Bedrijfsprocessen (UPP) toelichting in HTML
[WARVW]	Wet aanvullende regels veiligheid wegtunnels (Warvw). Zie: http://wetten.overheid.nl/
[WWIA]	Werkwijzer uitvoering impactanalyse bij toepassing tunnelstandaard in bestaande tunnels
[WWAT]	Werkwijze aanleg tunnels
[WWAS]	Werkwijzer aanpassing software in bestaande tunnels

3 Locatie in de tunnel

Dit hoofdstuk beschrijft de systematiek voor de naamgeving en codering van de locatie in de tunnel. De locatie in de tunnel wordt aangeduid aan de hand van de onderdelen van de civiele constructie van de tunnel. De codering van de locatie in de tunnel heeft een vaste lengte.

Onderstaand model toont de structuur en samenhang van de civiele constructie van een tunnel waarin de onderdelen als blokken weergegeven inclusief de onderlinge relaties.



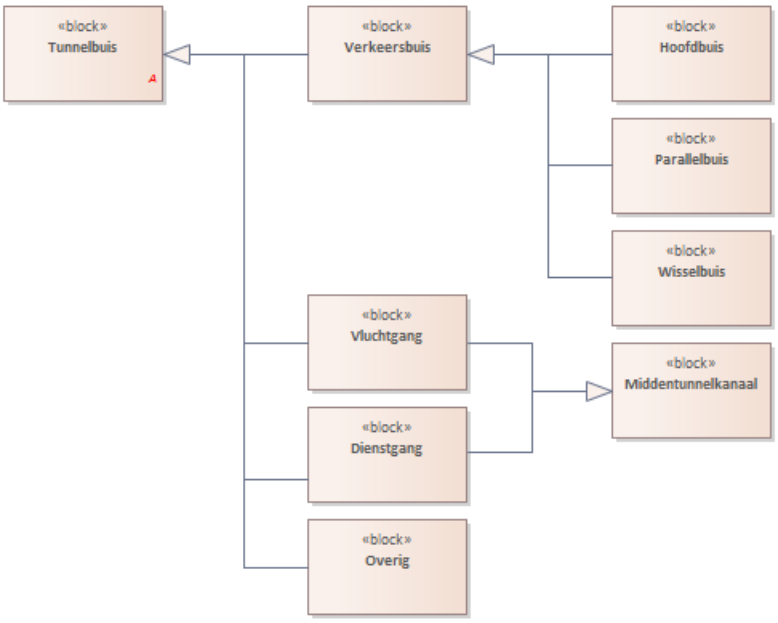
Afbeelding 1 – Civiel model van de tunnel

3.1 Tunnel

De tunnel zijnde de civiele constructie van het kunstwerk waarin de tunnel technische installaties zijn geplaatst, wordt aangeduid met een 3-letter code. Zie Bijlage A voor het overzicht van de door Landelijk Tunnelbeheer vastgestelde naamgeving en codering van alle Rijkstunnels in Nederland.

3.2 Tunnelbuis

Onderstaand model geeft een overzicht van de verschillende soorten tunnelbuizen. Hier wordt gebruik gemaakt van een specialisatie relatie, zoals eerder uitgelegd in 1.7. Eigenschappen die aan ‘Tunnelbuis’ zijn toegekend gelden ook voor ‘Verkeersbuis’. ‘Verkeersbuis’ kan eigenschappen toevoegen of eigenschappen herdefiniëren.



Afbeelding 2 – Overzicht soorten tunnelbuizen

In een tunnel worden de volgende soorten tunnelbuizen onderscheiden:
- Verkeersbuis, biedt ruimte voor een rijbaan van het hoofdwegennet;
- Vluchtgang, kanaal tussen twee verkeersbuizen dat dienst doet als vluchtroute;
- Dienstgang, kanaal waarin o.a. kabels, leidingen en systeemkasten zijn aangebracht;
- Overig, bijvoorbeeld een tunnelbuis voor langzaam verkeer of fietsers.

Een vluchtgang en dienstgang vormen samen vaak het Middentunnelkanaal.

In tunnels met meer dan twee verkeersbuizen worden de volgende verkeersbuizen onderscheiden:
- Hoofdbuis;
- Parallelbuis;
- Wisselbuis.

Tunnels met meer dan twee verkeersbuizen zijn doorgaans voorzien van meer dan één middentunnelkanaal. Elk middentunnelkanaal heeft een eigen vlucht- en dienstgang.

Een dienstgang is niet altijd onderdeel van een middentunnelkanaal. In bijvoorbeeld een boortunnel kan de dienstgang zijn gerealiseerd in de ruimte onder het wegdek.
Bij tunnels met een vluchtconcept via de middenwand naar de ondersteunende buis is er geen vluchtgang. De middenwand is onderdeel van de civiele constructie van de verkeersbuizen.

Naast de verkeersbuizen en de vlucht- en dienstgangen zijn er tunnelbuizen die voor andere doeleinden worden gebruikt, bijvoorbeeld:
- Langzaam verkeer in de tweede Heinenoordtunnel;
- Fietsbuizen in de Benelux tunnel.

Als een tunnel meer dan één tunnelbuis van dezelfde soort heeft, worden de buizen onderling onderscheiden met behulp van de positie van de buis ten opzichte van de wegoriëntatielijn.

De tunnelbuizen worden gecodeerd met een 2-letter code bestaande uit de aanduiding van de soort tunnelbuis eventueel gevolgd door de positie ten opzichte van de wegoriëntatielijn.

De tunnelbuizen worden in de lengterichting opgedeeld in secties van 50 meter. Deze secties worden aangeduid als tunnelsectie en moeten niet worden verward met de betonnen tunnelsegmenten (moten) waarmee de tunnelbuizen zijn gecreëerd. De nummering van de tunnelsecties begint bij 1 en loopt op in de richting van oplopende hectometrering.

De in- en uitritten in de open tunnelbak in het verlengde van de tunnelbuizen worden ook aangemerkt als tunnelsectie. De gehele open tunnelbak wordt als één sectie aangemerkt. De lengte van deze sectie is gelijk aan de lengte van de open tunnelbak en is dus meestal niet 50 meter. De inrit van de verkeersbuizen rechts en de uitrit van de verkeersbuizen links worden aangeduid met sectienummer 0. De uitrit rechts en de inrit links worden aangeduid met het nummer dat gelijk is aan het aantal tunnelsecties plus 1.

De plaats in de tunnelbuizen en de in- en uitritten wordt aangeduid aan de hand van het nummer van de tunnelsecties. Per tunnel dient een plattegrond beschikbaar te zijn met de tunnelbuizen en de nummering en omschrijving van de tunnelsegmenten incl. in- en uitritten.

De codering van de locatie in de tunnelbuizen is als volgt opgebouwd:
- Scheidingsteken <+>;
- De code van de soort tunnelbuis;
- Optioneel de positie van de tunnelbuis ten opzichte van de wegoriëntatielijn;
- Scheidingsteken <pt>;
- Twee-cijferig nummer van de tunnelsectie met voorloopnullen.

Onderstaande tabel toont de codering van de locatie in tunnelbuizen.

Verkeersbuis	Code	Positie	Codering	Sectie	Locatiecode
Verkeersbuis (2-buis tunnel)	Li/Re	n.v.t.	Li/Re	XX	+Li.XX
Parallelbuis	P	L/R	PL/PR	XX	+PL.XX
Hoofdbuis	H	L/R	HL/HR	XX	+HL.XX
Wisselbuis	Wi	n.v.t.	Wi	XX	+Wi.XX

Vluchtgang	Code	Positie	Codering	Sectie	Locatiecode
Vluchtgang (2-buis tunnel)	VG	n.v.t.	VG	XX	+VG.XX
Vluchtgang	V	L/R	VL/VR	XX	+VL.XX

Dienstgang	Code	Positie	Codering	Sectie	Locatiecode
Dienstgang (2-buis tunnel)	DG	n.v.t.	DG	XX	+DG.XX
Dienstgang	D	L/R	DL/DR	XX	+DL.XX

Overig	Code	Positie	Codering	Sectie	Locatiecode
Fietsbuis (enkel)	FB	n.v.t.	FB	XX	+FB.XX
Fietsbuis	F	L/R	FL/FR	XX	+FL.XX
Langzaam verkeer (enkel)	LV	n.v.t.	LV	XX	+LV.XX
Langzaam verkeer	L	L/R	LL/LR	XX	+LR.XX

Tabel 1 – Codering locatie in tunnelbuizen

3.3 Dwarsverbinding

Een dwarsverbinding is een verbinding tussen tunnelbuizen.
In een dwarsverbindingen worden de volgende ruimten onderscheiden:

- Vluchtruimte;
- Dienstruimte;

De dwarsverbindingen worden aangeduid met een volgnummer en zijn niet gerelateerd aan de tunnelsecties. De nummering begint bij 1 en loopt op in de richting van oplopende hectometrering.

De codering van de dwarsverbindingen is als volgt opgebouwd:

- Scheidingsteken <+>;
- De code van de ruimte in de dwarsverbinding;
- Scheidingsteken <pt>;
- Twee-cijferig volgnummer met voorloopnullen.

Onderstaande tabel toont de codering van de locatie in dwarsverbindingen.

Dwarsverbinding	Codering	Volgnummer	Locatiecode
Vluchtruimte	DV	XX	+DV.XX
Dienstruimte	DD	XX	+DD.XX

Tabel 2 – Codering locatie in dwarsverbindingen

3.4 Dienstgebouw

Een dienstgebouw van een tunnel huisvest de dienstruimtes waar apparatuur ten behoeve van (een deel van) de tunnel technische installaties wordt geplaatst. Het gebouw biedt bescherming tegen ongewenste, externe natuurlijke en menselijke invloeden. Ook kan een dienstgebouw een bedienruimte en kantoren bevatten. Per tunnel zijn er doorgaans meerdere dienstgebouwen.
De codering van de dienstgebouwen is afhankelijk van de positie van het dienstgebouw ten opzichte van de oriëntatierichting van de tunnel op basis van kompas richtingen (NOZWM).

De plaats in de dienstgebouwen wordt aangeduid aan de hand van niveau- en ruimtenummers. De niveaus worden aangeduid met een 1-cijferig nummer. De ruimtes worden aangeduid met een 2-cijferig nummer. Per dienstgebouw dient per niveau een plattegrond beschikbaar te zijn met de nummering en omschrijving van de functie van de afzonderlijke ruimten.

De codering van de locatie in de dienstgebouwen wordt voorafgegaan door de positie van het niveau ten opzichte van de begane grond: <+> voor de niveaus van de begane grond (ingang) en hoger en <-> voor de niveaus onder de begane grond.

De codering van de locatie in de dienstgebouwen is als volgt opgebouwd:
- Positie ten opzichte van de begane grond;
- Code van de dienstgebouw;
- Positie van het dienstgebouw;
- 1-cijferig nummer voor het niveau;
- 2-cijferig nummer van de ruimte met voorloopnullen.

Onderstaande tabel toont de codering van de locatie in dienstgebouwen.

Dienstgebouw	Code	Positie	Codering	Niveau	Ruimte	Locatiecode
Noord	D	N	DN	y	xx	+DNyxx
Oost	D	O	DO	y	xx	+DOyxx
Zuid	D	Z	DZ	-1	xx	-DZ1xx
West	D	W	DW	0	xx	+DW0xx
Midden	D	M	DM	+1	xx	+DM1xx

Tabel 3 – Codering locatie in dienstgebouwen

3.5 Vloeistofkelder

In een tunnel worden de volgende soorten vloeistofkelders onderscheiden:
- Middenkelder op het diepste punt onder de tunnelbuizen;
- Hoofdkelders aan het begin van de tunnelbuizen;
- Hellingkelders ter hoogte van de toeritten.

In veel gevallen zijn de hoofdkelders onderdeel van de dienstgebouwen. In dat geval is de codering van de hoofdkelders onderdeel van de codering voor de dienstgebouwen. Als de hoofdkelders buiten de dienstgebouwen zijn gerealiseerd, worden deze als vloeistofkelder gecodeerd.
In de praktijk worden de ruimtes in de vloeistofkelders niet apart gecodeerd. De vloeistofkelders worden gecodeerd op basis van de locatie van de kelder ten opzichte van de tunnel en of de weg.

De hoofd- en middenkelders worden gecodeerd op basis van de positie van de kelders ten opzichte van de oriëntatierichting van de tunnel op basis van kompas richtingen (NOZWM) en de plaats in de tunnelbuizen. De plaats in de tunnelbuizen worden aangeduid met behulp van de tunnelsecties.

De hellingkelders worden gecodeerd op basis van de locatie in het gebied buiten de tunnel. De codering van de locatie op het terrein buiten de tunnel is beschreven in de volgende paragraaf.

De codering van de locatie van de vloeistofkelders is als volgt opgebouwd:

- Scheidingsteken <+>;
- Code voor vloeistofkelders;
- Positie ten opzichte van de wegoriëntatielijn (alleen voor hellingkelders);
- Positie ten opzichte van de oriëntatierichting van de tunnel;
- Scheidingsteken <pt> (alleen voor hoofd- en middelkelders);
- Twee-cijferig sectienummer met voorloopnullen.

Onderstaande tabel toont de codering van de locatie in vloeistofkelders.

Vloeistofkelder	Code	Pos Wol	Pos Tun	Codering	Sectie	Locatiecode
Middenkelder	V	n.v.t.	M	VM	XX	+VM.XX
Hoofdkelder	V	n.v.t.	N/O/Z/W	VN/…	XX	+VN.XX
Hellingkelder	V	L/R	N/O/Z/W	VLN/…	XX	+VLNXX

Tabel 4 – Codering locatie in vloeistofkelders

3.6 Terrein

Het terrein van de tunnel omvat het gebied buiten de tunnel met uitzondering van de tunnelbuizen en de rijbanen in het verlengde ervan. De volgende gebieden onderscheiden:

- Hoofdrijbanen;
- Parallelbanen;
- Wisselbanen;
- Middenbermen;
- Tussenbermen;
- Ingesloten bermen;
- Buitenbermen;
- Overige gebieden.

Het gebied buiten de tunnel is onderverdeeld in deelgebieden op basis van

- positie ten opzichte van de wegoriëntatielijn;
- positie ten opzichte van de oriëntatierichting van de tunnel.

Het gebied buiten de tunnel wordt net als de tunnelbuizen en de in- en uitritten ingedeeld in secties. De secties in het gebied buiten de tunnel worden aangeduid als terreinsecties. De terreinsecties hebben een lengte van 100 meter m.u.v. de eerste sectie ter hoogte van de open tunnelbak. De lengte van deze terreinsectie is gelijk aan de lengte van de open tunnelbak en is dus meestal niet 50 meter. De lengte is gelijk aan die van de tunnelsectie in de open tunnelbak. De nummering begint bij 0 en neemt toe in de richting van de tunnel vandaan.

De codering van de locatie in het gebied buiten de tunnel is als volgt opgebouwd:

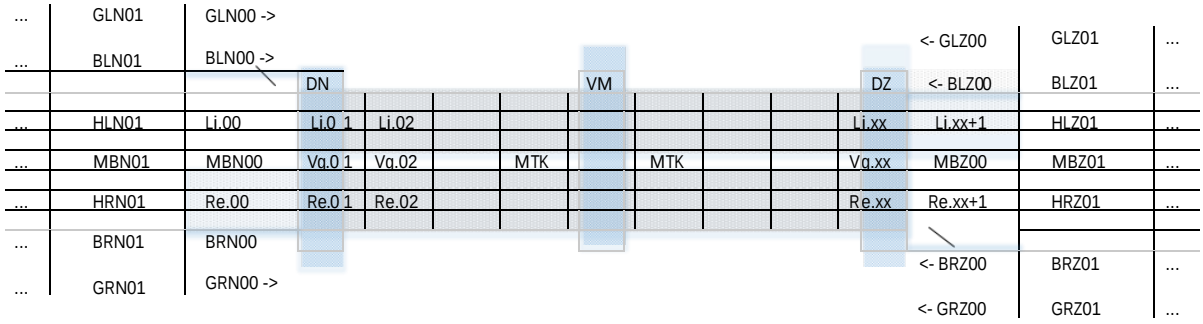
- Scheidingsteken <+>;
- Code voor soort terrein;
- Positie ten opzichte van de wegoriëntatielijn (m.u.v. middenberm);
- Positie ten opzichte van de oriëntatierichting van de tunnel;
- Scheidingsteken <pt> (alleen bij middenberm);
- Twee-cijferig nummer van de terreinsectie met voorloopnullen.

Onderstaande tabel toont de codering van de locatie in de deelgebieden buiten de tunnel.

Deelgebieden	Code	Pos Wol	Pos Tun	Codering	Sectie	Locatiecode
Hoofdrijbaan	H	L/R	N/O/Z/W	HLN/...	XX	+HLNXX
Parallelbaan	P	L/R	N/O/Z/W	PLN/...	XX	+PLNXX
Wisselbaan	WI	n.v.t.	N/O/Z/W	WIN/...	XX	+WINXX
Middenberm	MB	n.v.t.	N/O/Z/W	MBN/...	XX	+MBNXX
Tussenberm	T	L/R	N/O/Z/W	TLN/...	XX	+TLNXX
Ingesloten berm	I	L/R	N/O/Z/W	ILN/...	XX	+ILNXX
Buitenberm	B	L/R	N/O/Z/W	BLN/...	XX	+BLNXX
Overige gebieden	G	L/R	N/O/Z/W	GLN/...	XX	+GLNXX

Tabel 5 – Codering locatie in terrein

Onderstaande afbeelding geeft een voorbeeld van de locatiecodes voor een 2-buis tunnel met MTK.



Afbeelding 3 – Locatiecodes 2-buis tunnel met MTK

Naast de dienstgebouwen en de vloeistofkelders worden in sommige gevallen ook andere gebouwen op het tunnelterrein gerealiseerd. Dergelijke gebouwen zijn geen onderdeel van het RWS Tunnelsysteem maar er is wel een raakvlak. Vooralsnog worden alleen de gebouwen voor de aansluiting op het elektriciteitsnet en het landelijke netwerk van Rijkswaterstaat onderkend.

Onderstaande tabel toont de codering van de locatie van de overige gebouwen op het terrein.

Overige gebouwen	Code	Pos Wol	Pos Tun	Sectie	Locatiecode
Energiegebouw	E	L/R	N/O/Z/W	XX	+ELNXX
Netwerkgebouw (CVR)	N	L/R	N/O/Z/W	XX	+NLNXX

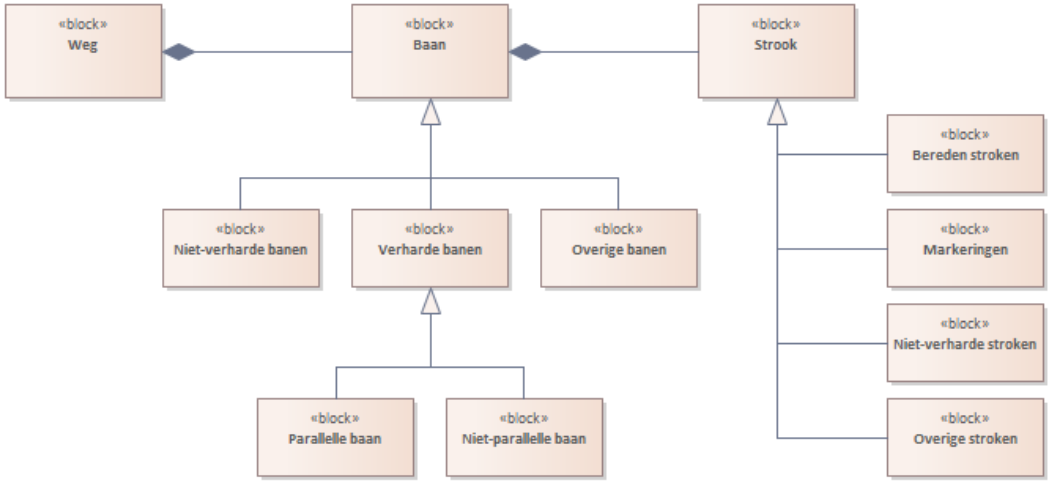
Tabel 6 – Codering locatie overige gebouwen op terrein

4 Locatie op de weg

Dit hoofdstuk beschrijft de systematiek voor de naamgeving en codering van de locatie op de weg. Naast de locatie in de civiele constructie van de tunnel is de locatie op de weg minstens zo belangrijk. Deze aanduiding wordt voornamelijk gebruikt in de communicatie tussen de wegverkeersleiders, weginspecteurs, hulpverleningsdiensten en weggebruikers.

De plaatsbepaling op de wegen in het RWS Tunnelsysteem is gebaseerd op het document ‘Beschrijvende Plaatsbepaling Systematiek’, ref. [BPS]. Voor het RWS Tunnelsysteem is het van belang de afzonderlijke wegen, banen en eventueel stroken eenduidig te identificeren.
Als gevolg hiervan heeft de codering van de locatie op de weg geen vaste lengte.

De locatie op de wegen wordt bepaald aan de hand van onderstaand civiel model van de weg.



Afbeelding 4 – Civiel model van de weg

4.1 Weg

Een weg is een voor verkeersdoeleinden bestemd gebied, in lengte- en dwarsrichting begrensd door weggrenzen. Dit kunnen onderhoudsgrenzen, eigendomsgrenzen of beheergrenzen zijn.
De plaats op de weg wordt bepaald op basis van wegsoort, wegnummer en de positie op de weg.

4.1.1 Wegsoort

Volgens [BPS] worden de wegen gecodeerd op basis van wegsoorten, bijvoorbeeld rijksweg en provinciale weg, gevolgd door het wegnummer met voorloopnullen. In de praktijk wordt deze codering niet of nauwelijks gebruikt. In plaats daarvan worden de wegen gecodeerd op basis van wegtype en wegnummer zonder voorloopnullen.

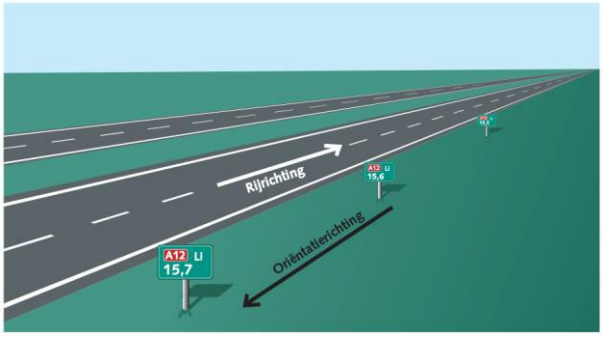
Onderstaande tabel geeft een overzicht van de verschillende wegtypes.

Wegtype	Codering
Autosnelweg	A
Niet-autosnelweg	N
Stadsroute	S

Tabel 7 – Codering wegtype

4.1.2 Positie op weg

Voor het bepalen van de positie in de lengterichting van de weg wordt gebruik gemaakt van de oriëntatierichting van de weg. De oriëntatierichting van de weg is de richting van de oplopende hectometrering. De oriëntatierichting is dus niet altijd gelijk aan de rijrichting van het verkeer.



Afbeelding 5 – Oriëntatierichting van en rijrichting op de weg

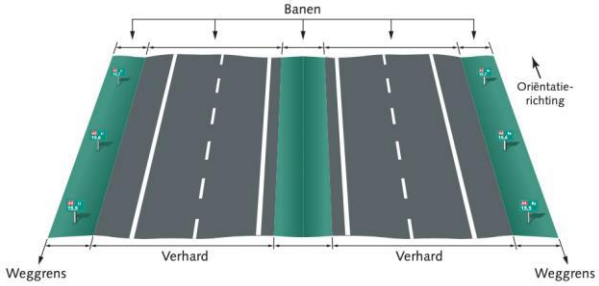
De positie in de lengterichting van de weg wordt bepaald met behulp van de hectometerborden langs de weg en de afstand tot het dichtstbijzijnde hectometerbord. Kijkend in de oriëntatierichting van de weg kan de positie zich zowel voor als achter het hectometerbord bevinden. De afstand is negatief als de positie op de weg, kijkend in de oriëntatierichting van de weg, voor het hectometerbord ligt. De afstand is positief als de positie op de weg achter het hectometerbord ligt.

De positie in de lengterichting van de weg is gelijk aan de som van de hectometrering op het hectometerbord en de afstand tot dit bord in hele meters.

4.2 Baan

Een weg is in de dwarsrichting (breedte) opgedeeld in banen.

Een baan is een gebied op de weg, in lengterichting begrensd door een begin- en een eindraai[1], en in dwarsrichting begrensd door twee opeenvolgende overgangsgrenzen verhard/onverhard, of door een overgangsgrens verhard/onverhard en een weggrens in dwarsrichting.



Afbeelding 6 – Voorbeeld van banen op een weg

De plaats van een baan op de weg wordt bepaald aan de hand van de soort baan, de positie van de baan ten opzichte van de wegoriëntatielijn en het volgnummer van de baan.

4.2.1 Baansoort

In [BPS] is een onderverdeling gemaakt in baansoorten. Daarbij wordt onderscheid gemaakt in verharde en niet-verharde banen en in parallelle en niet-parallelle banen.

Parallelle banen zijn banen die parallel liggen ten opzichte van de wegoriëntatielijn. Voor het RWS Tunnelsysteem zijn alleen de hoofdrijbanen (verhard) en de bermen (niet-verhard) van belang.

[1] Een raai is een denkbeeldige lijn dwars op de weg.

Onderstaande tabel toont de codering van de voor tunnels relevante parallelle banen.

Parallelle baan	Codering
Hoofdrijbaan	HR
Middenberm	MB
Tussenberm	TB
Ingesloten berm	IB
Buitenberm	BB

Tabel 8 – Codering parallelle banen

Niet-parallelle banen zijn banen die niet parallel liggen ten opzichte van de wegoriëntatielijn. Voor het RWS Tunnelsysteem zijn alleen de verbindingswegen van belang.

Voor de codering van verbindingswegen wordt uitgegaan van de door de beheerder vastgestelde hectometreringsletter op basis van de nota Plaatsaanduiding in knooppunten en aansluitingen (ref. [BPK]). De hectometreringsletter is afhankelijk van het type verbindingsweg en de oriëntatierichting op de hoofdrijbaan (oplopende/aflopende hectometrering).

Onderstaande tabel toont de codering van de voor tunnels relevante verbindingswegen.

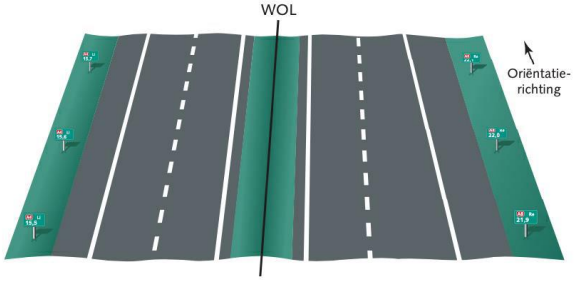
Verbindingsweg	Hectometrering	Codering
Afrit	Oplopend	a
Toerit	Oplopend	b
Afrit	Aflopend	c
Toerit	Aflopend	d
Parallelbaan	Oplopend	m, x
Parallelbaan	Aflopend	n, y
Wisselbaan	n.v.t.	z

Tabel 9 – Codering verbindingswegen

4.2.2 Positie baan op weg

De positie van een baan in de dwarsrichting van de weg wordt bepaald aan de hand van de wegoriëntatielijn (wol). Het bepalen van de positie is alleen van toepassing voor parallelle banen.

De wegoriëntatielijn is een lijn ten opzichte waarvan de positie van een buis in een tunnel of een baan op een weg in de dwarsrichting wordt bepaald. De wegoriëntatielijn is niet altijd zichtbaar.



Afbeelding 7 – De plaats van de wegoriëntatielijn op de weg

Onderstaande tabel toont de codering van de positie van de banen t.o.v. de wegoriëntatielijn kijkend in de richting van de oplopende hectometrering.

Positie t.o.v. wegoriëntatielijn	Codering
Links	L/Li
Rechts	R/Re
Midden	M
Niet van toepassing	n.v.t.

Tabel 10 – Codering positie baan t.o.v. wegoriëntatielijn

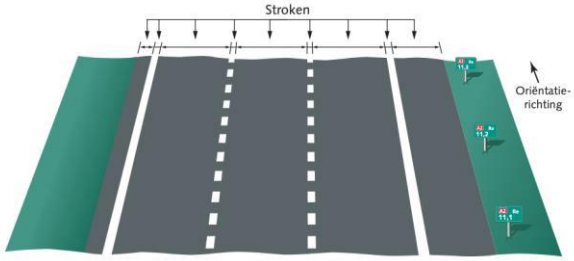
4.2.3 Volgnummer baan

Het toekennen van een volgnummer is alleen van toepassing voor parallelle banen. Voor het volgnummer van de baan worden vanaf de wegoriëntatielijn de banen van dezelfde soort geteld. Een baan met positie Midden heeft een volgnummer 0. Om de codering compact te houden, wordt het volgnummer alleen vermeld als deze groter is dan 1.

4.3 Strook

Een baan is in de dwarsrichting (breedte) opgedeeld in stroken.

Een strook is een gebied op een baan (van de weg) in lengterichting begrensd door een begin- en een eindraai, en in dwarsrichting begrensd door twee opeenvolgende zichtbare overgangsgrenzen tussen verschillende materies of door zichtbare kniklijnen. De mogelijke materies zijn: betonverharding, bitumenverharding, bestrating en lengtemarkering.



Afbeelding 8 – De stroken op een rijbaan

De plaats van een strook op een baan van de weg wordt bepaald aan de hand van de soort strook, de positie van de strook ten opzichte van de baanoriëntatielijn en het volgnummer van de strook.

4.3.1 Strooksoort

In [BPS] is een onderverdelen gemaakt in strooksoorten. Daarbij wordt onderscheid gemaakt in bereden stroken, markeringen, niet-verharde en overige stroken.

Onderstaande tabel toont de codering van de voor het RWS Tunnelsysteem relevante stroken.

Strooksoort	Codering
Bereden stroken	
Rijstrook	R-
Vuchtstrook	V-
Correctiestrook / Redresseerstrook	C-
Uitrijstrook	U-
Invoegstrook	I-
Weefstrook	W-
Kruipstrook	L-

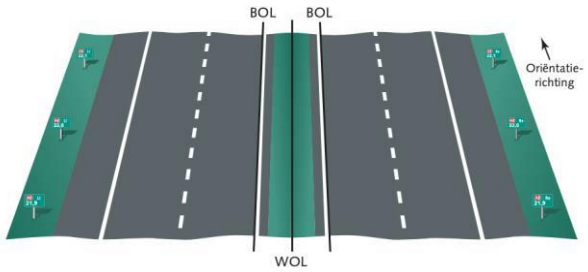
Markeringen	
Kantstreep	K-
Deelstreep	D-
Asstreep	A-
Niet-verharde stroken	
Bovenberm	BB
Talud	TU
Onderberm	OB

Tabel 11 – Codering strooksoorten

4.3.2 Positie strook op baan

De positie van een strook in de dwarsrichting van de baan wordt bepaald aan de hand van de baanoriëntatielijn (bol). De baanoriëntatielijn is een lijn ten opzichte waarvan de positie van een strook op een baan in de dwarsrichting wordt bepaald. De baanoriëntatielijn is niet altijd zichtbaar.

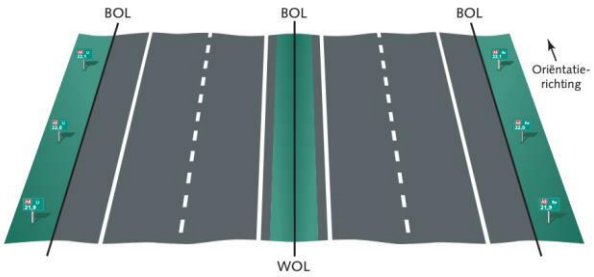
Op een baan met één rijrichting bevindt de baanoriëntatielijn zich op de binnenste grens van de binnenste rijstrook gezien vanuit de positie van de wegoriëntatielijn. Bij een verbindingsweg wordt de binnenste rijstrook bepaald vanaf het beginpunt van de verbindingsweg.



Afbeelding 9 – De plaats van de baanoriëntatielijn voor hoofdrijbanen

Op een baan die niet bestemd is voor verkeer (bermen), bevindt de baanoriëntatielijn zich:

- Bij de middenberm in het midden van deze baan
- Bij de overige bermen op de binnenste grens van de berm (vanuit de wegoriëntatielijn)



Afbeelding 10 – De plaats van de baanoriëntatielijn voor bermen

Onderstaande tabel toont de codering van de positie van stroken t.o.v. de baanoriëntatielijn kijkend in de oriëntatierichting van de weg (in de richting van de oplopende hectometrering).

Positie t.o.v. baanoriëntatielijn	Codering
Links	L
Rechts	R
Midden	M
Niet van toepassing	N

Tabel 12 – Codering positie strook t.o.v. baanoriëntatielijn

Dit betekent dat op de hoofdrijbanen rechts t.o.v. de wegoriëntatielijn de rijstroken altijd rechts liggen t.o.v. de baanoriëntatielijn en op de hoofdrijbanen links de rijstroken altijd links liggen.

4.3.3 Volgnummer strook

Voor het volgnummer van de strook worden vanaf de baanoriëntatielijn de stroken van dezelfde soort geteld. Een strook met positie M (midden) heeft volgnummer 0, bijvoorbeeld een asstreep.

4.4 Codering van de locatie op de weg

De codering van de weg is als volgt opgebouwd:
- Wegsoort;
- Wegnummer zonder voorloopnullen.

De codering van de hoofdrijbanen is als volgt opgebouwd:
- Wegsoort;
- Wegnummer zonder voorloopnullen;
- Scheidingsteken <sp>;
- Positie van de baan ten opzichte van de wegoriëntatielijn (lange notatie).

De codering van de bermen is als volgt opgebouwd:
- Wegsoort;
- Wegnummer zonder voorloopnullen;
- Scheidingsteken <sp>;
- Volgnummer van de baan (alleen bij 2 of meer);
- Bermsoort;
- Positie van de baan ten opzichte van de wegoriëntatielijn (m.u.v. middenberm).

De codering van de verbindingswegen is als volgt opgebouwd:
- Wegsoort;
- Wegnummer zonder voorloopnullen;
- Hectometreringsletter.

Onderstaande tabel toont de codering van de locatie op de weg.

Baan	Nummer	Soort	Positie	Letter	Positie	Locatiecode
Hoofdrijbaan	1	HR	Li/Re	n.v.t.	X,XX	A4 Li X,XX
Middenberm	0	MB	M	n.v.t.	X,XX	A5 MB X,XX
Tussenberm	1	TB	L/R	n.v.t.	X,XX	A6 TBL X,XX
Tussenberm	>1	TB	L/R	n.v.t.	X,XX	A9 2TBL X,XX
Buitenberm	1	BB	L/R	n.v.t.	X,XX	A10 BBR X,XX
Ingeslotenberm	1	IB	L/R	n.v.t.	X,XX	A12 IBL X,XX
Verbindingsweg	n.v.t.	VW	n.v.t.	a-z	X,XX	A9x X,XX

Tabel 13 – Codering locatie op de weg

5 Tunnel technische installaties

Dit hoofdstuk beschrijft de systematiek voor de naamgeving en codering van de diverse onderdelen van de tunnel technische installaties van het RWS Tunnelsysteem.

5.1 Decompositie

Voor de naamgeving en codering van de diverse onderdelen van de tunnel technische installaties wordt uitgegaan van een generieke decompositie op basis van [SATO] en [NEN2767].

In de SATO zijn de tunnel technische installaties ingedeeld in een aantal categorieën en zijn de installaties voorzien van een standaard installatienummer.

Volgens de NEN is de tunnel een beheerobject dat is opgebouwd uit elementen. De elementen komen overeen met de technische installaties en de delen van de civiele constructie. De elementen zelf zijn ook opgebouwd uit verschillende onderdelen of apparaten, de bouwdelen. De NEN kent ook componenten die onderliggend zijn aan de bouwdelen. Deze leidraad beperkt zich tot de naamgeving en codering van de tunnel technische installaties tot het niveau van bouwdelen.

Bijlage B bevat de door Landelijk Tunnelbeheer (LTB) vastgestelde generieke decompositie van het RWS Tunnelsysteem met per installatie de omschrijving en het installatienummer volgens de SATO en de codering en omschrijving van de bijbehorende elementen volgens de NEN2767.

5.2 Naamgeving en codering

Voor een eenduidige communicatie is het van belang dat alle gebruikers van het RWS Tunnel-systeem voor de installaties en de bouwdelen dezelfde naamgeving en codering hanteren.

Bijlage C geeft een overzicht van de tunnel technische installaties met per installatie de standaard naamgeving en codering.

Bijlage D bevat een overzicht van de bouwdelen met per bouwdeel de standaard naamgeving en codering.

Voor een unieke codering is naast de naamgeving en codering een identificatie van de installatie of het bouwdeel noodzakelijk.

De identificatie van de installaties is gebaseerd op de locatie in de civiele constructie van de tunnel of weg. De identificatie van de bouwdelen is eveneens gebaseerd op de locatie in de civiele constructie aangevuld met een volgnummer binnen het betreffende onderdeel van de constructie.

5.3 Nummering

Het volgnummer in de identificatie van de bouwdelen is afhankelijk van de locatie in de civiele constructie van de tunnel of weg. De nummering van bouwdelen wordt hierna nader toegelicht. Het identificatienummer van de bouwdelen is een 3-cijferig nummer met voorloopnullen.

5.3.1 Verkeersbuis

De bouwdelen in de verkeersbuizen en op de rijbanen in het verlengde van de verkeersbuizen worden genummerd in de lengterichting, in de dwarsrichting of een combinatie van beide.

Voorbeelden van bouwdelen die alleen in de lengterichting worden genummerd zijn camera's. Bouwdelen die alleen in de dwarsrichting worden genummerd zijn bijvoorbeeld verkeerslichten. Voorbeelden van bouwdelen die zowel in de lengterichting als in de dwarsrichting worden genummerd zijn SOS detectielussen, SOS secties en de ventilatieclusters.

De bouwdelen worden per installatie en per verkeersbuis inclusief de rijbanen genummerd.
De nummering in de lengterichting begint bij 1 en loopt op in de rijrichting van het verkeer.

De nummering in de dwarsrichting begint bij 1 en loopt op van links naar rechts kijkend in de rijrichting van het verkeer. Het identificatienummer is een 3-cijferig nummer bestaande uit 1) alleen een 3-cijferig nummer in de lengterichting, of 2) een 2-cijferig nummer in de lengterichting gevolgd door een 1-cijferig nummer in de dwarsrichting. Alle voorzien van voorloopnullen.

NB: het volgnummer in de dwarsrichting betreft een logische nummering en moet niet worden verward met het volgnummer van de stroken op de baan als onderdeel van de codering van de locatie op de weg (zie Hoofdstuk 4).

5.3.2 Vluchtdeuren en Hulpposten

De nummering van vluchtdeuren en de hulpposten is afwijkend ten opzichte van de overige bouwdelen in de verkeersbuizen. De volgende type vluchtdeuren worden onderscheiden:

- Vluchtdeuren, voor het vluchten van de calamiteitenbuis naar de vluchtgang in het middentunnelkanaal of naar de ondersteunende buis. Er zijn fail-safe afsluitbare varianten van de vluchtdeuren. Deze hebben dezelfde naamgeving als de niet-afsluitbare varianten;
- Aanvalsdeuren, worden door de brandweer gebruikt om via de ondersteunende buis in de calamiteitenbuis te komen;
- Einddeuren, bieden een veilige uitgang vanuit de vluchtgang in de gescheiden secties in het middentunnelkanaal via de ondersteunende buis naar de verzamelplaats;
- Kopdeuren, bieden een veilige uitgang vanuit de vluchtgang in het middentunnelkanaal naar de verzamelplaats (een kopdeur is dus geen onderdeel van een verkeerbuis).

De vluchtdeuren, aanvalsdeuren en einddeuren worden aangeduid met een 2-cijferig nummer.

De vluchtdeuren, aanvalsdeuren en einddeuren hebben een eigen nummering, beginnend bij 1, die meeloopt met de hectometrering. Tegenover elkaar liggende vluchtdeuren van een middentunnel-kanaal of een dwarsverbinding hebben hetzelfde nummer. Dit geldt ook voor de tegenover elkaar liggende einddeuren in de secties van een middentunnelkanaal. Dit betekent dat in tunnels met verspringende tunnelmonden de nummering van de deuren niet in alle buizen altijd bij 1 begint.

De kopdeuren van het middentunnelkanaal worden aangeduid aan de hand van de codering van het middentunnelkanaal en de positie van de kopdeur t.o.v. de oriëntatierichting van de tunnel.

De hulpposten worden genummerd rondom een vluchtdeur met een 3-cijferig nummer. Een hulppostkast hoort bij de dichtstbijzijnde vluchtdeur. De eerste twee cijfers zijn gelijk aan het nummer van de dichtstbijzijnde vluchtdeur. Het derde cijfer is het volgnummer van de hulppost. Het volgnummer begint bij 1 en loopt mee met de hectometrering. De hulpposten aan de zijde van de middenwand, dwarsverbindingen of middentunnelkanaal worden oneven genummerd. De hulpposten aan de andere zijde van de verkeersbuis worden even genummerd.

5.3.3 Vluchtgang en Dienstgang

De bouwdelen in de vlucht- en dienstgangen kunnen betrekking hebben op de installaties t.b.v. de vlucht- en dienstgang zelf en op de installaties t.b.v. de verkeersbuizen links en rechts van de gang. Deze bouwdelen worden onderling onderscheiden door middel van het identificatienummer.

Het identificatienummer van de bouwdelen in de vlucht- en dienstgangen is een 3-cijferig nummer met voorloopnullen. De bouwdelen worden per gang en per installatie als volgt genummerd.

- 001-399 voor de bouwdelen t.b.v. de installaties in de vlucht- en dienstgang zelf;
- 401-699 voor de bouwdelen t.b.v. de verkeersbuis links van de vlucht- of dienstgang;
- 701-999 voor de bouwdelen t.b.v. de verkeersbuis rechts van de vlucht- of dienstgang.

De nummering van de bouwdelen in de vlucht- en dienstgangen begint bij xx1. De nummering van de bouwdelen t.b.v. de installaties in de vlucht- en dienstgangen zelf loopt op in de richting van de oplopende hectometrering. De nummering van de bouwdelen t.b.v. de installaties in de verkeersbuizen links en rechts van de gangen loopt op in de rijrichting van het verkeer.

5.3.4 Dienstgebouw en Vloeistofkelder

De bouwdelen van de installaties in de dienstgebouwen en de vloeistofkelders worden per gebouw en per installatie genummerd beginnend bij 1.

5.3.5 Buiten de tunnel

De bouwdelen buiten de tunnel op de terreinen en in de bermen die niet zijn gerelateerd aan een verkeersbuis, dienstgebouw of vloeistofkelder worden genummerd per deelgebied beginnend bij 1.

5.4 Codering van de bouwdelen

De codering van de bouwdelen heeft een vaste lengte en is als volgt opgebouwd:

- Objectidentificatie, de 3-lettercode van de tunnel;
- Locatie in de tunnel, zie Hoofdstuk 3;
- Scheidingsteken <->;
- Installatiecode, het 2-cijferig nummer van de deelinstallatie volgens de SATO;
- Scheidingsteken <->;
- Bouwdeelcode, de 3-lettercode van het bouwdeel;
- Nummer, het 3-cijferig identificatienummer van het bouwdeel.

Voorbeelden van de codering van willekeurige bouwdelen van willekeurige installaties:

Bouwdeel	Tunnel	Locatie	Installatie	Bouwdeel	Nummer	Bouwdeelcodering
Vluchtdeur	EHT	+Li.02	91	VLD	002	EHT+Li.02-91-VLD002
Hulppost	EHT	+Li.02	53	HPA	021	EHT+Li.02-53-HPA021
Noodtelefoon	EHT	+Li.02	64	NTT	021	EHT+Li.02-64-NTT021
Camera	EHT	+Re.14	61	CAM	018	EHT+Re.14-61-CAM018
Luidspreker	EHT	+VG.01	63	LSP	052	EHT+VG.01-63-LSP052
Ventilator	EHT	+Re.00	36	VVB	013	EHT+Re.00-36-VEN013
Afsluitboom	EHT	+MBN01	44	ASB	002	EHT+MBN01-44-ASB002
Brandblus-pomp	EHT	-DZ204	51	BBP	001	EHT-DZ204-51-BBP001

Tabel 14 – Voorbeelden van de codering van willekeurige bouwdelen.

6 Kabels en Leidingen

Dit hoofdstuk beschrijft de systematiek voor de naamgeving en codering van de diverse kabels en leidingen ten behoeve van de tunnel technische installaties van het RWS Tunnelsysteem.

6.1 Codering

De codering van de kabels en leidingen heeft een vaste lengte en is als volgt opgebouwd:

- Objectidentificatie, de 3-lettercode van de tunnel;
- Scheidingsteken <->;
- Installatiecode, het 2-cijferig nummer van de installatie waar de kabel naar toe gaat;
- Scheidingsteken <->;
- Identificatienummer, het 4-cijferig nummer van de kabel of leiding.

Bijvoorbeeld: EHT-10-1001.

6.2 Nummering

Kabels en leidingen hebben een uniek 4-cijferig nummer. Bij de nummering van de afzonderlijke kabels en leidingen wordt rekening gehouden met de verschillende soorten die worden toegepast. Het eerste cijfer, de duizendtallen, representeert de soort kabel of leiding. Onderstaande tabel toont de duizendtallen die aan de diverse soorten kabels en leidingen zijn toegekend.

Kabels en leidingen	Codering
Leidingen	0000
Voeding	1000
NoBreak voeding	3000
Signaal / koper	5000
Netwerk / koper	6000
Netwerk / glas	7000
Netwerk / PoE	8000
Combikabel	9000

Tabel 15 – Nummering kabels en leidingen

Binnen deze duizendtallen wordt aan elke kabel en leiding een uniek nummer toegekend.

6.3 Registratie

Bij het uitgeven van kabelnummers worden de volgende gegevens geregistreerd:

- Beheerobject, afgebakende eenheid van bovenliggend netwerk. In dit geval “tunnels”;
- Objectidentificatie, de 3-lettercode van de tunnel;
- Installatiecode, het 2-cijferig nummer van de deelinstallatie volgens de SATO;
- Kabelnummer, het 4-cijferig identificatienummer van de kabel of leiding;
- Begin, de onderdeelcodering van het bouwdeel aan het begin van de kabel of leiding;
- Einde, de onderdeelcodering van het bouwdeel aan het einde van de kabel of leiding;
- Kabeltype, bijvoorbeeld YMvK-mb;
- Kabeldoorsnede, in aantal aderen x oppervlakte in mm^2, bijvoorbeeld 2x1,5 mm^2;
- Kabellengte, lengte van de kabel in meters;
- Status: geleverd, gereserveerd, in gebruik, niet gebruikt, vervallen, verwijderd, beschadigd;
- Beheerder, eigenaar van de kabel/leiding, bijvoorbeeld WNN, WNZ, PPO, CIV.

6.4 Labels

Alle kabels en leidingen worden voorzien van labels met daarop de codering van de betreffende kabel of leiding. De kabels en leidingen dienen op de volgende plaatsen te zijn voorzien van labels:

- Op onderlinge afstanden van maximaal 10 m en in het middentunnelkanaal maximaal 30m;
- Bij een bundeling van kabels, binnen een afstand van 2 m;
- Bij een doorgang door vloer of muur, binnen een afstand van 1 m aan beide zijden;
- Bij een horizontale of verticale bocht, binnen een afstand van 1 m aan beide zijden;
- Op kabellasdozen voor het verlengen van een kabel;
- Nabij de invoering van schakel- en verdeelinrichtingen, binnen een afstand van 50 cm;
- Nabij de invoering van een aan te sluiten apparaat, binnen een afstand van 50 cm.

De uitvoering van de labels is als volgt:

- Grootte 50x15 mm;
- Kleur achtergrond geel;
- Kleur opdruk zwart;
- Hoogte opdruk 10 mm;
- Bevestiging met kabelbundelbandje aan beide uiteindes van het label.

7 Toepassing in Beheer management systeem

De beheerder registreert de ‘areaal gegevens’ van de tunnel in een beheer management systeem (BMS) als basis voor de registratie van de statusinformatie (technische werking) en bijbehorende storingsmeldingen en de resultaten van de toestands- en instandhoudingsinspecties (staat van onderhoud) ten behoeve van het monitoren van de prestaties van het tunnelobject.

Een uniforme naamgeving en codering van de installaties en de bouwdelen is een voorwaarde voor standaardisatie van de ‘areaal gegevens’ als basis voor een landelijk uniforme programmering en de management informatie over de verschillende tunnelobjecten.

Voor de registratie van de bouwdelen maakt de beheerder gebruik van de generieke decompositie zoals beschreven in §5.1 Decompositie.

7.1 Categorieën

In het beheer management systeem wordt per tunnel een standaard indeling van de categorieën op basis van SATO getoond. De categorieën worden aangeduid met een 3-cijferig nummer (met voorloopnullen) en de omschrijving van de categorieën op basis van SATO, zie Bijlage B.

In het beheer management systeem ziet de standaard indeling per tunnel er als volgt uit.

- Hoofdsysteem (Voor tunnels is dit altijd “HoofdWegenNet”);
  - Systeem (Voor de Wijkertunnel is dit “Rijksweg 09”);
    - Deelsysteem (Voor de Wijkertunnel is dit “KP Velzen – Uitgeest (R)”);
      - Beheerobject (Voor de Wijkertunnel is dit “Wijkertunnel (A9)”);
        - 000 Algemeen;
        - 010 Energievoorziening;
        - 020 Verlichting;
        - 030 Vloeistofpompinstallatie;
        - 035 Ventilatiesystemen;
        - 040 Verkeersinstallaties;
        - 050 Brandblus installaties;
        - 060 Communicatie;
        - 070 Gebouwinstallaties;
        - 080 Besturingsinstallaties;
        - 090 Diverse installaties;
        - 100 Tunnelbuis civiel;
        - 200 Toetritten civiel;
        - 300 Dienstgebouwen civiel;
        - 400 Terrein.

7.2 Tunnel technische installaties

Per categorie wordt een standaard indeling van de installaties getoond. De installaties worden aangeduid met een 2-cijferig nummer (met voorloopnullen) en de naam van de installaties op basis van SATO, zie Bijlage B.

In het beheer management systeem ziet de indeling van bijvoorbeeld de ventilatiesystemen er als volgt uit.

- 035 Ventilatiesystemen;
  - 36 Ventilatie installatie Tunnel;
  - 37 Meetinstallatie Luchtkwaliteit;
  - 38 Overdrukinstallatie Grensruimte;
  - 39 Overdrukinstallatie Veilige Ruimte.

7.3 Bouwdelen

Per installatie worden de bouwdelen geregistreerd. De bouwdelen worden gegroepeerd op basis van de naam van een bouwdeel. Zie Bijlage D voor de naam van de bouwdelen.

Als een bouwdeel in verschillende delen van de civiele constructie voorkomt, wordt een onderverdeling gemaakt op basis van de locatie in de tunnel. Voor de groepering wordt de naam van het bouwdeel aangevuld met de codering van het onderdeel van de civiele constructie.

In het beheer management systeem ziet de indeling van bijv. ventilatiesystemen er als volgt uit.

- 035 Ventilatiesystemen;
  - 36 Ventilatie installatie Tunnel;
    - Ventilator verkeersbuis Li;
    - Ventilator verkeersbuis Re;
    - Werkschakelaar Li;
    - Werkschakelaar Re;
    - Klemmenkast.

Binnen deze onderverdeling worden de afzonderlijke instanties van de bouwdelen geregistreerd.
De bouwdelen worden aangeduid met de naam en de onderdeelcodering van het bouwdeel.
Als van het betreffende bouwdeel een locatie op de weg beschikbaar is, wordt deze toegevoegd.

- Zie Bijlage D voor de naam van de bouwdelen.
- Zie Hoofdstuk 5 voor de onderdeelcodering van de bouwdelen.
- Zie Hoofdstuk 4 voor de codering van de locatie op de weg.

Voor een eenduidige communicatie tussen wegverkeersleiders, beheerder en onderhoudsaannemer wordt in de tunnelapplicatie van de wegverkeersleiders en in het beheer management systeem van de beheerder dezelfde naam, codering en identificatienummer van de bouwdelen gehanteerd.

In het beheer management systeem worden per bouwdeel de volgende gegevens vastgelegd:

- SATO categorienummer en –omschrijving;
- SATO installatienummer en –omschrijving;
- NEN elementnummer en –omschrijving;
- NEN bouwdeelnummer en –omschrijving;
- Locatie op de weg (indien van toepassing).

7.4 Voorbeelden

Voorbeelden van de codering in het beheer management systeem van willekeurige bouwdelen:

Hiërarchie in BMS	Bouwdeelcodering	Locatiecodering weg
030 Vloeistofpompinstallatie		
31 Hoofdpompinstallatie		
Pomp		
Pomp	WKT+DN002-31-VAP001	
035 Ventilatiesystemen		
36 Ventilatie installatie		
Ventilatie Verkeersbuis Li		
Ventilator Verkeersbuis	WKT+Li.07-36-VVB023	A9 Li 53,45
Klemmenkast		
Klemmenkast	WKT+DG.07-36-KLK421	
060 Communicatie		
61 CCTV		
Aansluitkast		
Aansluitkast	WKT+DG.06-61-AKA411	-
Camera Li		
Camera	WKT+Li.06-61-CAM004	A9 Li 52,17

8 Toepassing in tunnelapplicatie

Voor de communicatie tussen wegverkeersleiders, weginspecteurs en hulpverleningsdiensten wordt gebruik gemaakt van de aanduidingen van de installaties en de bouwdelen in de MMI van de wegverkeersleider. Belangrijkste uitgangspunt is consistente toepassing van de naamgeving en codering in met name de tunnelapplicatie (GUI), het aanraakpaneel (MAP) en de videobeelden.

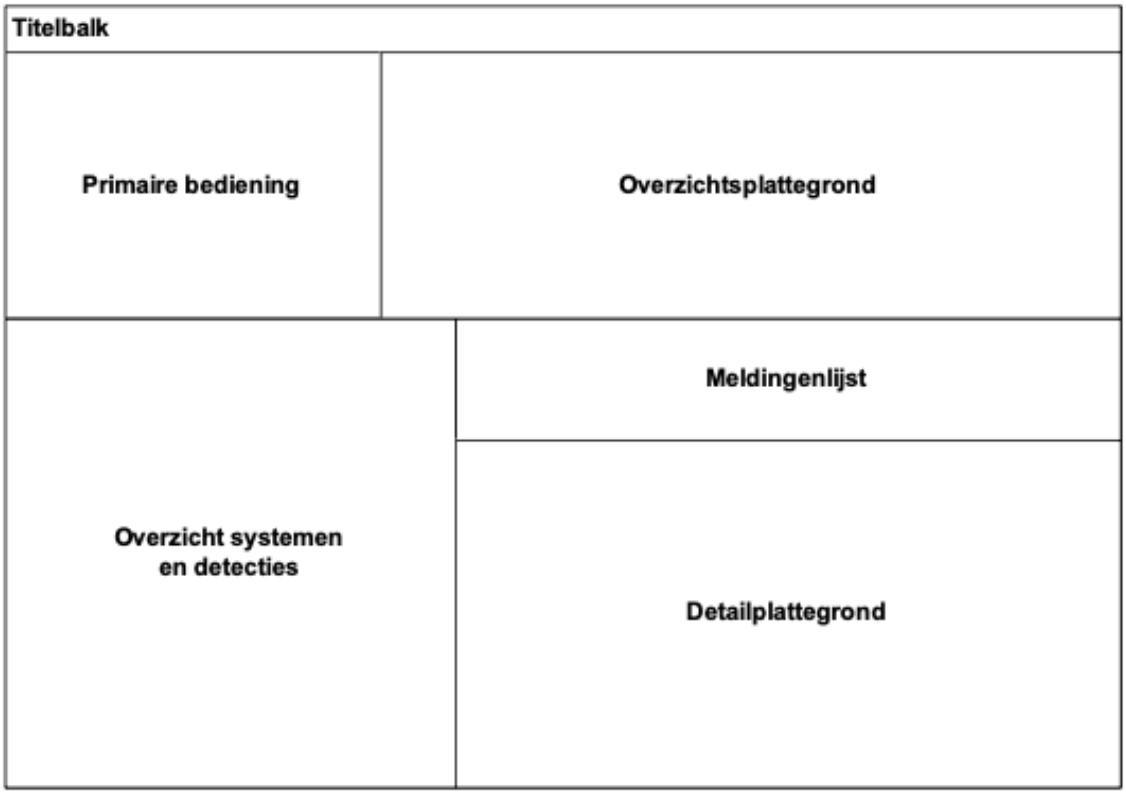
Voor een eenduidige communicatie tussen wegverkeersleiders en de beheerder en onderhouds-aannemer is het van belang dat de naamgeving en codering van de installaties en bouwdelen in de MMI van de wegverkeersleiders consistent is met die in het beheer management systeem (BMS) van de beheerder. Daarvoor is het noodzakelijk dat de codering voor bediening eenduidig kan worden afgebeeld op de codering voor beheer en onderhoud. Andersom niet per definitie.

Het ontwerp van de MMI voor wegverkeersleiders, bestaande uit de tunnelapplicatie (GUI), het aanraakpaneel (MAP) en de videobeelden op de videowand, is beschreven in de basisspecificatie van de MMI (ref. [BSMMI]) en het basisontwerp van de MMI (ref. [BOMMI]).

Dit hoofdstuk beschrijft hoe de naamgeving en codering van de civiele constructie van de tunnel, de wegen door de tunnel en de tunnel technische installaties in de tunnel uit de voorgaande hoofdstukken worden toegepast in de verschillende delen van de MMI voor wegverkeersleiders.

8.1 Tunnelapplicatie (GUI)

De tunnelapplicatie bestaat uit vijf panelen en een titelbalk.



Afbeelding 11 – Schematische weergave van de tunnelapplicatie

In de volgende paragrafen wordt per paneel de functie van het paneel en de naamgeving en de codering van de relevante onderdelen van het tunnelobject in het paneel nader toegelicht.

8.1.1 Titelbalk

De titelbalk toont de door Landelijk Tunnelbeheer vastgestelde naam van de tunnel, zie Bijlage A.

8.1.2 Primaire bediening

De primaire bediening is het gedeelte van het scherm met bedieningsmogelijkheden en informatie die óf veel gebruikt zijn, óf belangrijk zijn om snel te kunnen bedienen (in geval van incidenten).

Per verkeersbuis omvat de primaire bediening het instellen van de state, het bedienen van de verkeerslichten en afsluitbomen en belangrijke camera gerelateerde bediening.

- Zie Tabel 1 voor de codering van de verkeersbuizen.

8.1.3 Overzichtsplattegrond

De overzichtsplattegrond toont een visualisatie van de plattegrond van het tunneltracé met de constructie van de tunnel en de relevante rijbanen. Het betreft de rijbanen door de verkeersbuizen en de aansluitende wegen van het hoofdwegennet en eventueel onderliggend wegennet.
Afhankelijk van het vluchtconcept wordt de veilige ruimte aangeduid met de vaste aanduiding “Middentunnelkanaal” of de codering van de dwarsverbindingen. De hectometerborden komen overeen met de borden langs de weg en bevatten de rijbaan aanduiding en de hectometer positie.

- Zie Bijlage A voor de naam van de tunnel(s);
- Zie Tabel 2 voor de codering van de dwarsverbindingen;
- Zie Hoofdstuk 3 voor de codering van de verkeersbuizen;
- Zie Hoofdstuk 4 voor de codering van de wegen en de rijbanen.

8.1.4 Meldingenlijst

De meldingenlijst bevat de volgende velden:

- Type alarm of melding;
- Identificatienummer van de camera, indien van toepassing;
- Datum en tijdstip waarop de melding is opgekomen;
- Locatie van de installatie of het bouwdeel;
- Meldtekst conform Alarmenlijst van [LTS];
- Notitie als vrije tekst.

Meldingen van installaties bevatten de naam van de installatie waarop de melding betrekking heeft, gevolgd door de meldtekst zelf. Het veld locatie bevat de codering van de tunnelbuis, dienstgebouw, vloeistofkelder of “Tunnel” (voor installaties op het niveau van tunnel).
Zie Bijlage C voor de naam van de installatie.
Zie Hoofdstuk 3 voor de codering van de tunnelbuizen, dienstgebouwen en vloeistofkelders.

Meldingen van bouwdelen bevatten de codering en het identificatienummer van het bouwdeel waarop de melding betrekking heeft, gevolgd door de meldtekst zelf. Het veld locatie bevat bij voorkeur de codering van de locatie of de weg of anders de locatie in de tunnel.

- Zie Hoofdstuk 3 voor de codering van de locatie in de tunnel;
- Zie Hoofdstuk 4 voor de codering van de locatie op de weg;
- Zie Hoofdstuk 5 voor de codering en nummering van de bouwdelen.

8.1.5 Detailplattegrond

De detailplattegrond geeft een deel van de tunnel weer, inclusief relevante aanwezige systemen. Het betreft de weergave van meldingen, verkeerskundige plattegrond of een systeemoverzicht.

8.1.5.1 Meldingen

Door op het ‘Meldingen’ tab te klikken, wordt een overzicht van de bevestigde meldingen getoond. Deze bevestigde meldingenlijst bevat dezelfde velden als de meldingenlijst (zie §8.1.4).

8.1.5.2 Verkeerskundige plattegrond

De verkeerskundige plattegrond kan worden geopend door op het ‘Verkeer’ tab te klikken. Het geeft een afbeelding van een deel van de tunnel. De afbeelding toont de verkeersbuizen en wegen, met op de juiste plek alle actieve meldingen en de relevante bouwdelen die in het betreffende deel van de tunnel aanwezig zijn waaronder verkeerslichten, afsluitbomen, camera’s en vluchtdeuren. Van de camera’s en de vluchtdeuren zijn de identificatienummers zichtbaar.

- Zie Tabel 1 voor de codering van de verkeersbuizen;
- Zie Hoofdstuk 5 voor de nummering van camera’s en vluchtdeuren.

8.1.5.3 Systeemoverzicht

Het Systeemoverzicht kan worden geopend door op één van de ‘Systeem’ tabs te klikken. Het aantal tabs hangt af van de opbouw van de tunnel.

De systeem tabs hebben een vaste indeling met knoppen voor de installaties gegroepeerd per verkeersbuis, veilige ruimte, dienstgebouw en tunnel.

Zie Tabel 1 en *Tabel 3* voor de codering van respectievelijk de verkeersbuizen en dienstgebouwen. Afhankelijk van het vluchtconcept wordt de veilige ruimte aangeduid met de vaste tekst “MTK” in geval van een Middentunnelkanaal of “DV” in geval van dwarsverbindingen.
Zie Bijlage C voor de naam van de installaties die in de knoppen wordt getoond.

Na indrukken van één van de knoppen in het Systeemoverzicht wordt het detailsysteemoverzicht van de betreffende installatie geopend. Er is een detailsysteemoverzicht voor alle voor beheer noodzakelijke installaties. De detailoverzichten tonen de afzonderlijke bouwdelen van de installaties. Zie Bijlage C en Bijlage D voor de codering van de installaties en de bouwdelen.

8.1.5.4 Overzicht Systemen en Detecties

Het ‘Overzicht Systemen en Detecties’ kan worden geopend door op één van de tabs te klikken. Het aantal tabs hangt af van de opbouw van de tunnel. In dit overzicht is een – wat de wegverkeersleiders betreft – compleet overzicht te zien van de installaties en bouwdelen, deelsysteemalarmen, deelsysteemstoringen en verkeerskundige alarmen in de tunnel.

Van de installaties worden de naam van de installatie en de codering van het civiele onderdeel getoond. Zie Bijlage C voor de naam van de installatie en Hoofdstuk 3 voor de codering van het civiele onderdeel van de tunnel.

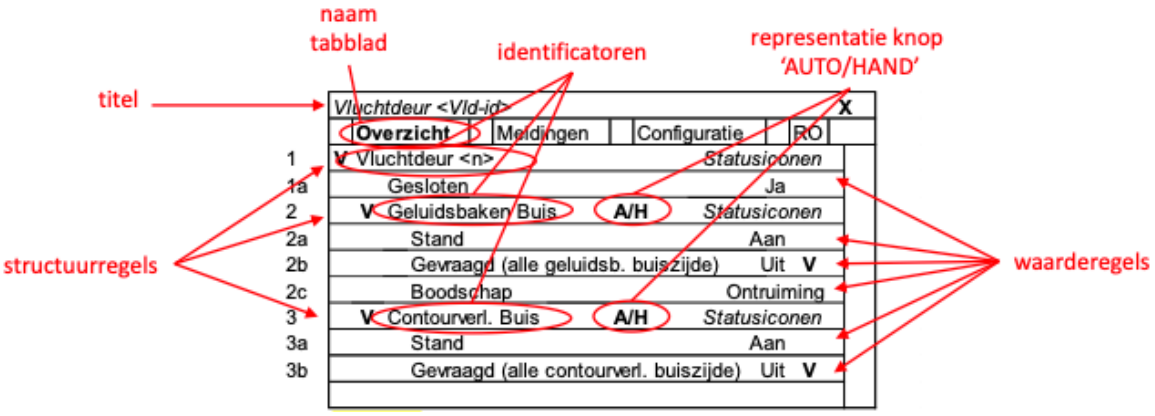
Van de bouwdelen wordt de naam van het bouwdeel, de codering van het civiele onderdeel en het identificatienummer van het bouwdeel getoond. Zie Hoofdstuk 3 voor de codering van het civiele onderdeel van Hoofdstuk 5 voor de naamgeving en nummering van de bouwdelen.

8.1.6 Visuele elementen

De tunnelapplicatie bevat een aantal visuele elementen waaruit de hierboven beschreven panelen zijn opgebouwd en die op diverse plaatsen in de tunnelapplicatie terugkomen. De naamgeving en codering in de elementen met installaties en bouwdelen worden hieronder beschreven.

8.1.6.1 Faceplates

Per installatie/bouwdeel waarvoor een icoon op de detailplattegrond voorkomt, is een faceplate beschikbaar. Onderstaande afbeelding toont een schematische weergave van een faceplate.



Afbeelding 12 – Voorbeeld visueel overzicht van faceplate Vluchtdeur, tabblad 'Overzicht'

In een faceplate worden naast een titelregel ook structuurregels en waarderegels onderscheiden. Structuurregels groeperen de waarderegels volgens de logische opbouw en bevatten identificaties van de installaties en bouwdelen. Waarderegels bevatten informatie over installaties en bouwdelen. Dit komt overeen met de naamgeving en codering in het Overzicht Systemen en Detecties.

8.1.6.2 Pop-up bedienmenu's

Door met een enkele muisklik rechts op een icoon in de detailplattegrond te klikken, verschijnt een klein pop-up-bedienmenu voor het bedienen van het betreffende bouwdeel. De kopregel van het pop-up-bedienmenu bevat de naam van het bouwdeel, de codering van het civiele onderdeel en het identificatienummer van het bouwdeel. Zie Hoofdstuk 3 voor de codering van het civiele onderdeel van Hoofdstuk 5 voor de naamgeving en nummering van de bouwdelen.

8.1.6.3 Tooltips

Als de muispointer zich langer dan een halve seconde boven een icoon op de detailplattegrond bevindt, wordt een informatieve tekst getoond met daarin de naam en de codering van het betreffende bouwdeel en de locatie van het bouwdeel op de weg.

- Zie hoofdstuk 4 voor de codering van de locatie op de weg;
- Zie hoofdstuk 5 voor de naamgeving en codering van de bouwdelen.

8.2 Aanraakpaneel

Het aanraakpaneel op de werkplek van de wegverkeersleider en biedt naast functies voor werkplekbediening ook functies voor communicatie en bediening op afstand. In volgende paragrafen is de naamgeving en codering met betrekking tot tunnels beschreven.

8.2.1 Communicatie

Een oproep van intercom of noodtelefoon wordt getoond in de wachtrij op het aanraakpaneel op de werkplek o.v.v. het nummer en de identificatie van het intercom of noodtelefoon toestel.
Zie Hoofdstuk 5 voor de codering van de intercom- en noodtelefoontoestellen.

8.2.2 Bediening op afstand

Het aanraakpaneel biedt functionaliteit voor de bediening van tunnels op afstand. Het betreft de functies voor calamiteitenbediening, noodbediening en omroep toespreken. Deze functies zijn voor een tunnel beschikbaar in een apart tabblad op het aanraakpaneel.
Op de tab wordt de codering van de tunnel getoond, zie Bijlage A.

8.2.2.1 calamiteitenbediening

In het tabbladgedeelte voor calamiteitenbediening wordt per verkeersbuis een calamiteitenknop getoond met per knop de identificatie van de verkeersbuis en de actuele state van de buis.

Zie Tabel 1 voor de codering van de verkeersbuizen.

8.2.2.2 Live toespreken

Voor het live toespreken in de tunnel wordt in het tabblad een spreeksleutel getoond. Onder de spreeksleutel wordt aangegeven welk deel van de tunnel toegesproken gaat worden:

- Tunnel;
- Verkeersbuis;
- Omroepsectie;
- Omroepsectie bij camera;
- Veilige ruimte[2];
- Omroepsectie veilige ruimte.

Zie Tabel 1 voor de codering van de verkeersbuizen.
Afhankelijk van het vluchtconcept wordt de veilige ruimte aangeduid met de codering van de vluchtgang, zie *Tabel 1*, of de codering van de dwarsverbindingen, zie *Tabel 2*.

8.2.2.3 Noodbediening

In het tabbladgedeelte voor Noodbediening is het mogelijk de afzonderlijke verkeersbuizen en toeleidende rijbanen naar de verkeersbuizen af te sluiten voor het verkeer. Per afsluiter wordt bij de knoppen “VKL Rood” en “Afsluitbomen Neer” de identificatie van de verkeersbuis of toeleidende rijbaan getoond.

Zie Tabel 1 voor de codering van de verkeersbuizen.
Zie Hoofdstuk 4 voor de codering van de locatie op de wegen en de rijbanen.

Bij de knop “Afsluitbomen Neer” wordt de identificatie van de afzonderlijke afsluitbomen getoond
De identificatie van de afsluitboom is opgebouwd uit de naam van het bouwdeel gevolgd door de codering van de rijbaan en eventueel het volgnummer van de afsluitboom.

8.3 Videobeelden

In het videobeeld wordt linksboven de identificatie van de camera en linksonder de locatie van de camera getoond. Daarbij wordt onderscheid gemaakt tussen de camera’s in de verkeersbuizen en in het verlengde ervan en de camera’s rondom dienstgebouwen.

De identificatie van de camera’s in de verkeersbuizen bestaat uit de identificatie van de tunnel en het identificatienummer van de camera in de verkeersbuis of op de rijbaan in het verlengde van de verkeersbuis gescheiden door een spatie, bijvoorbeeld MDT 01.

- Zie Bijlage A voor de naam van de tunnel(s);
- Zie hoofdstuk 5 voor de nummering van de camera’s.

De locatie van de camera in de verkeersbuizen en in het verlengde ervan is gebaseerd op de locatie van de camera op de rijbaan. Bijvoorbeeld A24 Li 2,54 of A15f 42,49.
Zie hoofdstuk 4 voor de codering van de locatie op de weg.

De identificatie van de camera’s rondom dienstgebouwen bestaat uit de identificatie van de tunnel (optioneel, zie Bijlage A), de identificatie van het dienstgebouw en (zie *Tabel 3*) en het identificatienummer van de camera (zie Hoofdstuk 5). Bijvoorbeeld DN 01 of MDT DZ 04.

De locatie van de camera rondom de dienstgebouwen betreft de toegang waarvan de camera primair beeld geeft. Bijvoorbeeld “Entree”, “Hek”, “Parkeer”, “Trap”.

[2] De verzameling van dwarsverbindingen tussen twee buizen wordt als één veilige ruimte aangemerkt.

8.4 Voorbeelden

Voorbeelden van de naamgeving en codering van installaties en bouwdelen in de tunnelapplicatie.

Systemen en Detecties	Identificatie	Codering
Tabblad	Verkeersbuis	Li
Buis		
Ventilatie	Verkeersbuis	Li
Ventilatiecluster	Identificatie lengterichting	1
Ventilator	Identificatie lengte- en dwarsrichting	1.1
CCTV		
CCTV	Verkeersbuis	
Camera	Identificatie lengterichting + weglocatie	01 – A9 Li 52,17
Tunnel		
Vloeistofafvoer		
Vloeistofpompinstallatie	Dienstgebouw of Vloeistofkelder	DN
Vloeistofpomp	Identificatie	1

Bijlage A. Rijkstunnels

Onderstaande tabel bevat de door Landelijk Tunnelbeheer (LTB) vastgestelde naamgeving en codering van alle rijkstunnels in Nederland. Hiermee wordt de civiele constructie van het kunstwerk aangeduid waarin de onderdelen van de tunnel technische installaties zijn gerealiseerd.

Tunnel	Codering
Beneluxtunnel	BET
Botlektunnel	BOT
Coentunnel	CNT
Corbulotunnel	RYT
Drechttunnel	DET
Gaasperdammertunnel	GDT
Eerste Heinenoordtunnel	EHT
Tweede Heinenoordtunnel	THT
Hollandtunnel	HOT
Ketheltunnel	KET
Koning Willem-Alexandertunnel	KWA
Leidsche Rijntunnel	LRT
Maasdeltatunnel	MDT
Noordtunnel	NOT
Sijtwendetunnel	SYT
Spoortunnel	ST1
Parktunnel	ST2
Vliettunnel	ST3
Roertunnel	ROE
Rottemerentunnel	RMT
Salland Twentetunnel	STT
Schipholtunnel	SHT
Swalmen tunnel	SWA
Thomassentunnel	THO
Velsertunnel	VST
Vlaketunnel	VLK
Wijkertunnel	WKT
Zeeburgertunnel	ZBT
Zuidasdoktunnel	ZAD

Bijlage B. Generieke decompositie

B.1. Decompositie tunnel technische installaties

Onderstaande tabel bevat de door Landelijk Tunnelbeheer vastgestelde generieke decompositie van de tunnel technische installaties met de naamgeving en codering volgens de SATO en NEN2767.

SATO -Nr	SATO Installaties (per categorie)	NEN-Nr	NEN Elementen
00	Algemeen		
01	Werkplek wegverkeersleider		
02	Werkplek tunnelbeheer		
03	Werkplek onderhoud		
04	Opleidings- en trainingssysteem		
05	Algemeen technisch en administratief		
10	Energievoorziening		
11	Netaansluiting		
12	Aarding, bliksem- en overspanningsbeveiliging	105	Aarding- en bliksembeveiligingsinstallatie
13	Laagspanningsinstallatie	162	Laagspanningsinstallatie
14	Noodstroominstallatie (roterend)	171	Noodstroominstallatie (roterend)
15	Noodstroominstallatie (statisch)	172	Noodstroominstallatie (statisch)
16	Hoogspanningsinstallatie	149	Hoogspanningsinstallatie
17	Duurzame energiebron	129	Duurzame energiebron
20	Verlichting		
21	Openbare verlichting (verkeersbuis)	179	Openbare verlichting (OV)
22	Verlichting Veilige Ruimte	115	Binnenverlichting
23	Openbare verlichting (OV)	179	Openbare verlichting (OV)
26	Verlichting Dienstgang	115	Binnenverlichting
30	Vloeistofpompinstallatie		
31	Hoofdpompinstallatie	186	Pompinstallatie
32	Middenpompinstallatie	186	Pompinstallatie
33	Hellingpompinstallatie	186	Pompinstallatie
34	Lenspompinstallatie	186	Pompinstallatie
35	Ventilatiesystemen		
36	Ventilatie-installatie Tunnel	213	Ventilatie-installatie
37	Meetinstallatie Luchtkwaliteit	374	Meetinstallatie
38	Overdrukinstallatie Grensruimte	182	Over- en onderdrukinstallatie
39	Overdrukinstallatie Veilige Ruimte	182	Over- en onderdrukinstallatie
40	Verkeersinstallaties		
41	Wegkantsysteem (WKS)	169	Wegkantsysteem (WKS)
42	Verkeersdetectie-installatie	226	Verkeersdetectie-installatie
43	Hoogtedetectie-installatie	150	Hoogtedetectie-installatie
44	Afsluitboominstallatie	107	Afsluitboominstallatie
45	Verkeersregelinstallatie (VRI)	227	Verkeersregelinstallatie (VRI)
46	Verplaatsbare Vangrail installatie (VEVA)	229	Verplaatsbare Vangrail installatie (VEVA)
49	Calamiteiten Doorsteek installatie (CADO)	121	Calamiteiten Doorsteek installatie (CADO)

50	Brandblusinstallaties		
51	Brandblusinstallatie	119	Brandblusinstallatie
53	Hulppost installatie	119	Brandblusinstallatie
60	Communicatie		
61	CCTV	122	Closed Circuit TeleVision installatie (CCTV)
62	Hoog Frequent installatie (HF en C2000)	145	Hoog Frequent installatie (HF)
63	Omroepinstallatie	175	Omroepinstallatie
64	Intercominstallatie (noodtelefooninstallatie)	153	Intercominstallatie
65	Telefooninstallatie	206	Telefooninstallatie
70	Gebouwinstallaties		
71	Klimaatinstallatie	337	Klimaatinstallatie
72	Inbraakbeveiligingsinstallatie	250	Inbraakbeveiligingsinstallatie
74	Brandmeld- en ontruimingsinstallatie (BMI)	120	Brandmeld- en ontruimingsinstallatie (BMI)
75	Brandblusinstallatie	119	Brandblusinstallatie
76	Waarschuwings- en alarmeringssysteem (WAS)	372	Waarschuwings- en alarmeringssysteem (WAS)
77	Verlichting Dienstgebouw	115	Binnenverlichting
79	Toegangscontrole-installatie	400	Toegangscontrole-installatie
80	Besturingsinstallaties		
81	Bedieningsinstallatie	112	Bedienings- en besturingsinstallatie
82	Besturingsinstallatie (coördinerend)	112	Bedienings- en besturingsinstallatie
83	Noodbedieningsinstallatie	112	Bedienings- en besturingsinstallatie
84	Hulpdienstpaneel Verkeersbuis	112	Bedienings- en besturingsinstallatie
86	Transmissie netwerk	124	Transmissie-installatie
87	Externe koppeling	112	Bedienings- en besturingsinstallatie
88	Plaatselijke bediening installatie	112	Bedienings- en besturingsinstallatie
89	Installatie derden		
90	Diverse installaties		
91	Vluchtdeur	232	Vluchtweginstallatie
92	Kabeldraagconstructie	156	Kabeldraagconstructie
94	Dynamische Vluchtroute Indicatie Veilige Ruimte	130	Dynamische bewegwijzering en informatie systemen
95	Kabels en Leidingen	113	Kabel
96	Vluchtdeurindicatie Verkeersbuis	232	Vluchtweginstallatie
97	Pictogrammen en bebording	111	Bebording en bewegwijzering (statisch)
98	Installaties derden		

B.2. Decompositie civiele constructie

Onderstaande tabel bevat de door Landelijk Tunnelbeheer vastgestelde generieke decompositie van de civiele constructie van de tunnel met de naamgeving en codering volgens de SATO en NEN2767.

SATO-Nr	SATO Installaties (per categorie)	NEN-Nr	NEN Elementen
100	Tunnelbuis-Civiel		
101	Fundering	133	Fundering
102	Wandconstructie	388	Wandconstructie
103	Dakconstructie	391	Dakconstructie
104	Hoofddraagconstructie	147	Hoofddraagconstructie
105	Voegovergang	233	Voegovergang
106	Verharding	219	Verharding wegtype 1 (hoofdwegennet)
107	Vloerconstructie (MTK)	389	Vloerconstructie
108	Pompkelder	187	Pompkelder
109	Hemelwaterafvoer	144	Hemelwaterafvoer (HWA)
110	Geleideconstructie	136	Geleideconstructie
111	Wegmarkering	238	Wegmarkering
112	Hittewerende voorziening	212	Tunnelbuis
200	Toeritten-Civiel		
201	Fundering	133	Fundering
202	Wandconstructie	388	Wandconstructie
203	Kerende constructie	157	Kerende constructie
204	Folieconstructie	132	Folieconstructie
205	Voegovergang	233	Voegovergang
206	Verharding	219	Verharding wegtype 1 (hoofdwegennet)
207	Lichtroosterconstructie	212	Tunnelbuis
208	Geluidbeperkende constructie	137	Geluidbeperkende constructie
209	Verkeerskundige draagconstructie	188	Portaal
210	Geleideconstructie	136	Geleideconstructie
211	Wegmarkering	238	Wegmarkering
212	Talud	272	Talud
213	Leuningconstructie	414	Leuningconstructie
214	Hemelwaterafvoer	144	Hemelwaterafvoer (HWA)
215	Drainage	127	Drainage
216	Groen (incl. watergang en kanteldijken)	114	Berm
217	Bebording en bewegwijzering (statisch)	111	Bebording en bewegwijzering (statisch)
218	Hittewerende voorziening	212	Tunnelbuis
300	Dienstgebouwen-Civiel		
301	Vluchtweginstallatie	232	Vluchtweginstallatie

302	Sanitaire installatie	394	Sanitaire installatie
303	Dakconstructie	391	Dakconstructie
304	Vloerconstructie	389	Vloerconstructie
305	Hijs- en hefinstallatie	146	Hijs- en hefinstallatie
306	Binnen-, buitendeur en rolluik	181	Opstal
307	Brandcompartimentering en rookscheiding		
308	Branddoorvoering		
309	Zonweringsinstallatie	401	Zonweringsinstallatie
310	Interieur	181	Opstal
311	Trapconstructie	390	Trapconstructie
312	Watertapinstallatie	395	Watertapinstallatie
314	Wandconstructie		
400	Terrein		
401	Verlichting Terrein	173	Objectverlichting
402	Verharding	222	Verharding wegtype 4 (licht belast)
403	Wegmarkering	238	Wegmarkering
404	Terrein Riolering	358	Inlaatvoorziening
405	Hekwerk en terreinafscheiding	306	Afscheiding
406	Rolhek en looppoort	209	Toegangshek
407	Laadpaal elektrische voertuig		
408	Voorzieningen hulpdienst		
409	Peilbuis	374	Meetinstallatie

Bijlage C. Tunnel technische installaties

Onderstaande tabel bevat de standaard naamgeving van de tunnel technische installaties zoals deze dienen te worden toegepast in de tunnelapplicatie en beheer management systemen.
De codering komt overeen met het SATO nummer van de installatie in Bijlage B.

Installatie (per categorie)	Codering	Naam
Energievoorziening		
Netaansluiting	11	Netaansluiting
Aarding, bliksem- en overspanningsbeveiliging	12	Aarding en overspanningsbeveiliging
Laagspanningsinstallatie	13	Laagspanningsinstallaties
Noodstroominstallatie (roterend)	14	Noodstroom
Noodstroominstallatie (statisch)	15	No-Break
Hoogspanningsinstallatie	16	Hoogspanningsinstallatie
Verlichting		
Openbare verlichting (verkeersbuis)	21	Verlichting verkeersbuis
Verlichting Veilige Ruimte	22	Verlichting veilige ruimte
Openbare verlichting (OV)	23	Verlichting openbaar
Verlichting Dienstgang	26	Verlichting dienstgang
Vloeistofpompinstallatie		
Hoofdpompinstallatie	31	Vloeistofafvoer
Middenpompinstallatie	32	Vloeistofafvoer
Hellingpompinstallatie	33	Vloeistofafvoer
Lenspompinstallatie	34	Vloeistofafvoer
Ventilatiesystemen		
Ventilatie installatie	36	Ventilatie
Meetinstallatie Luchtkwaliteit	37	Luchtkwaliteit
Overdrukinstallatie Grensruimte	38	Overdruk GR
Overdrukinstallatie Veilige Ruimte	39	Overdruk
Verkeersinstallaties		
Wegkantsysteem (WKS)	41	MTM-koppeling
Verkeersdetectie-installatie	42	SOS
Hoogtedetectie-installatie	43	Hoogtedetectie
Afsluitboominstallatie	44	Afsluitbomen
Verkeersregelinstallatie (VRI)	45	Verkeerslichten
Verplaatsbare Vangrail installatie (VEVA)	46	VEVA
Calamiteiten Doorsteek installatie (CADO)	49	CADO
Brandblusinstallaties		
Brandblusinstallatie	51	Blusvoorziening

Hulppost installatie	53	Hulpposten
Communicatie		
CCTV	61	CCTV
Hoog Frequent (HF en C2000)	62	HF / C2000
Omroepinstallatie	63	Omroep
Intercom/Noodtelefooninstallatie	64	Noodtelefoon
Telefooninstallatie	65	Telefoon
Gebouwinstallaties		
Klimaatinstallatie	71	Klimaatregeling
Inbraakbeveiligingsinstallatie	72	Inbraakalarm
Brandmeld- en Ontruimingsinstallatie	74	Brandmeld
Brandblusinstallatie	75	Blusvoorziening
Waarschuwings- en alarmeringssysteem	76	Waarschuwing
Verlichting dienstgebouw	77	Verlichting
Toegangscontrole installatie	79	Toegangscontrole
Besturingsinstallaties		
Bedieningsinstallatie	81	Bediening
Besturingsinstallatie (coördinerend)	82	Besturing
Noodbedieningsinstallatie	83	Noodbediening
Hulpdienstpaneel verkeersbuis	84	Hulpdienstpaneel
Transmissienetwerk	86	Transmissie
Externe koppelingen	87	Externe koppelingen
Plaatselijke bediening installatie	88	Plaatselijke bediening
Diverse installaties		
Vluchtdeuren	91	Vluchtdeuren
Kabeldraagconstructie	92	Kabeldraagconstructie
Dynamische Vluchtroute Indicatie	94	Vluchtroute
Kabels en Leidingen	95	Kabels
Vluchtdeurindicatie verkeersbuis	96	Indicatie
Pictogrammen en bebording	97	Pictogrammen
Installaties derden	98	

Bijlage D. Onderdelen van de tunnel technische installaties

Onderstaande tabel bevat de naamgeving en codering van de onderdelen van de tunnel technische installaties op het niveau van bouwdelen die worden toegepast in het RWS Tunnelsysteem.

Naam	Codering
A	
Afsluitboom	ASB
Antenne	ANT
Aarding en overspanning (gegroepeerd)	
Aardlekschakelaar	ALS
Aardingspunt	APU
Aardrail	ARA
Overspanningsbeveiliging	OSB
B	
Blusvoorziening (gegroepeerd)	
Bluswaterreservoir	BVR
Bluswaterdistributieleiding	BVD
Bluswatersuppletieleiding	BVL
Brandbluspomp	BVP
Jockeypomp	BVJ
Slanghaspel	BVS
Handblusser	BVH
Storz-koppeling	BVK
Brandmelding (gegroepeerd)	
Brandmeldcentrale	BMC
Brandmeldindicator (visueel/akoestisch)	BMI
Brandmeldpaneel (bij ingang dienstgebouw)	BMP
Brandmeldalarm slow whoop (akoestisch)	BMS
Brandmeldalarm nevenindicator (visueel)	BMN
Brandmelder automatisch (optisch/ionisatie)	BMA
Brandmelder hand	BMH
C	
Calamiteiten Doorsteek	CAD
CCTV (gegroepeerd)	
Camera	CAM
Decoder	DEC
Encoder	ENC
Video-opslag	VOS
D	
Detectielus	DLU

E	
Energie (gegroepeerd)	
Brandstofpomp	EBP
Brandstoftank	EBT
Distributienetwerk	EDN
Hoogspanningsverdeler	EHV
Laagspanningsverdeler	ELV
Netaansluiting	ENA
NoBreak	ENB
Noodstroom	ENS
Transformator	ETR
F	
G	
H	
Hoogtedetectie Adviesfase	HDA
Hoogtedetectie Waarschuwingsfase	HDW
Hoogtedetectie Roodfase	HDR
Hulpdienstpaneel	HDP
Hulppost (type A)	HPA
Hulppost (type C)	HPC
Hulppost Pictogram	HPP
I	
Inbraakcentrale	IBC
Intercomtoestel	ICT
J	
K	
Kasten (gegroepeerd)	
Aansluitkast	AKA
Klemmenkast	KLK
Klimaatregelkast	KRK
Laskast	LKA
Luskoppelkast	LKK
Modulaire aansluitkast	MAK
Overdrukkast	ODK
Overgangskast	OGK
Patchkast	PAK
Routerkast	RTK
Sterpuntkast	SPK
Systeemkast	SKA

Verkeerskast	VKK
Voedingskast	LSK
Kleppen / afsluiters (gegroepeerd)	
Afsluiter of klep handbediend	AFH
Afsluiter of klep motor bediend	AFM
Brandklep	BKL
Elektrisch bediend klep	EKL
Luchtklep	LKL
Luchtklep regelbaar	LKR
Magneetklep Motor(bediende) afsluiter	MKL
Ontluchtklep	OKL
Terugslagklep	TSK
Veiligheidsklep	VHK
L	
Luidspreker	LSP
M	
N	
Nood Bedienpaneel	NBP
Noodtelefoontoestel	NTT
O	
P	
Plaatselijk Bedienpaneel	PBP
Q	
R	
S	
Sensoren / Meters (gegroepeerd)	
Deurcontact (open/dicht)	DCO
Deurkleefmagneet	DKM
Deurstandsignalering (open/dicht)	DSS
Drukmeter	DME
Drukverschilmeter	DVM
Lichtmeter	LME
Luchtkwaliteitsmeter	LKM
Meetmicrofoon	MMF
Niveaumeter	NME
Quantity meter	QME
Stroommeter	SME
Temperatuurmeter	TME
Tracing controlunit	TRU

Trilling meter	TSE
Vlotter hooghoogwater	VHH
Vlotter laaghoogwater	VLH
Vlotter maximaal startwater	VMS
Vlotter laaglaagwater	VLL
Voltmeter	VME
Zichtmeter	ZME
T	
U	
V	
Verkeerslicht	VKL
Verkeerslichten voorwaarschuwing	J32
Ventilatie (gegroepeerd)	
Ventilator Verkeersbuis	VVB
Ventilator Overdruk Veilige Ruimte	VVR
Ventilator Overdruk Grensruimte	VGR
Verlichting (gegroepeerd)	
Armatuur	ARM
Basisverlichtingsarmatuur	BVA
Driverbox	DRB
Ingangsverlichtingsarmatuur	IVA
Master Control Unit	MCU
Noodverlichtingsarmatuur	NVA
Oriëntatieverlichting	OVE
Uitgangsverlichtingsarmatuur	UVA
Vloeistofafvoer (gegroepeerd)	
Pomp	VAP
Afvoerleiding	VAL
Vluchtdeuren (gegroepeerd)	
Aanstraalverlichting	VDA
Aanvalsdeur	VDB
Contourverlichting	VDC
Einddeur	VDE
Geluidsbaken	VDG
Kopdeur	VDK
Pictogram	VDP
Vluchtdeur verkeersbuis	VDV
Vluchtroute (gegroepeerd)	
Vluchtroute indicator (dynamisch)	VRI

Vluchtroute pictogram	VRP
W	
Waarschuwingsinstallatie	WIS
Wandcontactdoos	WCD
Werkschakelaar	WSC
X	
Y	
Z	

Bijlage V J-STD-016

Rijkswaterstaat
Ministerie van Infrastructuur en Waterstaat

Bijlage J-STD-016

Bijlage bij Vraagspecificatie Proces

D&C Vervanging Verlichting Schipholtunnel
Zaaknummer: 31212908

J-STD-016-1995
30 September 1995

Trial-Use Standard Standard for Information Technology Software Life Cycle Processes Software Development Acquirer-Supplier Agreement

Keywords: Builds/incremental development, Database, Joint Technical/management reviews, Operational concept, Reusable software, Risk management, Security/privacy protection, Software, Software configuration management, Software development, Software documentation, Software implementation, Software management indicators, Software product evaluation, Software quality assurance, Software requirements definition, Software safety, Software maintenance, Software testing, Software unit, Tailoring.

Prepared by a Joint IEEE / EIA Working Group

This is a joint IEEE/EIA Standards Project, subject to change. Permission is hereby granted for IEEE/EIA Standards Committee participants to reproduce this document for purposes of IEEE/EIA standardization activities, including balloting and coordination. If this document is to be submitted to ISO or IEC, notification shall be given to the IEEE/EIA. Permission is also granted for member bodies and technical committees of ISO and IEC to reproduce this document for the purpose of developing an international position. Other entities seeking permission to reproduce portions of this document for these and other uses must contact the IEEE or EIA.

Institute of Electrical and Electronic Engineers, Inc. 345 East 47th Street New York, NY 10017, USA

Electronic Industries Association 2600 Wilson Blvd. Arlington, VA 22201-3834

PDF: ISBN 0-7381-0427-2, SS94377
Print: SH94377

NOTICE

EIA and IEEE Engineering Standards and Publications are designed to serve the public interest through eliminating misunderstandings between manufacturers and purchasers, facilitating interchangeability and improvement of products, and assisting the purchaser in selecting and obtaining with minimum delay the proper product for his particular need. Use of such Standards and Publications is wholly voluntary. Existence of such Standards and Publications shall not in any respect preclude any member or nonmember of EIA and IEEE from manufacturing or selling products not conforming to such Standards and Publications, nor shall the existence of such Standards and Publications preclude their voluntary use by those other than EIA and IEEE members, whether the standard is to be used either domestically or internationally.

Standards and Publications are approved by EIA and IEEE in accordance with the American National Standards Institute (ANSI) patent policy. By such action, EIA and IEEE do not assume any liability to any patent owner, nor do they assume any obligation whatever to parties adopting the Standard or Publication.

Note: Attention is called to the possibility that implementation of this standard may require use of subject matter covered by patent rights. By publication of this standard, no position is taken with respect to the existence or validity of any patent rights in connection therewith. EIA and IEEE shall not be responsible for identifying all patents for which a license may be required by an EIA and IEEE standard or for conducting inquiries into the legal validity or scope of those patents that are brought to its attention.

INTERIM (TRIAL-USE) STANDARDS

This EIA/IEEE Interim (Trial-Use) Standard is based upon the major technical content of ISO/IEC 12207 Information Technology Software Life Cycle Process, 22 February 1995, for the software development process. It conforms in all essential respects with this process of the ISO/IEC Standard.

EIA/IEEE Interim (Trial-Use) Standards contain information deemed to be of technical value to the industry, and are published at the request of the originating Committee without necessarily following the rigorous public review and resolution of comments which is a procedural part of the development of an EIA/IEEE Standard.

EIA Interim Standards should be reviewed on an annual basis by the formulating Committee and a decision made on whether to proceed to develop an EIA/IEEE Standard on this subject. EIA Interim Standards must be cancelled by the Committee and removed from the EIA Standards Catalog before the end of their fifth year of existence. In accordance with IEEE policy, trial-use standards are effective for 24 months from the date of publication. Comments for revision will be accepted for 18 months after publication. It is expected that following the 24-month period, this trial-use standard, revised as necessary, shall be submitted to the IEEE Standards Board for approval as a full-use standard.

(This Interim (Trial-Use) Standard was developed by the Joint EIA/IEEE Working Group on Software Development. Members of the Joint Committee serve voluntarily and without compensation. They are not necessarily members of EIA or IEEE.

Comments on standards and requests for interpretation should be addressed to:

Vice President, Standards and Technology
Electronic Industries Association
2500 Wilson Boulevard
Arlington, Virginia 22201-3834
Published by
©ELECTRONIC INDUSTRIES ASSOCIATION 1996
Engineering Department
2500 Wilson Boulevard
Arlington, Virginia 22201
PRICE: Please refer to the current
Catalog of EIA, JEDEC, and TIA STANDARDS and ENGINEERING PUBLICATIONS
or call Global Engineering Documents, USA and Canada (1-800-854-7179)
International (303-397-7956)
All rights reserved
Printed in U.S.A.

CAUTION—PLEASE!

DON'T VIOLATETHELAW!

This document is copyrighted by the EIA and may not be reproduced without permission.

Organizations may obtain permission to reproduce a limited number of copies through entering into a license agreement. For information, contact:

Global Engineering Documents15 Inverness Way EastEnglewood, CO 80112-5704 or callU.S.A. and Canada 1-800-854-7179, International (303) 397-7956

Foreword

1. This standard defines a set of software development activities and resulting software products. It provides a framework for software development planning and engineering.

2. This standard is written in contractual language. This choice is based on the fact that it is easier for non-contractual users to adapt contractual language to their use than for contractual users to apply non-contractual language.

3. This standard is the first step in the implementation of ISO/IEC 12207, Software Life Cycle Processes. Future versions are intended to implement additional software life cycle processes and supplier roles, such as the operator and maintainer. Those activities of the maintainer that are the same as those of a developer are covered in this version of the standard. For purposes of this implementation, the "supplier" of ISO/IEC 12207 is always the "developer," and the term "developer" is used throughout this standard.

4. This standard is meant to be tailored to ensure that only necessary and cost-effective requirements are applied. It is not intended to specify or discourage the use of any particular software development method. The developer is responsible for selecting software development methods that support the achievement of contract requirements.

5. This standard emphasizes that information resulting from the activities required by this standard is intrinsic to the software development process, to be recorded regardless of whether a deliverable is required. When information is not required to be delivered, the software products cited in this standard are to be used as checklists of items to be covered, as applicable, in the planning and engineering activities for the project.

6. This standard allows information to be recorded in representations other than traditional documents (for example, computer-aided software engineering (CASE) tools) and provides relaxed requirements for the format and structure of that information for such representations.

Introduction

J-STD-016-1995 is a standard for the software development process. It is applicable throughout the system life cycle. It establishes uniform requirements for acquiring, developing, modifying, and documenting software. It defines standard terminology and establishes activities, tasks, and products for a software development or maintenance project. It can be applied to any type of software, including application software, operating system software, the software portion of firmware, reusable software, and software employed to develop deliverable software.

The activities in the standard form a comprehensive set, sufficient for a large, complex project. The standard is meant to be tailored as needed for each project by specifying in the contract which provisions of the standard apply.

The standard is intended to be responsive to the rapidly evolving software discipline. It is independent of any particular methodology, ensuring the acquirer's right to specify the product and the developer's right to be technologically creative and innovative. In particular:

- The activities and tasks in the standard tell what to do, not how to do it. For example, the standard requires the developer to perform architectural design, but does not require use of the object-oriented design method.
- The standard does not specify or encourage any software life cycle model (waterfall, incremental, evolutionary, spiral, etc.). Instead, the standard provides the building blocks needed to create a life-cycle model for a software project.
- The standard does not specify or depend on any design or programming language. It is meant to be applicable regardless of the language used.
- The standard provides flexibility regarding documentation:
  - A distinction is made between the task of generating and recording planning or engineering information and the task of generating a deliverable containing that information.
  - Information and deliverables can be in hardcopy form (using contractor or software product format) or in computer-aided software engineering (CASE) tools.
- The standard does not emphasize any particular software quality factor, such as reliability, maintainability, or reusability. This choice is left to each project.
- The standard can be used within an organization or contractually between two parties.
- The standard provides a performance-based distinction between requirements for a product and design of a product. A requirement is a characteristic that a system or software item is required to possess in order to be acceptable to the acquirer while design is a characteristic that the acquirer is willing to leave up to the developer. This emphasis on required performance can allow a developer to provide quality products at reduced costs when unique product solutions are not required.

J-STD-016-1995 specifically removes key problems found in the use of predecessor standards. J-STD-016-1995:

a) **ls usable with any development strategy** . J-STD-016-1995 has been structured to better accommodate incremental, evolutionary, and other development models than the traditional "waterfall" model. It is structured to avoid time-oriented dependencies and implications, provides alternatives to formal reviews (that can force a waterfall development model), and explains how to apply the standard across multiple builds or iterations.

b) **Is usable with any development methods** . To improve compatibility with object-oriented and other methods not using functional decomposition, J-STD-016-1995 allows the developer to define in the software development plan the design and implementation structures to be used, and to use that structure in the documentation.

c) **Is compatible with CASE tools** . J-STD-016-1995 recognizes that much of the significant work on a software development project does not involve writing documents. The standard: 1) separates planning and engineering activities from preparation of deliverables to make it easier to call for one without the other; 2) provides language that permits the recording of project information in forms other than traditional documents, such as CASE tools; 3) acknowledges data in CASE tools as a substitute for traditional documents; and 4) provides guidance to prevent unnecessary deliverables.

d) **Provides requirements for software reuse** . J-STD-016-1995 recognizes that many projects incorporate or are based on reusable software. To provide clearer requirements when this is the case, the standard: 1) identifies criteria for use in evaluating reusable software, and 2) provides guidance on interpreting J-STD-016-1995's activities and deliverables when applied to reusable software.

e) **Supports the use of software management indicators** . J-STD-016-1995 supports the use of software management indicators. It has incorporated a requirement to identify and apply such indicators, and included an annex of candidate indicators that might be used.

f) **Emphasizes software supportability** . J-STD-016-1995 has enhanced software supportability requirements. Examples are requirements to: 1) record the rationale for key decisions made on the project; 2) identify all resources the maintenance organization will need to maintain the software, and 3) demonstrate that those resources are sufficient to maintain the software.

g) **Provides a role for software in the system** . J-STD-016-1995 recognizes that software exists in the context of a system. It provides a role for the software developer both in the case of a hardware-software system and where the software (possibly with the computers on which it will run) is considered to constitute the system.

Participants

At the time this trial use standard was completed, the Joint Industry Working Group on Software Development had the following membership:

Perry DeWeese, ***(EIA Co-Chair)***
Raghu Singh, ***(IEEE Co-Chair)***

Stuart Campbell
John Chihorek
Richard Evans
Lewis GrayLewis Gray
Robert Hegland
Jim Heil
Helmut Hummel
Tim Janes
Capt Jonathan Liles
Marv Lubofsky
David Maibor
James Moore
Myrna Olson
Al Peschel
Alex Polack
Norma Stopyra
Leonard Tripp

Other individuals who have contributed review and comments are the following:

Dennis Ahern
Mordechai Ben-Menachim
Dave Benson
Ron Berlack
William J. Boll
John Bowers
Don Calvert
Andrew Campbell
Jaya R. Carl
Theo Clarke
Jack Cooper
Paul Cooley
Rita Costello
Kenneth Costello
Geoff Cozens
Gregory Daich
Neil Davis
Chris Denham
Bostjan K. Derganc
Dave Dikel
Treasure Diehl
Peter Eirich
Bob Elston
SueEllen Eslinger
Eva Freund
William Gess
Gregg Glesler
Lawrence Gunther
Ranwa Haddad
John Hamlin
Nancy Hannon
John Harauz
Robert Harley
Rick Hefner
Carl Hirshfield
John Horch
Stephen Huffman
George Jackelen
Allan Jaworski
Diana Kang
Ron Kenett
Judy Kerner
John Kerr
Larry Klos
Rick Kreke
Dorothy Kuckuck
Jerome Lake
Dennis Lawrence
Jim Longbucco
Joan Lovelace
Stan Magee
John Marshall
Judy McCloskey
P. D. McCray
Jack McGarry
Archibald McKinley
Celia Modell
Dennis Nickle
Bart Nigro
James Orr
Gerald L. Ourada
Mark Paulk
Sherry Paquin
John G. Phippen
Peter Poon
Lawrence Przybylski
Ken Ptack
Jane Radatz
Larry Reed
Dennis Rilling
Keith Shewbridge
Katsutoshi Shintani
Carl A. Singer
Melford E. Smyre
Don Sova
Richard Storch
Richard Summers
David J. Szymanski
Booker T. Thomas
Patricia Trellue
Ann Turner
Dennis Turner
Theodore Urbanowicz
Howard Vern
Delores Wallace
Steven Wang
Scott Whitmire
Charles Wilson
Audrey Winston
Paul Wolfgang
Paul Work
Grady Wright
Gene Yancy
Natalie Yopconka
Geraldine Zimmerman
Peter Zoll

CONTENTS

1. Scope 1
1.1 Purpose 1
1.2 Application 1
2. Referenced documents 4
3. Definitions 4
3.1. Terms 4
4. General requirements 8
4.1 Software development process 8
4.2 General requirements for software development 8
5. Detailed requirements 10
5.1 Project planning and oversight 10
5.2 Establishing a software development environment 13
5.3 System requirements definition 14
5.4 System design 15
5.5 Software requirements definition 15
5.6 Software design 15
5.7 Software implementation and unit testing 16
5.8 Unit integration and testing 17
5.9 Software item qualification testing 18
5.10 Software/hardware item integration and testing 19
5.11 System qualification testing 20
5.12 Preparing for software use 21
5.13 Preparing for software transition 22
5.14 Software configuration management 24
5.15 Software product evaluation 25
5.16 Software quality assurance 25
5.17 Corrective action 26
5.18 Joint technical and management reviews 26
5.19 Risk management 27
5.20 Software management indicators 27
5.21 Administrative security and privacy protection 28
5.22 Managing subcontractors 28
5.23 Interfacing with software IV&V agents 28
5.24 Coordinating with associate developers 28
5.25 Project process improvement 28
6. Notes 28
6.1 Cross reference of standard subclauses to annex subclauses 28
6.2 Delivery of tool contents 29

Annex A (normative) Tailoring this standard for a project 30
A.1 Scope 30
A.2 Tailoring process 30
A.3 Identifying the project environment 30
A.4 Soliciting input 30
A.5 Selecting processes, activities, and tasks 30
A.6 Specifying tailoring decisions 31

Annex B (informative)Guidance on development strategies, tailoring, and build planning 32
B.1 Scope 32
B.2 Candidate development strategies 32
B.3 Selecting an appropriate development strategy 33

B.4 Relationship of this standard to development strategies 33
B.5 Planning software builds and tailoring this standard..... 33

Annex C (informative) Guidance on ordering deliverables 41
C.1 Scope 41
C.2 Ordering deliverables 41
C.3 Scheduling deliverables..... 41
C.4 Format of deliverables..... 41
C.5 Tailoring the content requirements for deliverables 42

Annex D (informative) Interpreting this standard for incorporation of reusable software products 43
D.1 Scope..... 43
D.2 Evaluating reusable software products..... 43
D.3 Interpreting this standard's activities for reusable software products..... 43

Annex E (normative) Planning software product descriptions 46
E.1 Scope 46
E.2 Software products covered 46

Annex F (normative) Concept and requirements software product descriptions 63
F.1 Scope..... 63
F.2 Software products covered..... 63

Annex G (normative) Design software product descriptions..... 83
G.1 Scope..... 83
G.2 Software products covered..... 83

Annex H (normative) Qualification testing software product descriptions 100
H.1Scope..... 100
H.2 Contents of the Software Test Description (STD) 100

Annex I (normative) Maintenance software product descriptions..... 106
I.1 Scope..... 106
I.2 Software products covered 106

Annex J (normative) User/operator software product descriptions 115
J.1 Scope 115
J.2 Software products covered 115
Annex K (informative) Software product description format and structure 129
K.1 Scope..... 129
K.2 Software products covered..... 129
K.3 Format and structure for all software products 129
K.3.3 Title page or identifier..... 133
K.3.4 Table of contents and index 133
K.3.5 Page numbering/labeling..... 133
K.3.6 Response to tailoring instructions 133
K.3.7 Multiple clauses and their subordinates 133
K.3.8 Alternative presentation styles 133
K.3.9 Substitution of existing documents 133
K.3.10 Standard data descriptions..... 134
K.3.11 Applicability of required contents 134

Annex L (normative) Software product evaluations 135

L.1 Scope 135
L.2 Required evaluations 135
L.3 Criteria definitions 135

Annex M (normative) Category and priority classifications for problem reporting 142
M.1 Scope 142
M.2 Classification by category 142
M.3 Classification by priority 142

Annex N (informative) Candidate joint management reviews 144
N.1 Scope 144
N.2 Assumptions 144
N.3 Candidate reviews 144

Annex O (informative) Candidate management indicators 147
O.1 Scope 147
O.2 Candidate indicators 147

Annex P (informative) Questionnaire on use of this standard 148

Trial-Use Standard
Standard for Information Technology
Software Life Cycle Processes
Software Development
Acquirer-Supplier Agreement

1. Scope

1.1 Purpose

This standard establishes uniform requirements for software development activities and resulting software products. It is also intended to merge commercial and Government software development requirements within the framework of the software life cycle process requirements of the Electronic Industries Association (EIA), Institute of Electrical and Electronics Engineers (IEEE), and International Organization for Standardization (ISO). The term "software development" is used as an inclusive term encompassing new development, modification, reuse, reengineering, maintenance, and all other processes or activities resulting in software products.

1.2 Application

The requirements in this standard are intended for application to the development of systems that contain software (such as software embedded in hardware-software systems), to systems consisting of software alone, and to stand-alone software products. This standard is intended to be applied as follows.

1.2.1 Candidate uses

This standard can be:

a) Included or referenced in contracts or similar agreements, with the parties (called the acquirer and the developer) agreeing that the developer will perform software development in accordance with the standard
b) Adopted as an in-house standard by a project or organization that decides to perform software development in accordance with the standard
c) Used as the basis for an organization's software development process

1.2.2 Organizations and agreements

This standard can be applied to contractors, subcontractors, or in-house organizations performing software development. For uniformity, the term "acquirer" is used for the organization requiring the technical effort, "developer" for the organization performing the technical effort, "contract" for the agreement between these parties, "Statement of Work" (SOW) for the list of tasks to be performed by the developer, "subcontractor" for any organization tasked by the developer to perform part of the required effort, "user" for the persons or

organizations that will operate and/or use the software, and “maintenance organization” for the organization that will have responsibility for modifying and otherwise maintaining the software after transition from the development organization.

1.2.3 Contract-specific application

When this standard is invoked in a contract, it applies to each software product and to each type of software covered by the contract, regardless of storage medium, to the extent specified in the contract. Examples of types of software include deliverable versus non-deliverable, software designed to meet user needs versus software in the engineering and test environments, and software designed to meet one user need versus software designed to meet another. The acquirer is expected to specify the types of software to which the standard applies. Software installed in firmware is subject to all of the aforementioned provisions. This standard does not apply to the hardware element of firmware.

1.2.4 In-house application

When this standard is used to assist an organization in defining and establishing its software development process, it is intended for reference as a source of recommended software development activities and products on which to build specific organizational practices and procedures. When the standard is applied on an in-house development project, it is intended to be used as a source for selecting software development activities and products to satisfy specific project needs.

1.2.5 Tailoring

This standard is meant to be tailored for each type of software to which it is applied. The standard is to be tailored to the specific requirements of a particular program, program phase, or contractual structure. Tailoring takes the form of deletion of unnecessary requirements, alteration of requirements to more explicitly reflect the application to a particular effort, or addition of requirements as needed. Care is to be taken to eliminate tasks and data that add unnecessary costs or that do not add value to the activity or the product for the project. The tailoring requirements of this standard are normative (that is, binding) to be performed in accordance with this standard. Tailoring requirements, specified in annex A, are not subject to tailoring. All other requirements of this standard are considered tailorable. While final tailoring decisions are the responsibility of the acquirer, tailoring may be performed jointly with prospective or selected developers. Tailoring guidance can be found in annexes B and C.

1.2.6 Compliance

Compliance with this standard means “compliance with the standard as tailored for the project and recorded in the contract.”

NOTE—Regulatory and legal requirements are invoked separately through the contract.

1.2.6.1 Compliance with the “as tailored” standard

Compliance with the “as tailored”standard is defined as:

a) Performing the activities that resulted from tailoring this standard for a specific project as recorded in the contract
b) Recording applicable information resulting from the performance of the selected activities

1.2.6.2 Activity completion criteria

An activity is complete when all items constituting the activity, as specified in the contract, have been accomplished and applicable information has been recorded.

1.2.6.3 Compliance stipulation

Any entity (such as, person, company, Military Service, industrial association, organization) imposing this standard as a condition of trade is responsible for identifying and making public the minimum set of activities and resulting software products that is required to be fulfilled by a developer.

1.2.7 Interpretation of selected terms

The following terms have a special interpretation as used in this standard. These are not "definitions" of the terms, but clarifications of their use.

1.2.7.1 Interpretation of "system"

The following interpretations apply:

a) The term "system," as used in this standard, may mean: (1) a hardware-software system (for example, a radar system) for which this standard covers only the software portion, or (2) a software system (for example, a payroll system) for which this standard governs overall development.
b) If a system consists of subsystems, all requirements in this standard concerning systems apply to the subsystems as well. If a contract is based on alternatives to systems and subsystems, the requirements in this standard concerning the system and its specification apply to these alternatives and their specifications.

1.2.7.2 Interpretation of "participate" in system development

The term "participate" in subclauses regarding system-level activities is to be interpreted as follows: if the software covered by this standard is part of a hardware-software system, the term "participate" is to be interpreted as "take part in, as described in the Software Development Plan." If the software (possibly with its computers) is considered to constitute a system, the term "participate" is to be interpreted as "be responsible for." If the software in a hardware-software system is changed, but the hardware is not, the term "participate" may also be interpreted as "be responsible for."

1.2.7.3 Interpretation of "develop," "define," etc.

Throughout this standard, requirements to "develop," "define," "establish," or "identify" information are to be interpreted to include new development, modification, reuse, reengineering, maintenance, or any other activity or combination of activities resulting in software products.

1.2.7.4 Interpretation of "record"

Throughout this standard, requirements to "record" information are to be interpreted to mean "set down in a manner that can be retrieved and viewed." The result may take many forms, including, but not limited to, hand-written notes, hard-copy or electronic documents, and data recorded in computer-aided software engineering (CASE) and project management tools.

1.2.7.5 Interpretation of "applicable"

Throughout this standard, requirements to provide "applicable" information and perform "applicable" activities are to be interpreted to mean "provide the information and perform the activities that are natural by-products created by performing the activities required for the project in accordance with the tools, methods, and procedures described in the software development plan." The term "applicable" conveys the meaning that not all projects will generate the information or require the activity. "Applicability" is to be agreed upon jointly by the acquirer and developer.

2. Referenced documents

This standard shall be used in conjunction with the following publications.

FIPS PUB 39, Glossary for Computer Systems Security

IEEE Std 610.12-1990, IEEE Standard Glossary of Software Engineering Terminology/(ANSI)

3. Definitions

NOTE—In addition to the definitions and acronyms provided here, clause 1 describes this standard's interpretation or special usage of the following terms: acquirer, applicable, contract, define, develop, developer, establish, identify, participate, record, software development, Statement of Work, subcontractor, subsystem, maintenance organization, system, and user.

3.1. Terms

3.1.1 acceptance: An action by an authorized representative of the acquirer by which the acquirer assumes ownership of software products as partial or complete performance of a contract.

3.1.2 acquirer: An organization that procures software products for itself or another organization.

3.1.3 approval: Written notification by an authorized representative of the acquirer that a developer's plans, design, or other aspects of the project appear to be sound and can be used as the basis for further work. Such approval does not shift responsibility from the developer to meet contractual requirements.

3.1.4 architecture: The organizational structure of a system or a software item, identifying its components, their interfaces, and a concept of execution among them.

3.1.5 associate developer: An organization that is neither prime contractor nor subcontractor to the developer, but who has a development role on the same or related system or project.

3.1.6 behavioral design: The design of how an overall system or software item will behave, from a user's point of view, in meeting its requirements, ignoring the internal implementation of the system or software item. This design contrasts with architectural design, which identifies the internal components of the system or software item, and with the detailed design of those components.

3.1.7 build: (1) A version of software that meets a specified subset of the requirements that the completed software will meet. (2) The period of time during which such a version is developed.

> NOTE—The relationship of the terms "build" and "version" is up to the developer; for example, it may take several versions to reach a build, a build may be released in several parallel versions (such as to different sites), or the terms may be used as synonyms.

3.1.8 computer database: *See* : database.

3.1.9 computer hardware: Devices capable of accepting and storing computer data, executing a systematic sequence of operations on computer data, or producing control outputs. Such devices can perform substantial interpretation, computation, communication, control, or other logical functions.

3.1.10 computer program: A combination of computer instructions and data definitions that enable computer hardware to perform computational or control functions. (Source IEEE Std 610.12-1990).

3.1.11 computer software: *See:* software.

3.1.12 database: A collection of related data stored in one or more computerized files in a manner that can be accessed by users or computer programs via a database management system. (Adapted from IEEE Std 610.12-1990).

3.1.13 database management system: An integrated set of computer programs that provide the capabilities needed to establish, modify, make available, and maintain the integrity of a database.

3.1.14 deliverable software product: A software product that is required by the contract to be delivered to the acquirer or other designated recipient.

3.1.15 design: Those characteristics of a system or a software item that are selected by the developer in response to the requirements. Some will match the requirements; others will be elaborations of requirements, such as definitions of all error messages in response to a requirement to display error messages; others will be implementation related, such as decisions about what software units and logic to use to satisfy the requirements.

3.1.16 developer: An organization that develops software products ("develops" may include new development, modification, reuse, reengineering, maintenance, or any other activity that results in software products, and includes the testing, quality assurance, configuration management, and other activities applied to these products).

3.1.17 document/documentation: A collection of data, regardless of the medium on which it is recorded, that generally has permanence and can be read by humans or machines. (Adapted from IEEE Std 610.12-1990).

3.1.18 evaluation: The process of determining whether an item or activity meets specified criteria.

3.1.19 firmware: The combination of a hardware device and computer instructions and/or computer data that reside as read-only software on the hardware device. (Adapted from IEEE Std 610.12-1990).

3.1.20 hardware item: An aggregation of hardware that is designated for purposes of specification, testing, interfacing, configuration management, or other purposes.

3.1.21 independent verification and validation (IV&V): Systematic evaluation of software products and activities by an organization that is not responsible for developing the product or performing the activity being evaluated. IV&V is not within the scope of this standard.

3.1.22 interface: In software development, a relationship among two or more entities (such as software item - software item, software item - hardware item, software item - user, or software unit - software unit) in which the entities share, provide, or exchange data. An interface is not a software item, software unit, or other system component; it is a relationship among them.

3.1.23 joint review: A process or meeting involving representatives of both the acquirer and the developer, during which project status, software products, and/or project issues are examined and discussed.

3.1.24 maintenance (of software): *See:* software maintenance.

3.1.25 non-deliverable software product: A software product that is not required by the contract to be delivered to the acquirer or other designated recipient.

3.1.26 privacy protection: The establishment of appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of data records and to protect both security and confidenti-

ality against any anticipated threats or hazards that could result in substantial harm, embarrassment, inconvenience or unfairness to any individual about whom such information is maintained. (Source FIPS PUB 39)

3.1.27 process: An organized set of activities performed for a given purpose; for example, the software development process.

3.1.28 qualification testing: Testing performed to demonstrate to the acquirer that a software item or a system meets its specified requirements.

3.1.29 reengineering: The process of examining and altering an existing system to reconstitute it in a new form. May include reverse engineering (analyzing a system and producing a representation at a higher level of abstraction, such as design from code), restructuring (transforming a system from one representation to another at the same level of abstraction), redocumentation (analyzing a system and producing user or maintenance documentation), forward engineering (using software products derived from an existing system, together with new requirements, to produce a new system), retargeting (transforming a system to install it on a different target system), and translation (transforming source code from one language to another or from one version of a language to another).

3.1.30 requirement: (1) A characteristic that a system or a software item is required to possess in order to be acceptable to the acquirer. (2) A binding statement in this standard or another portion of the contract. Requirements are expressed using the word ”shall.“

3.1.31 reusable software product: A software product developed for one use but having other uses, or one developed specifically to be usable on multiple projects or in multiple roles on one project. Examples include, but are not limited to, commercial off-the-shelf software products, acquirer-furnished software products, software products in reuse libraries, and pre-existing developer software products. Each use may include all or part of the software product and may involve its modification. This term can be applied to any software product (for example, requirements, architectures, etc.), not just to software itself.

3.1.32 software: Computer programs and computer databases.

> NOTE—Although some definitions of software include documentation, this standard limits the definition to computer programs and computer databases.

3.1.33 software development: A set of activities that results in software products. Software development may include new development, modification, reuse, reengineering, maintenance, or any other activities that result in software products.

3.1.34 software development file (SDF): A repository for material pertinent to the development of a particular body of software. Contents typically include (either directly or by reference) considerations, rationale, and constraints related to requirements definition, design, and implementation; developer-internal test information; and schedule and status information.

3.1.35 software development library (SDL): A controlled collection of software, documentation, other intermediate and final software products, and associated tools and procedures used to facilitate the orderly development and subsequent maintenance of software.

3.1.36 software development process: An organized set of activities performed to translate user needs into software products.

3.1.37 software item: An aggregation of software, such as a computer program or database, that satisfies an end use function and is designated for purposes of specification, qualification testing, interfacing, configuration management, or other purposes. Software items are selected based on trade-offs among software func-

tion, size, host or target computers, developer, support strategy, plans for reuse, criticality, interface considerations, need to be separately documented and controlled, and other factors. A software item is made up of one or more software units.

3.1.38 software maintenance: The set of activities that takes place to ensure that software installed for operational use continues to perform as intended and fulfill its intended role in system operation. Software maintenance includes improvements, aid to users, and related activities.

3.1.39 software product: Software or associated information created, modified, or incorporated to satisfy a contract. Examples include plans, requirements, design, code, databases, test information, and manuals.

3.1.40 software quality: The ability of software to satisfy its specified requirements.

3.1.41 software system: A system consisting solely of software and possibly the computer equipment on which the software operates.

3.1.42 software transition: The set of activities that enables responsibility for software development to pass from one organization, usually the organization that performs initial software development, to another, usually the organization that will perform software maintenance.

3.1.43 software unit: An element in the design of a software item; for example, a major subdivision of a software item, a component of that subdivision, a class, object, module, function, routine, or database. Software units may occur at different levels of a hierarchy and may consist of other software units. Software units in the design may or may not have a one-to-one relationship with the code and data entities (routines, procedures, databases, data files, etc.) that implement them or with the computer files containing those entities.

3.1.44 transition (of software): *See:* software transition.

3.2 Abbreviations and acronyms

CASE Computer-Aided Software Engineering
COM Computer Operation Manual
CPM Computer Programming Manual
DBDD Database Design Description
FSM Firmware Support Manual
HW Hardware
IDD Interface Design Description
IRS Interface Requirements Specification
IV&V Independent Verification and Validation
OCD Operational Concept Description
SCOM Software Center Operator Manual
SDD Software Design Description
SDF Software Development File
SDL Software Development Library
SDP Software Development Plan
SIOM Software Input/Output Manual
SIP Software Installation Plan
SOW Statement of Work
SPS Software Product Specification
SRS Software Requirements Specification
SSDD System/Subsystem Design Description
SSS System/Subsystem Specification
STD Software Test Description
STP Software Test Plan

STR Software Test Report
STrP Software Transition Plan
SUM Software User Manual
SVD Software Version Description
SW Software

4. General requirements

4.1 Software development process

The developer shall establish a software development process consistent with contract requirements. The software development process shall include the following major activities, which may overlap, may be applied iteratively, may be applied differently to different elements of software, and need not be performed in the order listed below. The software process established may use or reference an organization's existing process for performing these activities. Annex B provides examples. The developer's software development process shall be described in the Software Development Plan.

a) Project planning and oversight (clause 5.1)
b) Establishing a software development environment (5.2)
c) System requirements definition (5.3)
d) System design (5.4)
e) Software requirements definition (5.5)
f) Software design (5.6)
g) Software implementation and unit testing (5.7)
h) Unit integration and testing (5.8)
i) Software item qualification testing (5.9)
j) Software/hardware item integration and testing (5.10)
k) System qualification testing (5.11)
l) Preparing for software use (5.12)
m) Preparing for software transition (5.13)
n) Integral processes:
    1) Software configuration management (5.14)
    2) Software product evaluation (5.15)
    3) Software quality assurance (5.16)
    4) Corrective action (5.17)
    5) Joint technical and management reviews (5.18)
    6) Risk management (5.19)
    7) Software management indicators (5.20)
    8) Administrative security and privacy protection (5.21)
    9) Managing subcontractors (5.22)
    10) Interfacing with software IV&V agents (5.23)
    11) Coordinating with associate developers (5.24)
    12) Project process improvement (5.25)

4.2 General requirements for software development

The developer shall meet the following general requirements in carrying out the detailed requirements in clause 5 of this standard.

4.2.1 Software development methods

The developer shall use systematic, documented methods for all software development activities. These methods shall be described in, or referenced from, the Software Development Plan.

4.2.2 Standards and practices for software products

The developer shall establish and apply standards and practices for representing requirements, design, code, test cases, test procedures, and test results. These standards and practices shall be described in, or referenced from, the Software Development Plan.

4.2.3 Traceability

The developer shall perform traceability between levels of requirements, between requirements and design, between design and the software that implements it, between requirements and qualification test information, and between computer hardware resource utilization requirements and measured computer hardware resource utilization. The result shall include all applicable traceability items of the System/Subsystem Specification (see F.2.2), Interface Requirements Specification (see F.2.3), Software Requirements Specification (see F.2.4), System/Subsystem Design Description (see G.2.1), Interface Design Description (see G.2.2), Database Design Description (see G.2.3), Software Design Description (see G.2.4), Software Test Plan (see E.2.2), Software Test Description (see H.2.1), and Software Product Specification (see I.2.1).

NOTE—The intent of this requirement is to trace both upward and downward to 1) ensure that all requirements are implemented and tested and 2) provide information for software maintenance.

4.2.4 Reusable software products

The developer shall identify and evaluate reusable software products (e.g., commercial off-the-shelf, acquirer-furnished, software products in reuse libraries, and pre-existing developer software products), that meet specified requirements and are cost-effective over the life of the system, for use in fulfilling the requirements of the contract. The scope of the search and the criteria to be used for evaluation and incorporation shall be as described in the Software Development Plan. Annex D provides candidate evaluation criteria and interprets this standard for incorporation of reusable software products.

NOTE—In addition, the developer may be required by the contract to develop software products specifically for reuse.

4.2.5 Assurance of safety, security, privacy protection, or other critical requirements

If a system relies on software to satisfy requirements deemed critical by the contract or by system specifications, the developer shall identify those software items or portions thereof whose failure could lead to violation of those critical requirements; develop a strategy, including both test and analyses, to assure that the requirements, design, implementation, and operating procedures for the identified software minimize or eliminate the potential for such violations; record the strategy in the Software Development Plan; implement the strategy; and produce evidence, as part of the required software products, that the assurance strategy hasbeen carried out. The developer shall identify by type, and develop strategies for, the following types of critical requirements:

a) Safety-critical: those software items or portions thereof whose failure could lead to a hazardous system state (one that could result in unintended death, injury, loss of property, or environmental harm)
b) Security-critical: those software items or portions thereof whose failure could lead to a breach of system security
c) Privacy protection-critical: those software items or portions thereof whose failure could lead to a breach of system privacy protection

NOTE—For purposes of this standard, privacy protection is concerned with preventing unauthorized disclosure of confidential data such as salary information; security is concerned with any accidental or malicious modification, destruction, or disclosure of computer software or computer data.

4.2.6 Computer hardware resource utilization.

The developer shall analyze contract requirements concerning computer hardware resource utilization (such as maximum allowable use of processor capacity, memory capacity, input/output device capacity, auxiliary storage device capacity, and communications/network equipment capacity). The developer shall allocate computer hardware resources among the software items, monitor the utilization of these resources for the duration specified in the contract, and reallocate or identify the need for additional resources as necessary to meet contract requirements.

4.2.7 Recording rationale

The developer shall record rationale that will be useful to the maintenance organization for key decisions made in specifying, designing, implementing, and testing the software. The rationale shall include trade-offs considered, analysis methods, and criteria used to make the decisions. The rationale shall be recorded in documents, code comments, or other media that will transition to the maintenance organization. The meaning of "key decisions" and the approach for providing the rationale shall be described in the Software Development Plan.

4.2.8 Access for acquirer review

The developer shall provide the acquirer or its authorized representative access to developer and subcontractor facilities, including the software engineering and test environments, for review of software products and activities required by the contract.

5. Detailed requirements

The order of the requirements in this clause is not intended to specify the order in which they are required to be carried out. Some activities may not apply to the project or the contracted effort. Many of the activities may be ongoing at one time; different software products may proceed at different paces; and activities specified in early subclauses may depend on input from activities in later subclauses. If the software is developed in multiple builds, some activities may be performed in every build, others may be performed only in selected builds, and activities and software products may not be complete until several or all builds are accomplished. Figure 1 provides an example of how each activity may be applied in one or more builds. Non-binding notes throughout clause 5 explain how to interpret each activity on a project involving multiple builds. A project involving a single build will accomplish all required activities in that build. Annex B provides guidance for planning builds, determining which activities apply to each build, and scheduling these activities.

5.1 Project planning and oversight

The developer shall perform project planning and oversight in accordance with the following requirements.

NOTE—If a system or software item is developed in multiple builds, planning for each build is interpreted to include: a) overall planning for the contract, b) detailed planning for the current build, and c) planning for future builds covered under the contract to a level of detail compatible with the information available.

5.1.1 Software development planning

The developer shall develop and record plans for conducting the activities required by this standard and by other software-related requirements in the contract. This planning shall be consistent with system-level planning and shall include all applicable items in the Software Development Plan (SDP) (see E.2.1).

NOTES:

1—The wording here and throughout this standard is designed to: 1) Emphasize that the development and recording of planning and engineering information is an intrinsic part of the software development process, to be performed regardless of whether a deliverable is required; 2) Use software products in annexes E through J as checklists of items to be covered in the planning and engineering activities; and 3) Permit representations other than traditional documents for recording the information (for example, computer-aided software engineering (CASE) tools).

2—If the contract specifies delivery of the information generated by this or any other subclause, the developer is required to format, assemble, mark, copy, and distribute the deliverable in accordance with the contract. This task is recognized to be separate from the task of generating and recording the required information and to require additional time and effort on the part of the developer. Annex K provides information on format and structure of deliverable information.

3—The Software Development Plan covers all activities required by this standard. Portions of the plan may be bound or maintained separately if this approach enhances the usability of the information. Examples include separate plans for software quality assurance and software configuration management.

4—The requirement to develop and record software development planning information may be satisfied by referencing an organization's existing practices and procedures that comply with the requirements of the contract.

Activity	Builds			
	Build 1	Build 2	Build 3	Build 4
5.1 Project planning and oversight	x	x	x	x
5.2 Establishing a software development environment	x	x	x	x
5.3 System requirements definition	x	x		
5.4 System design	x	x	x	
5.5 Software requirements definition	x	x	x	x
5.6 Software design	x	x	x	x
5.7 Software implementation and unit testing	x	x	x	x
5.8 Unit integration and testing	x	x	x	x
5.9 Software item qualification testing		x	x	x
5.10 Software/hardware item integration and testing		x	x	x
5.11 System qualification testing			x	x
5.12 Preparing for software use	x	x	x	x
5.13 Preparing for software transition				x
Integral processes:				
5.14 Software configuration management	x	x	x	x
5.15 Software product evaluation	x	x	x	x
5.16 Software quality assurance	x	x	x	x
5.17 Corrective action	x	x	x	x
5.18 Joint technical and management reviews	x	x	x	x
5.19 Risk management	x	x	x	x
5.20 Software management indicators			x	x
5.21 Administrative security and privacy protection				
5.22 Managing subcontractors	x	x		
5.23 Interfacing with software IV&V agents				
5.24 Coordinating with associate developers				
5.25 Project process improvement	x	x	x	

Figure 1 — One possible mapping of this standard's activities to multiple builds

5.1.2 Software item test planning

The developer shall develop and record plans for conducting software item qualification testing. This planning shall include all applicable items in the Software Test Plan (STP) (see E.2.2).

5.1.3 System test planning

The developer shall participate in developing and recording plans for conducting system qualification testing. For software systems, this planning shall include all applicable items in the Software Test Plan (STP) (see E.2.2). (The intent for software systems is a single Software Test Plan covering both software item and system qualification testing.)

5.1.4 Software installation planning

The developer shall develop and record plans for performing software installation and training at the user sites specified in the contract. This planning shall include all applicable items in the Software Installation Plan (SIP) (see E.2.3).

5.1.5 Software transition planning

The developer shall identify all software development resources that will be needed by the maintenance organization to fulfill the support strategy specified in the contract. The developer shall develop and record plans identifying these resources and describing the approach to be followed for transitioning deliverable items to the maintenance organization. This planning shall include all applicable items in the Software Transition Plan (STrP) (see E.2.4).

5.1.6 Following and updating plans

Following acquirer approval of any of the plans in this clause, the developer shall conduct the relevant activities in accordance with the plan. The developer's management shall review the software development process at intervals specified in the Software Development Plan to assure that the process complies with the contract and adheres to the plans. With the exception of developer-internal scheduling and related staffing information, updates to plans shall be subject to acquirer approval.

5.2 Establishing a software development environment

The developer shall establish a software development environment in accordance with the following requirements.

NOTE—If a system or software item is developed in multiple builds, establishing the software development environment in each build is interpreted to mean establishing the environment needed to complete that build.

5.2.1 Software engineering environment

The developer shall establish, control, and maintain a software engineering environment (e.g., the facilities, hardware, software, firmware, procedures, and documentation, such as computer-aided software engineering (CASE) tools, compilers, assemblers, linkers, loaders, operating systems, debuggers, simulators, emulators, documentation tools, and databasemanagement systems) to perform the software engineering effort. The developer shall ensure that each element of the environment performs its intended functions prior to its use on the project.

5.2.2 Software test environment

The developer shall establish, control, and maintain a software test environment (e.g., the facilities, hardware, software, firmware, procedures, and documentation, such as simulators, code analyzers, test case generators, and path analyzers, and possibly other items of the software engineering environment) to perform qualification, and possibly other, testing of software. The developer shall ensure that each element of the environment performs its intended functions prior to its use on the project.

5.2.3 Software development library

The developer shall establish, control, and maintain a software development library (SDL) to facilitate the orderly development and subsequent maintenance of software. The SDL may be an integral part of the software engineering and test environments. The developer shall maintain the SDL for the duration specified in the contract.

5.2.4 Software development files

The developer shall establish, control, and maintain a software development file (SDF) for each software unit or logically related group of software units, for each software item, and, as applicable, for logical groups of software items, for subsystems, and for the overall system. The developer shall record information about the development of the software in appropriate SDFs and shall maintain the SDFs for the duration specified in the contract.

5.2.5 Non-deliverable software

The developer may use non-deliverable software in the development of deliverable software provided: 1) the operation and maintenance of the deliverable software after delivery to the acquirer do not depend on the non-deliverable software, or 2) the acquirer has or can obtain the same software. The developer shall ensure that all non-deliverable software used on the project performs its intended functions prior to its use on the project.

5.3 System requirements definition

The developer shall participate in system requirements definition in accordance with the following requirements.

NOTE—If a system is developed in multiple builds, its requirements may not be fully defined until the final build. The developer's planning will identify the subset of system requirements to be defined in each build and the subset to be implemented in each build. System requirements definition for a given build is interpreted to mean defining the system requirements so identified for that build.

5.3.1 Analysis of user input

The developer shall participate in analyzing user input provided by the acquirer to gain an understanding of user needs. This input may take the form of need statements, surveys, problem/change reports, feedback on prototypes, interviews, or other user input or feedback.

NOTE—The intent of this requirement is to ensure that all interested parties, (such as user, acquirer, developer, and maintenance and test organizations), maintain on-going communications regarding user needs throughout the development of the system.

5.3.2 Operational concept

The developer shall participate in defining and recording the operational concept for the system. The result shall include all applicable items in the Operational Concept Description (OCD) (see F.2.1).

5.3.3 System requirements

Based on analysis of user needs, operational concepts, and other considerations, the developer shall participate in defining and recording the requirements to be met by the system and the methods to be used to ensure that each requirement has been met. The result shall include all applicable items in the System/Subsystem Specification (SSS) (see F.2.2). Depending on contract provisions, requirements concerning system interfaces may be included in the SSS or in Interface Requirements Specifications (IRSs).

NOTE—If a system consists of subsystems, the activity in 5.3.3 is intended to be performed iteratively with the activities in 5.4 (System design) to define system requirements, design the system and identify its subsystems, define the requirements for those subsystems, design the subsystems and identify their components, and so on.

5.4 System design

The developer shall participate in system design in accordance with the following requirements.

NOTE—If a system is developed in multiple builds, its design may not be fully defined until the final build. The developer's planning will identify the portion of the system design to be defined in each build. System design for a given build is interpreted to mean defining the portion of the system design identified for that build.

5.4.1 System-wide design decisions

The developer shall participate in defining and recording system-wide design decisions (that is, decisions about the system's behavioral design and other decisions affecting the selection and design of system components). The result shall include all applicable items in the system-wide design clause of the System/Subsystem Design Description (SSDD) (see G.2.1). Depending on contract provisions, design pertaining to interfaces may be included in the SSDD or in Interface Design Descriptions (IDDs), and design pertaining to databases may be included in the SSDD or in Database Design Descriptions (DBDDs).

NOTE—Design decisions act as developer-internal "requirements," to be implemented, imposed on subcontractors, if applicable, and confirmed by developer-internal testing, but their fulfillment need not be demonstrated to the acquirer.

5.4.2 System architectural design

The developer shall participate in defining and recording the architectural design of the system (identifying the components of the system, their interfaces, and a concept of execution among them) and the traceability between the system components and system requirements. The result shall include all applicable items in the architectural design and traceability clauses of the System/Subsystem Design Description (SSDD) (see G.2.1). Depending on contract provisions, design pertaining to interfaces may be included in the SSDD or in Interface Design Descriptions (IDDs), and design pertaining to databases may be included in the SSDD or in Database Design Descriptions (DBDDs).

NOTE—For brevity, this clause is written in terms of organizing a system into components. However, this should be interpreted to cover organizing a system into subsystems, organizing a subsystem into hardware items, software items, and manual operations, or other variations as appropriate.

5.5 Software requirements definition

Based on analysis of system requirements, system design, and other considerations, the developer shall define, and record the software requirements to be met by each software item, the methods to be used to ensure that each requirement has been met, and the traceability between the software item requirements and system requirements. The result shall include all applicable items in the Software Requirements Specification (SRS) (see F.2.4). Depending on contract provisions, requirements concerning software item interfaces may be included in SRSs or in Interface Requirements Specifications IRSs).

NOTE—If a software item is developed in multiple builds, its requirements may not be fully defined until the final build. The developer's planning will identify the subset of each software item's requirements to be defined in each build and the subset to be implemented in each build. Software requirements definition for a given build is interpreted to mean defining the software item requirements so identified for that build.

5.6 Software design

The developer shall perform software design in accordance with the following requirements.

NOTE—If a software item is developed in multiple builds, its design may not be fully defined until the final build. Software design in each build is interpreted to mean the design necessary to meet the software item requirements to be implemented in that build.

5.6.1 Software item-wide design decisions

The developer shall define and record software item-wide design decisions (that is, decisions about the software item's behavioral design and other decisions affecting the selection and design of the software units comprising the software item). The result shall include all applicable items in the software item-wide design clause of the Software Design Description (SDD) (see G.2.4). Depending on contract provisions, design pertaining to interfaces may be included in SDDs or in Interface Design Descriptions (IDDs), and design pertaining to databases may be included in SDDs or in Database Design Descriptions (DBDDs).

5.6.2 Software item architectural design

The developer shall define and record the architectural design of each software item (identifying the software units comprising the software item, their interfaces, and a concept of execution among them) and the traceability between the software units and the software item requirements. The result shall include all applicable items in the architectural design and traceability clauses of the Software Design Description (SDD) (see G.2.4). Depending on contract provisions, design pertaining to interfaces may be included in SDDs or in Interface Design Descriptions (IDDs), and design pertaining to databases may be included in SDDs or in Database Design Descriptions (DBDDs).

NOTE—Software units may be made up of other software units and may be organized into as many levels as are needed to represent the software item architecture. For example, a software item may be divided into three software units, each of which is divided into additional software units, and so on.

5.6.3 Software item detailed design

The developer shall develop and record a description of each software unit. The result shall include all applicable items in the detailed design clause of the Software Design Description (SDD) (see G.2.4). Depending on contract provisions, design pertaining to interfaces may be included in SDDs or in Interface Design Descriptions (IDDs), and design of software units that are databases or that access or manipulate databases may be included in SDDs or in Database Design Descriptions (DBDDs).

5.7 Software implementation and unit testing

The developer shall perform software implementation and unit testing in accordance with the following requirements.

NOTE—The term "software" includes both computer programs and computer databases. The term "implementation" means converting software design into computer programs and computer databases. If a software item is developed in multiple builds, software implementation and unit testing of that software item is complete when the final build is complete. Software implementation and unit testing in each build is interpreted to include those units, or parts of units, needed to meet the software item requirements to be implemented in that build.

5.7.1 Software implementation

The developer shall develop and record software corresponding to each software unit in the software item design. This activity shall include, as applicable, coding computer instructions and data definitions, building databases, populating databases and other data files with data values, and other activities needed to implement the design. For deliverable software, the developer shall use the programming language specified in the contract.

NOTE—Software units in the design may or may not have a one-to-one relationship with the code and data entities (routines, procedures, databases, data files, etc.) that implement them or with the computer files containing those entities.

5.7.2 Preparing for unit testing

The developer shall establish test cases (in terms of inputs, expected results, and evaluation criteria), test procedures, and test data for testing the software corresponding to each software unit. The test cases shall cover the unit's design. The developer shall record this information in the appropriate software development files (SDFs).

5.7.3 Performing unit testing

The developer shall test the software corresponding to each software unit. The testing shall be in accordance with the unit test cases and procedures.

5.7.4 Revision and retesting

Based on the results of unit testing, the developer shall make necessary revisions to the software, perform necessary retesting, and update the software development files (SDFs) and other software products as needed.

5.7.5 Analyzing and recording unit test results

The developer shall analyze the results of unit testing and shall record the test and analysis results in appropriate software development files (SDFs).

5.8 Unit integration and testing

The developer shall perform unit integration and testing in accordance with the following requirements.

NOTES:

1—Unit integration and testing means integrating the software corresponding to two or more software units, testing the resulting software to ensure that it works together as intended, and continuing this process until all software in each software item is integrated and tested. The last stage of this testing is developer-internal software item testing. Since units may consist of other units, some unit integration and testing may take place during unit testing. The requirements in this clause are not meant to duplicate those activities.

2—If a software item is developed in multiple builds, unit integration and testing of that software item will not be completed until the final build. Unit integration and testing in each build is interpreted to mean integrating software developed in the current build with other software developed in that and previous builds, and testing the results.

5.8.1 Preparing for unit integration and testing

The developer shall establish test cases (in terms of inputs, expected results, and evaluation criteria), test procedures, and test data for conducting unit integration and testing. The test cases shall cover the software item-wide and software item architectural design. The developer shall record this information in the appropriate software development files (SDFs).

5.8.2 Performing unit integration and testing

The developer shall perform unit integration and testing. The testing shall be in accordance with the unit integration test cases and procedures.

5.8.3 Revision and retesting

Based on the results of unit integration and testing, the developer shall make necessary revisions to the software, perform necessary retesting, and update the software development files (SDFs) and other software products as needed.

5.8.4 Analyzing and recording unit integration and test results

The developer shall analyze the results of unit integration and testing and shall record the test and analysis results in appropriate software development files (SDFs).

5.9 Software item qualification testing

The developer shall perform software item qualification testing in accordance with the following requirements.

NOTES:

1—Software item qualification testing is performed to demonstrate to the acquirer that software item requirements have been met. It covers the software item requirements in Software Requirements Specifications (SRSs) and in associated Interface Requirements Specifications (IRSs). This testing contrasts with developer-internal software item testing, performed as the final stage of unit integration and testing.

2—If a software item is developed in multiple builds, its software item qualification testing will not be completed until the final build for that software item, or possibly until later builds involving items with which the software item is required to interface. Software item qualification testing in each build is interpreted to mean planning and performing tests of the current build of each software item to ensure that the software item requirements to be implemented in that build have been met.

5.9.1 Independence in software item qualification testing

The person(s) responsible for qualification testing of a given software item shall not be the persons who performed detailed design or implementation of that software item. This does not preclude persons who performed detailed design or implementation of the software item from contributing to the process, for example, by contributing test cases that rely on knowledge of the software item's internal implementation.

5.9.2 Testing on the target computer system

Software item qualification testing shall include testing on the target computer system or an alternative system approved by the acquirer.

5.9.3 Preparing for software item qualification testing

The developer shall define and record the test preparations, test cases, and test procedures to be used for software item qualification testing and the traceability between the test cases and the software item requirements. The result shall include all applicable items in the Software Test Description (STD) (see H.2.1). The developer shall prepare the test data needed to carry out the test cases and provide the acquirer advance notice of the time and location of software item qualification testing.

5.9.4 Dry run of software item qualification testing

If software item qualification testing is to be witnessed by the acquirer, the developer shall dry run the software item test cases and procedures to ensure that they are complete and accurate and that the software is ready for witnessed testing. The developer shall record the results of this activity in appropriate software development files (SDFs) and shall update the software item test cases and procedures as appropriate.

5.9.5 Performing software item qualification testing

The developer shall perform qualification testing of each software item. The testing shall be in accordance with the software item test cases and procedures.

5.9.6 Revision and retesting

Based on the results of software item qualification testing, the developer shall make necessary revisions to the software, provide the acquirer advance notice of retesting, conduct necessary retesting, and update the software development files (SDFs) and other software products as needed.

5.9.7 Analyzing and recording software item qualification test results

The developer shall analyze and record the results of software item qualification testing. The results shall include all applicable items in the Software Test Report (STR) (see H.2.2).

5.10 Software/hardware item integration and testing

The developer shall participate in software/hardware item integration and testing activities in accordance with the following requirements.

NOTES:

1—Software/hardware item integration and testing means integrating software items with interfacing hardware items and software items, testing the resulting groupings to determine whether they work together as intended, and continuing this process until all software items and hardware items in the system are integrated and tested. The last stage of this testing is developer-internal system testing.

2—If a system or software item is developed in multiple builds, software/hardware item integration and testing may not be complete until the final build. Software/hardware item integration and testing in each build is interpreted to mean integrating the current build of each software item with the current build of other software items and hardware items and testing the results to ensure that the system requirements to be implemented in that build have been met.

5.10.1 Preparing for software/hardware item integration and testing

The developer shall participate in developing and recording test cases (in terms of inputs, expected results, and evaluation criteria), test procedures, and test data for conducting software/hardware item integration and testing. The test cases shall cover the system-wide and system architectural design. The developer shall record software-related information in appropriate software development files (SDFs).

5.10.2 Performing software/hardware item integration and testing

The developer shall participate in software/hardware item integration and testing. The testing shall be in accordance with the software/hardware item integration test cases and procedures.

5.10.3 Revision and retesting

Based on the results of software/hardware item integration and testing, the developer shall make necessary revisions to the software, participate in necessary retesting, and update the appropriate software development files (SDFs) and other software products as needed.

5.10.4 Analyzing and recording test results

The developer shall participate in analyzing the results of software/hardware item integration and testing. Software-related analysis and test results shall be recorded in appropriate software development files (SDFs).

5.11 System qualification testing

The developer shall participate in system qualification testing in accordance with the following requirements.

NOTES:

1—System qualification testing is performed to demonstrate to the acquirer that system requirements have been met. It covers the system requirements in the System/Subsystem Specifications (SSE) and in associated Interface Requirements Specifications (IRSs). This testing contrasts with developer-internal system testing, performed as the final stage of software/hardware item integration and testing.

2—If a system is developed in multiple builds, qualification testing of the completed system will not occur until the final build. System qualification testing in each build is interpreted to mean planning and performing tests of the current build of the system to ensure that the system requirements to be implemented in that build have been met.

5.11.1 Independence in system qualification testing

The person(s) responsible for fulfilling the requirements in this clause shall not be the persons who performed detailed design or implementation of software in the system. This does not preclude persons who performed detailed design or implementation of software in the system from contributing to the process, for example, by contributing test cases that rely on knowledge of the system's internal implementation.

5.11.2 Testing on the target computer system

The developer's system qualification testing shall include testing on the target computer system or an alternative system approved by the acquirer.

5.11.3 Preparing for system qualification testing

The developer shall participate in developing and recording the test preparations, test cases, and test procedures to be used for system qualification testing and the traceability between the test cases and the system requirements. For software systems, the results shall include all applicable items in the Software Test Description (STD) (see H.2.1). The developer shall participate in preparing the test data needed to carry out the test cases and in providing the acquirer advance notice of the time and location of system qualification testing.

5.11.4 Dry run of system qualification testing

If system qualification testing is to be witnessed by the acquirer, the developer shall participate in dry running the system test cases and procedures to ensure that they are complete and accurate and that the system is ready for witnessed testing. The developer shall record the software-related results of this activity in appropriate software development files (SDFs) and shall participate in updating the system test cases and procedures as appropriate.

5.11.5 Performing system qualification testing

The developer shall participate in system qualification testing. This testing shall be in accordance with the system test cases and procedures.

5.11.6 Revision and retesting

Based on the results of system qualification testing, the developer shall make necessary revisions to the software, provide the acquirer advance notice of retesting, participate in necessary retesting, and update the software development files (SDFs) and other software products as needed.

5.11.7 Analyzing and recording system qualification test results

The developer shall participate in analyzing and recording the results of system qualification testing. For software systems, the result shall include all applicable items in the Software Test Report (STR) (see H.2.2).

5.12 Preparing for software use

The developer shall prepare for software use in accordance with the following requirements.

NOTE—41 software is developed in multiple builds, the developer's planning identifies what software, if any, is to be distributed to users in each build and the extent of distribution (for example, full distribution or distribution to selected evaluators only). Preparing for software use in each build is interpreted to include those activities necessary to carry out the distribution plans for that build.

5.12.1 Preparing the executable software

The developer shall prepare the executable software for each user site, including any batch files, command files, data files, or other software files needed to install and operate the software on its target computer(s). The result shall include all applicable items in the executable software clause of the Software Product Specification (SPS) (see I.2.1).

NOTE—To order only the executable software (delaying delivery of source files and associated maintenance information to a later build), the acquirer can order an SPS, tailoring out all but the executable software clause of the SPS.

5.12.2 Preparing version descriptions for user sites

The developer shall identify and record the exact version of software prepared for each user site. The information shall include all applicable items in the Software Version Description (SVD) (see I.2.2).

5.12.3 Preparing user manuals

The developer shall prepare user manuals in accordance with the following requirements.

NOTE—Few, if any, systems will need all of the manuals in this clause. The intent is for the acquirer, with input from the developer, to determine which manuals are appropriate for a given system and to require the development of only those manuals. Commercial or other manuals that contain the required information can be substituted for the manuals specified in this standard. The manuals in this clause are normally developed in parallel with software development, ready for use in software item testing.

5.12.3.1 Software user manuals

The developer shall identify and record information needed by hands-on users of the software (persons who will both operate the software and make use of its results). The information shall include all applicable items in the Software User Manual (SUM) (see J.2.1).

5.12.3.2 Software input/output manuals

The developer shall identify and record information needed by persons who will submit input to, and receive output from, the software, relying on others to operate the software in a computer center or other centralized or networks software installation. The information shall include all applicable items in the Software Input/Output Manual (SIOM) (see J.2.2).

5.12.3.3 Software center operator manuals

The developer shall identify and record information needed by persons who will operate the software in a computer center or other centralized or networked software installation, so that it can be used by others. The information shall include all applicable items in the Software Center Operator Manual (SCOM) (see J.2.3).

5.12.3.4 Computer operation manuals

The developer shall identify and record information needed to operate the computers on which the software will run. The information shall include all applicable items in the Computer Operation Manual (COM) (see J.2.4).

5.12.4 Installation at user sites

The developer shall:

a) Install and check out the executable software at the user sites specified in the contract.
b) Provide training to users as specified in the contract.
c) Provide other assistance to user sites as specified in the contract.

5.13 Preparing for software transition

The developer shall prepare for software transition in accordance with the following requirements.

NOTE—If software is developed in multiple builds, the developer's planning identifies what software, if any, is to be transitional to the maintenance organization in each build. Preparing for software transition in each build is interpreted to include those activities necessary to carry out the transition plans for that build.

5.13.1 Preparing the executable software

The developer shall prepare the executable software to be transitioned to the maintenance site, including any batch files, command files, data files, or other software files needed to install and operate the software on its target computer(s). The result shall include all applicable items in the executable software clause of the Software Product Specification (SPS) (see I.2.1).

5.13.2 Preparing source files

The developer shall prepare the source files to be transitioned to the maintenance site, including any batch files, command files, data files, or other files needed to regenerate the executable software. The result shall include all applicable items in the source file clause of the Software Product Specification (SPS) (see I.2.1).

5.13.3 Preparing version descriptions for the maintenance site

The developer shall identify and record the exact version of software prepared for the maintenance site. The information shall include all applicable items in the Software Version Description (SVD) (see I.2.2).

5.13.4 Preparing the "as built" software item design and related information

The developer shall update the design description of each software item to match the "as built" software and shall define and record: the methods to be used to verify copies of the software, the measured computer hardware resource utilization for the software item, other information needed to maintain the software, and traceability between the software item's source files and software units and between the measured computer hardware resource utilization and the software item requirements concerning them. The result shall include

all applicable items in the qualification, software maintenance, and traceability clauses of the Software Product Specification (SPS) (see I.2.1).

NOTE—In hardware development, the final product is an approved design from which hardware items can be manufactured. In software development, by contrast, the final product is the software, not its design, and "manufacturing" consists of electronically duplicating the software, not recreating it from the design. The "as built" design is included in the Software Product Specification not as the product but as information that may help the maintenance organization understand the software in order to modify, enhance, and otherwise maintain it.

5.13.5 Updating the system design description

The developer shall participate in updating the system design description to match the "as built" system. The result shall include all applicable items in the System/Subsystem Design Description (SSDD) (see G.2.1).

5.13.6 Updating the software requirements

The developer shall update the software and interface requirements for each software item to match the approved "as built" software. The result shall include all applicable items in the Software Requirements Specification (SRS) (see F.2.4) and in the Interface Requirements Specification (IRS) (see F.2.3).

5.13.7 Updating the system requirements

The developer shall participate in updating the system requirements and associated interface requirements to match the approved "as built" system. The result shall include all applicable items in the System/Subsystem Specification (SSS) (see F.2.2) and in the Interface Requirements Specification (IRS) (see F.2.3).

5.13.8 Preparing maintenance manuals

The developer shall prepare maintenance manuals in accordance with the following requirements.

NOTE—Not all systems will need the manuals in this clause. The intent is for the acquirer, with input from the developer, to determine which manuals are appropriate for a given system and to require the development of only those manuals. Commercial or other manuals that contain the required information can be substituted for the manuals specified in this standard. The manuals in this clause supplement the System/Subsystem Design Description (SSDD) and the Software Product Specifications (SPS), which serve as the primary sources of information for software maintenance. The user manuals cited in 5.12.3 are also useful to maintenance personnel.

5.13.8.1 Computer programming manuals

The developer shall identify and record information needed to program the computers on which the software was developed or on which it will run. The information shall include all applicable items in the Computer Programming Manual (CPM) (see I.2.3).

5.13.8.2 Firmware support manuals

The developer shall identify and record information needed to program and reprogram any firmware devices in which the software will be installed. The information shall include all applicable items in the Firmware Support Manual (FSM) (see I.2.4).

5.13.9 Transition to the designated maintenance site

The developer shall:

a) Install and check out the deliverable software in the maintenance environment designated in the contract.

b) Demonstrate to the acquirer that the deliverable software can be regenerated (compiled/linked/loaded into an executable product) and maintained using commercially available, acquirer-owned, or contractually deliverable software and hardware designated in the contract or approved by the acquirer.
c) Provide training to the maintenance organization as specified in the contract.
d) Provide other assistance to the maintenance organization as specified in the contract.

5.14 Software configuration management

The developer shall perform software configuration management in accordance with the following requirements.

NOTE—If a system or software item is developed in multiple builds, the software products of each build may be refinements of, or additions to, software products of previous builds. Software configuration management in each build is understood to take place in the context of the software products and controls in place at the start of the build.

5.14.1 Configuration identification

The developer shall participate in selecting software items, as performed under system architectural design in 5.4.2 , shall identify the entities to be placed under configuration control, and shall assign a project-unique identifier to each software item and each additional entity to be placed under configuration control. These entities shall include the software products to be developed or used under the contract and the elements of the software development environment. The identification scheme shall be at the level at which entities will actually be controlled, for example, computer files, electronic media, documents, software units, hardware items, software items. The identification scheme shall include the version/revision/release status of each entity.

5.14.2 Configuration control

The developer shall establish and implement procedures designating the levels of control each identified entity is required to pass through (for example, author control, project-level control, acquirer control); the persons or groups with authority to authorize changes and to make changes at each level (for example, the programmer/analyst, the software lead, the project manager, the acquirer); and the steps to be followed to request authorization for changes, process change requests, track changes, distribute changes, and preserve past versions. Changes that affect an entity already under acquirer control shall be proposed to the acquirer in accordance with contractually established forms and procedures, if any.

NOTE—A number of requirements in this standard refer to “project-level or higher configuration control.” If “project-level” is not a level of control selected for the project, the Software Development Plan states how these requirements map to the selected levels.

5.14.3 Configuration status accounting

The developer shall prepare and maintain records of the configuration status of all entities that have been placed under project-level or higher configuration control. These records shall be maintained for the life of the contract. They shall include, as applicable, the current version/revision/release of each entity, a record of changes to the entity since being placed under project-level or higher configuration control, and the status of problem/change reports affecting the entity.

5.14.4 Configuration audits

The developer shall perform periodic audits of all entities that have been placed under project-level or higher configuration control. These audits shall ensure that each entity incorporates all approved changes, and no other changes, scheduled for inclusion at the time of the audit.

5.14.5 Packaging, storage, handling, and delivery

The developer shall establish and implement procedures for the packaging, storage, handling, and delivery of deliverable software products. Annex K provides guidance on the structure and format of deliverable software products. The developer shall maintain master copies of delivered software products for the duration specified in the contract.

5.15 Software product evaluation

The developer shall perform software product evaluation in accordance with the following requirements.

NOTE—If a system or software item is developed in multiple builds, the software products of each build are evaluated in the context of the objectives established for that build. A software product that meets those objectives can be considered satisfactory even though it is missing information designated for development in later builds.

5.15.1 In-process and final software product evaluations

The developer shall perform in-process evaluations of the software products generated in carrying out the requirements of this standard. In addition, the developer shall perform a final evaluation of each deliverable software product before its delivery. The software products to be evaluated, criteria to be used, and definitions for those criteria are given in annex L .

5.15.2 Software product evaluation records

The developer shall prepare and maintain records of each software product evaluation. These records shall be maintained for the duration specified in the contract. Problems in software products under project-level or higher configuration control shall be handled as described in 5.17 (Corrective action).

5.15.3 Independence in software product evaluation

The persons responsible for evaluating a software product shall not be the persons who developed the product. This does not preclude the persons who developed the software product from taking part in the evaluation (for example, as participants in a walk-through of the product).

5.16 Software quality assurance

The developer shall perform software quality assurance in accordance with the following requirements.

NOTE—If a system or software item is developed in multiple builds, the activities and software products of each build are evaluated in the context of the objectives established for that build. An activity or software product that meets those objectives can be considered satisfactory even though it is missing aspects designated for later builds. Planning for software quality assurance is included in software development planning (see 5.1.1).

5.16.1 Software quality assurance evaluations

The developer shall conduct on-going evaluations of software development activities and the resulting software products to:

a) Assure that each activity required by the contract or described in the Software Development Plan is being performed in accordance with the contract and with the Software Development Plan.
b) Assure that each software product required by this standard or by other contract provisions exists and has undergone software product evaluations, testing, and corrective action as required by this standard and by other contract provisions.

5.16.2 Software quality assurance records

The developer shall prepare and maintain records of each software quality assurance activity. These records shall be maintained for the duration specified in the contract. Problems in software products under project-level or higher configuration control and problems in activities required by the contract or described in the Software Development Plan shall be handled as described in 5.17 (Corrective action).

5.16.3 Independence in software quality assurance

The persons responsible for conducting software quality assurance evaluations shall not be the persons who developed the software product, performed the activity, or are responsible for the software product or activity. This does not preclude such persons from taking part in these evaluations. The persons responsible for assuring compliance with the contract shall have the resources, responsibility, authority, and organizational freedom to permit objective software quality assurance evaluations and to initiate and verify corrective actions.

5.17 Corrective action

The developer shall perform corrective action in accordance with the following requirements.

5.17.1 Problem/change reports

The developer shall prepare a problem/change report to describe each problem detected in software products under project-level or higher configuration control and each problem in activities required by the contract or described in the Software Development Plan. The problem/change report shall describe the problem, the corrective action needed, and the actions taken to date. These reports shall serve as input to the corrective action system.

5.17.2 Corrective action system

The developer shall implement a corrective action system for handling each problem detected in software products under project-level or higher configuration control and each problem in activities required by the contract or described in the Software Development Plan. The system shall meet the following requirements:

a) Input to the system shall consist of problem/change reports.
b) The system shall be closed-loop, ensuring that all detected problems are promptly reported and entered into the system, action is initiated on them, resolution is achieved, status is tracked, and records of the problems are maintained for the duration specified in the contract.
c) Each problem shall be classified by category and priority, using the categories and priorities in annex m or acquirer approved alternatives.
d) Analysis shall be performed to detect trends in the problems reported.
e) Corrective actions shall be evaluated to determine whether problems have been resolved, adverse trends have been reversed, and changes have been correctly implemented without introducing additional problems.

5.18 Joint technical and management reviews

The developer shall plan and take part in joint (acquirer/developer) technical and management reviews in accordance with the following requirements.

NOTE—If a system or software item is developed in multiple builds, the types of joint reviews held and the criteria applied will depend on the objectives of each build. Software products that meet those objectives can be considered satisfactory even though they are missing information designated for development in later builds.

5.18.1 Joint technical reviews

The developer shall plan and take part in joint technical reviews at locations and dates proposed by the developer and approved by the acquirer. These reviews shall be attended by persons with technical knowledge of the software products to be reviewed. The reviews shall focus on in-process and final software products, rather than materials generated especially for the review. The reviews shall have the following objectives:

a) Review evolving software products, using as criteria the software product evaluation criteria in annex L; review and demonstrate proposed technical solutions; provide insight and obtain feedback on the technical effort; surface and resolve technical issues.
b) Review project status; surface near- and long-term risks regarding technical, cost, and schedule issues.
c) Arrive at agreed-upon mitigation strategies for identified risks, within the authority of those present.
d) Identify risks and issues to be raised at joint management reviews.
e) Ensure on-going communication between acquirer and developer technical personnel.

5.18.2 Joint management reviews

The developer shall plan and take part in joint management reviews at locations and dates proposed by the developer and approved by the acquirer. These reviews shall be attended by persons with authority to make cost and schedule decisions and shall have the following objectives. Examples of such reviews are identified in annex N .

a) Keep management informed about project status, directions being taken, technical agreements reached, and overall status of evolving software products.
b) Resolve issues that could not be resolved at joint technical reviews.
c) Arrive at agreed-upon mitigation strategies for near- and long-term risks that could not be resolved at joint technical reviews.
d) Identify and resolve management-level issues and risks not raised at joint technical reviews.
e) Obtain commitments and acquirer approvals needed for timely accomplishment of the project.

5.19 Risk management

The developer shall perform risk management throughout the software development process. The developer shall identify, analyze, and prioritize the areas of the software development project that involve potential technical, cost, or schedule risks; develop strategies for managing those risks; record the risks and strategies in the Software Development Plan; and implement the strategies in accordance with the plan.

5.20 Software management indicators

The developer shall use software management indicators to aid in managing the software development process and communicating its status to the acquirer. The developer shall identify and define a set of software management indicators, including the data to be collected, the methods to be used to interpret and apply the data, and the planned reporting mechanism. The developer shall record this information in the Software Development Plan and shall collect, interpret, apply, and report on those indicators as described in the plan. Candidate indicators are given in annex O .

5.21 Administrative security and privacy protection

The developer shall meet the administrative security and privacy protection requirements specified in the contract. These requirements may affect access to and control of the software development effort, the resulting software products, or both.

5.22 Managing subcontractors

If subcontractors are used, the developer shall include in subcontracts all contractual requirements necessary to ensure that software products are developed in accordance with prime contract requirements.

5.23 Interfacing with software IV&V agents

The developer shall interface with the software Independent Verification and Validation (IV&V) agent(s) or independent auditors as specified in the contract.

5.24 Coordinating with associate developers

The developer shall coordinate with associate developers, working groups, and interface groups as specified in the contract.

5.25 Project process improvement

The developer shall periodically assess the processes used on the project to determine their suitability and effectiveness. Based on these assessments, the developer shall identify any necessary and beneficial improvements to the project-specific processes, shall identify these improvements to the acquirer in the form of proposed updates to the Software Development Plan and, if approved, shall implement the improvements on the project.

6. Notes

(The contents of this clause are for information only.)

6.1 Cross reference of standard subclauses to annex subclauses

Given below is a cross reference from the subclauses of the standard to subclauses of the annexes that specify the software products cited in each subclause of the standard.

Standard	Annex	Title of Software Product
5.1.1 , 5.16.2, 5.17.1, 5.17.2, 5.19, 5.20, 5.25	E.2.1	Software Development Plan (SDP)
5.1.2 , 5.1.3	E.2.2	Software Test Plan (STP)
5.1.4	E.2.3	Software Installation Plan (SIP)
5.1.5	E.2.4	Software Transition Plan (STrP)
5.3.2	F.2.1	Operational Concept Description (OCD)
5.3.3 , 5.13.7	F.2.2	System/Subsystem Specification (SSS)
5.3.3 , 5.5, 5.13.6, 5.13.7	F.2.3	Interface Requirements Specification (IRS)
5.4.1 , 5.4.2 , 5.13.5	G.2.1	System/Subsystem Design Description (SSDD)
5.4.1 , 5.4.2 , 5.6.1 , 5.6.2 , 5.6.3	G.2.2	Interface Design Description (IDD)
5.4.1 , 5.4.2 , 5.6.1 , 5.6.2 , 5.6.3	G.2.3	Database Design Description (DBDD)
5.5, 5.13.6	F.2.4	Software Requirements Specification (SRS)
5.6.1 , 5.6.2 , 5.6.3	G.2.4	Software Design Description (SDD)
5.9.3 , 5.11.3	H.2.1	Software Test Description (STD)
5.9.7 , 5.11.7	H.2.2	Software Test Report (STR)
5.12.1, 5.13.1, 5.13.2, 5.13.4	I.2.1	Software Product Specification (SPS)
5.12.2, 5.13.3	I.2.2	Software Version Description (SVD)
5.12.3.1	J.2.1	Software User Manual (SUM)
5.12.3.2	J.2.2	Software Input/Output Manual (SIOM)
5.12.3.3	J.2.3	Software Center Operator Manual (SCOM)
5.12.3.4	J.2.4	Computer Operation Manual (COM)
5.13.8.1	I.2.3	Computer Programming Manual (CPM)
5.13.8.2	I.2.4	Firmware Support Manual (FSM)

6.2 Delivery of tool contents

Depending on contract provisions, the developer may be permitted to satisfy delivery requirements by delivering: 1) a repository or database containing the information specified in the standard; 2) a means of accessing that repository or database, such as a CASE tool, if not already available to the designated recipients; and 3) a hard-copy or electronically stored table of contents, specifying how and where to access the information required in each subclause.

Annex A

(normative)

Tailoring this standard for a project

A.1 Scope

This annex contains requirements for tailoring this standard for a project. This annex is normative (that is, binding), and is not subject to tailoring by either the acquirer or developer.

A.2 Tailoring process

The tailoring process consists of the following activities:

a) Identifying the project environment
b) Soliciting input
c) Selecting activities and products
d) Specifying tailoring decisions

A.3 Identifying the project environment

Characteristics of the project environment that influence tailoring decisions shall be identified. Examples of characteristics include: objectives of this phase of the development (such as exploring concepts, demonstrating capabilities, manufacturing); system and software requirements; organizational policies, procedures, and strategies; size, criticality, and type of system; existing software products; and number of personnel and organizations involved.

A.4 Soliciting input

Input from the organizations affected by tailoring decisions shall be solicited. User, maintenance, contracts, and potential (or selected) development organizations should be involved in tailoring.

A.5 Selecting processes, activities, and tasks

The processes, activities and products applicable to the project shall be identified. The following guidance should be applied when selecting applicable activities and products for the project.

a) Evaluate the requirements in J-STD-016-1995 to determine whether each requirement is applicable based on the project environment characteristics. Annexes B and C provide guidance on tailoring this standard.
b) Decide which requirements in this standard are applicable and cost-effective over the life of the project.
c) Modify, if necessary, requirements in this standard to reflect unique or special needs of the project.

d) Decide which additional requirements not found in this standard, if any, should be specified.
e) Evaluate comments on tailoring decisions solicited from affected organizations.
f) Determine applicable requirements.
g) Record tailoring decisions and their rationale.

A.6 Specifying tailoring decisions

Tailoring decisions for the project shall be specified in the contract.

Annex B

(informative)

Guidance on development strategies, tailoring, and build planning

B.1 Scope

This annex describes three candidate development strategies and shows how this standard can be applied under each of these strategies and on a project involving reengineering. It is informative only, provided to aid in using this standard.

B.2 Candidate development strategies

There are many different development strategies that can be applied to software development. Three of these strategies are summarized below and in figure 2.

a) Once-through. The "once-through" strategy consists of performing the development process a single time. Simplistically: determine user needs, define requirements, design the system, implement the system, test, fix, and deliver.
b) Incremental. The "incremental" strategy determines user needs and defines the system requirements, then performs the rest of the development in a sequence of builds. The first build incorporates part of the planned capabilities, the next build adds more capabilities, and so on, until the system is complete.
c) Evolutionary. The "evolutionary" strategy also develops a system in builds, but differs from the incremental strategy in acknowledging that the user need is not fully understood and all requirements cannot be defined up front. In this strategy, user needs and system requirements are partially defined up front, then are refined in each succeeding build.

Development strategy	Define All Requirements First?	Multiple Development Cycles?	Distribute Interim Software?
Once-Through	Yes	No	No
Incremental (Preplanned Product Improvement)	Yes	Yes	Maybe
Evolutionary	No	Yes	Yes

Figure 2 — Key features of three development strategies

B.3 Selecting an appropriate development strategy

The development strategy is selected by the acquirer, but may be proposed by prospective or selected developers. Figure 3 illustrates a risk analysis approach for selecting an appropriate strategy. The approach consists of listing risk items (negatives) and opportunity items (positives) for each strategy; assigning each item a risk or opportunity level of High, Medium, or Low; and making a decision on which strategy to use based on a trade-off among the risks and opportunities. The fill-ins shown are sample considerations only. An actual analysis may use others. The “DECISION” entry on the bottom line shows which strategy was selected.

B.4 Relationship of this standard to development strategies

The development strategy usually applies to the overall system. The software within the system may be acquired under the same strategy or under a different one, such as requiring that all software be finalized in the first build of the system. Figures 4 , 5 , and 6 show how this standard might be applied under each of the development strategies identified in B.2. Figure 7 shows how this standard might be applied on a reengineering project. All four figures are, by necessity, simplified. For example, they show the standard’s activities in sequence when they might actually be ongoing, overlapping, or iterative, and they show each software product as a single entity, without depicting early drafts or updates.

B.5 Planning software builds and tailoring this standard

Planning the software builds on a project for each build may be accomplished in several ways. The acquirer might, for example, select an overall development strategy, leaving it to the developer to lay out the software builds. Alternatively, the acquirer might lay out the software builds as part of the contract. The approach selected will be project-dependent. The subclauses below provide guidelines for planning the builds and tailoring the standard without attempting to identify who performs each of the activities.

B.5.1 Identifying builds and their objectives

The first step in software build planning is to lay out a series of one or more builds and to identify the objectives of each build. The top part of figure 8 illustrates such planning. In the example, the System/Subsystem Specification (SSS) already exists and fulfillment of its requirements is divided into four builds, two of which will be prototypes distributed to a selected set of users, and two of which will be distributed to all users. A further objective of Build 4 is transitioning the software to the designated maintenance organization. An actual project would expand on these objectives.

Once-Through		Incremental		Evolutionary	
Risk Item (Reasons against this strategy)	Risk Level	Risk Item (Reasons against this strategy)	Risk Level	Risk Item (Reasons against this strategy)	Risk Level
- Requirements are not well understood	H	- Requirements are not well understood	H		
- System too large to do all at once	M	- User prefers all capabilities at first delivery	M	- User prefers all capabilities at first delivery	M
- Rapid changes in technology anticipated--may change the requirements	H	- Rapid changes in technology are expected--may change the requirements	H		
- Limited staff or budget available now	M				
Opportunity Item (Reasons to use this strategy)	Opp. Level	Opportunity Item (Reasons to use this strategy)	Opp. Level	Opportunity Item (Reasons to use this strategy)	Opp. Level
- User prefers all capabilities at first delivery	M	- Early capability is needed	H	- Early capability is needed	H
- User prefers to phase out old system all at once	L	- System breaks naturally into increments	M	- System breaks naturally into increments	M
		- Funding/staffing will be incremental	H	- Funding/staffing will be incremental	H
				- User feedback and monitoring of technology changes is needed to understand full requirements	H
				DECISION: USE THIS STRATEGY	

Figure 3 — Sample risk analysis for determining the appropriate development strategy

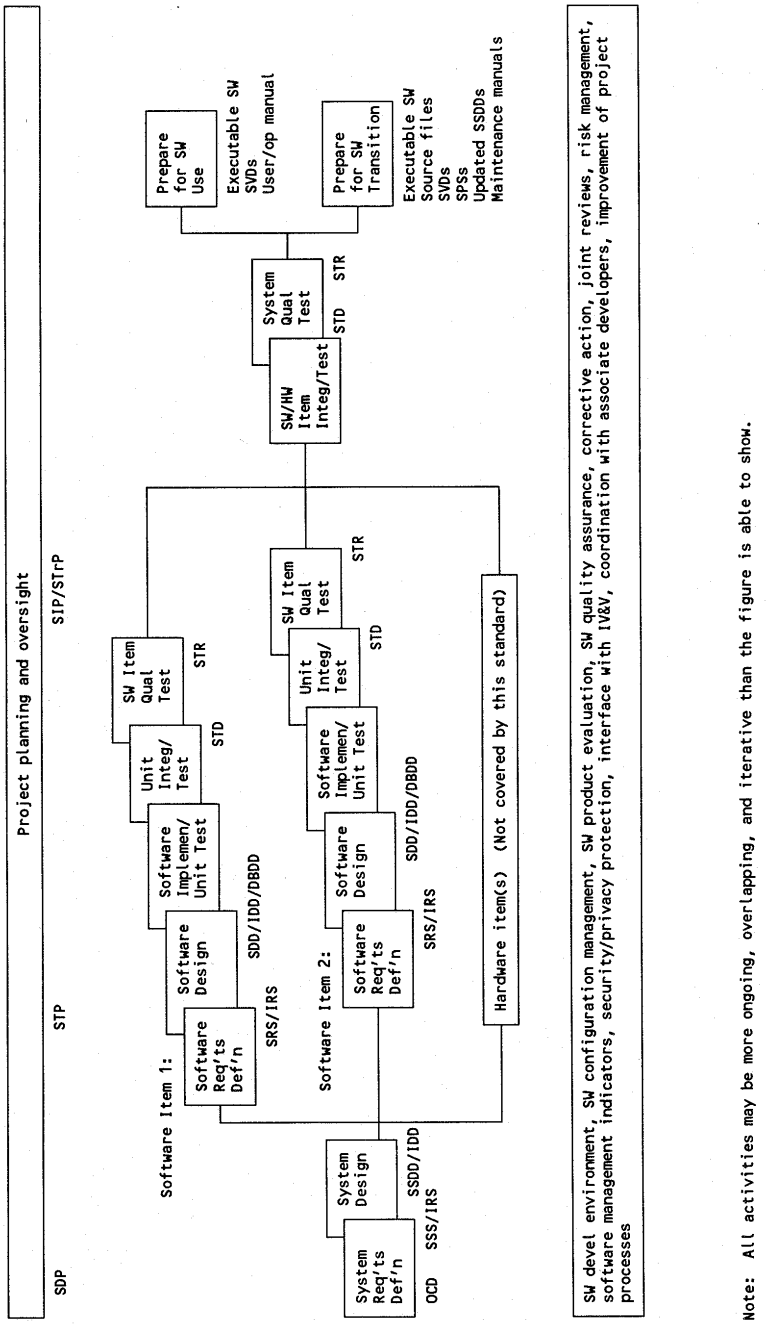


Figure 4 — One possible way of applying this standard to the Once-Through development strategy

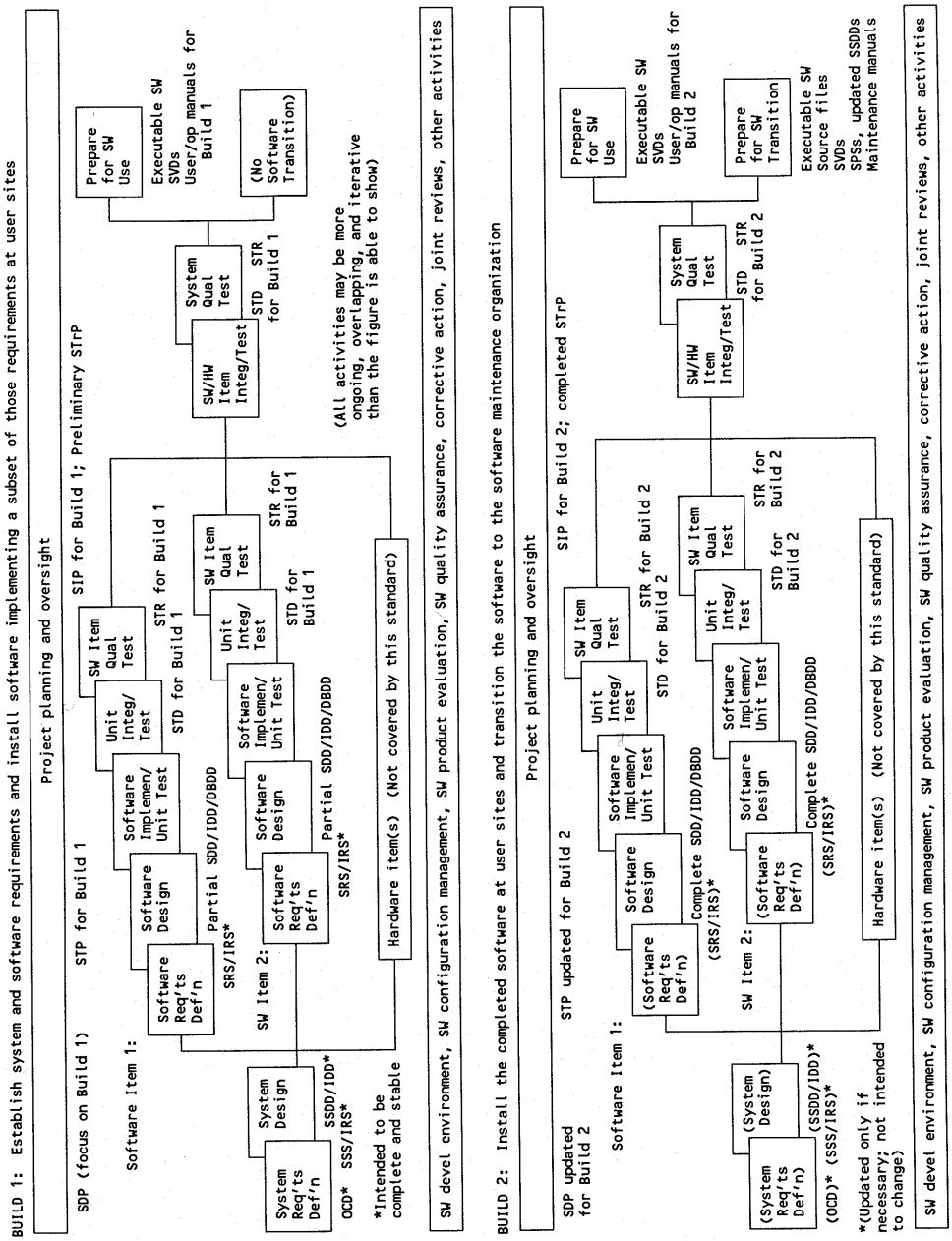


Figure 5 — One possible way of applying this standard to the Incremental development strategy

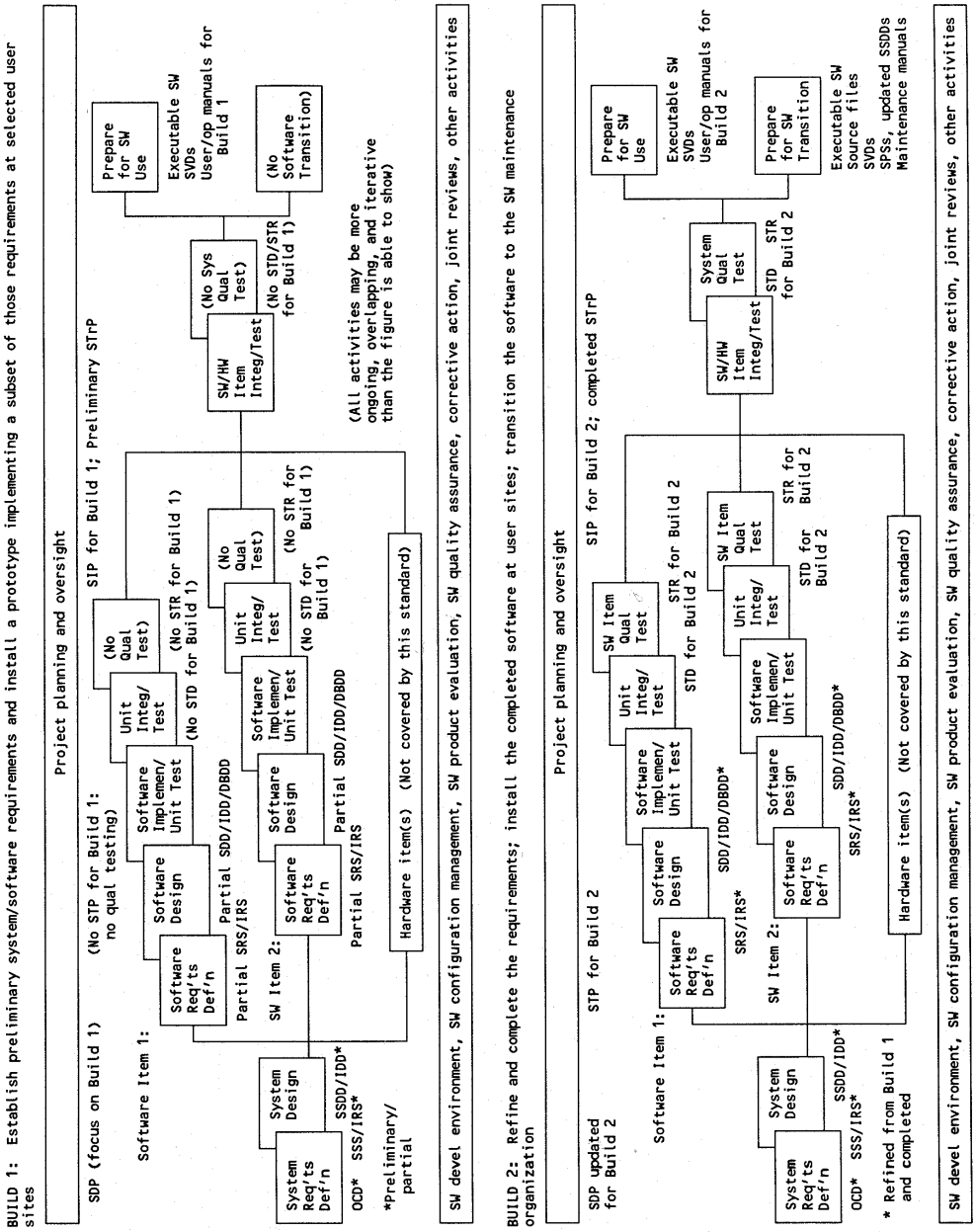


Figure6 — One possible way of applying this standard to the Evolutionary development strategy

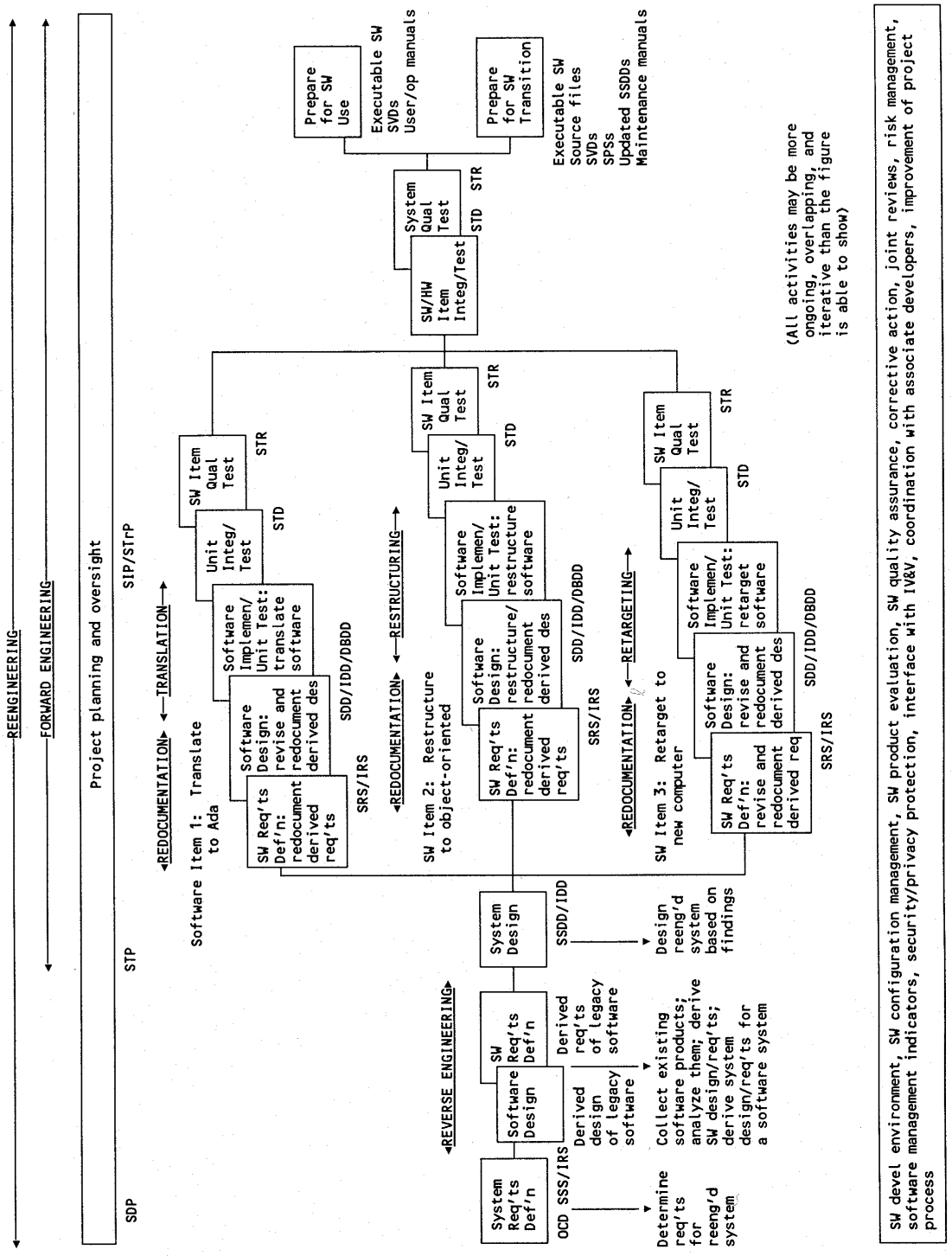


Figure7 — One possible way of applying this standard to a reengineering project

B.5.2 Identifying the activities to be performed in each build

The next step in build planning is identifying which activities apply in each build and determining the extent to which they apply. The activities of figure 8 show the start of this tailoring. Listed on the left are the subclauses of this standard. The worksheet entries indicate in which builds each activity is to be performed and include any notes regarding the nature of each activity in each build. For example, the figure shows that each build will include software development planning (5.1.1), but that the nature of that planning changes in each build. Some activities will not apply at all in a given build, some will apply identically in all builds, and some will apply differently in different builds. Since some aspects of the project, such as number and type of software items, may not have been identified at the time the worksheet is being filled out, completion of the worksheet may itself be incremental. The following guidelines apply:

a) Different decisions will apply to different types of software on a project. These differences can be shown within the entries of one worksheet or by using different worksheets for different types of software on a project.
b) If early builds are devoted to experimentation, developing "throw-away" software to arrive at a system concept or system requirements, it may be appropriate to forgo certain formalities, such as coding standards, that will be imposed later on the "real" software. If the early software will be used later, such formalities may be appropriate from the start. These decisions are project-dependent.

B.5.3 Recording tailoring decisions

Tailoring decisions made by the acquirer before the project begins are specified in the contract. Tailoring proposed by the developer may be communicated via feedback on draft requests for proposal, proposals, the Software Development Plan, joint reviews during the project, or by other means of communication. Refinements to the tailoring decisions may be ongoing as the project proceeds. Those involving contractual changes are handled accordingly.

B.5.4 Scheduling the selected activities in each build

Another important step in build planning is scheduling the activities in each build. As with tailoring, the acquirer may set forth general milestones and have the developer provide specifics or may provide specific schedules. The following guidelines apply:

a) A common mistake is to treat all software items as though they are required to be developed in "lock-step," reaching key milestones at the same time. Allowing software items to be on different schedules can result in more optimum development.
b) A similar mistake is to treat software units as though they are required to be developed in "lock-step," all designed by a certain date, implemented by a certain date, etc. Flexibility in the scheduling of software units can also be effective.
c) The activities in this standard need not be performed sequentially. Several may be taking place at one time, and an activity may be performed continually or intermittently throughout a build or over multiple builds. The activities in each build are to be laid out in the manner that best suits the work to be done.

BUILD PLANNING WORKSHEET		Build			
		1	2	3	4
1. Identify at right the objectives of each build 2. Indicate below which activities are to be accomplished during the development of each build. Add clarifying notes as needed.		Deliver to selected users an operational prototype that meets the following system-level requirements: SSS-1, SSS-5, ..., SSS-1250	Deliver to selected users an operational prototype that meets the requirements of Build 1 plus: SSS-2, SSS-3, SSS-15, ..., SSS-1249	Deliver to all users a tested system that meets the requirements of Builds 1 and 2 plus: SSS-4, SSS-7, SSS-10, ..., SSS-1248	Deliver to all users a tested system that meets all system-level requirements; transition to designated maintenance organization
Para	Activity				
5.1	PROJECT PLANNING AND OVERSIGHT				
5.1.1	Plan the software development effort	Yes: Plan Build 1 in detail; Builds 2-4 in general	Yes: Plan Build 2 in detail; Builds 3-4 in general	Yes: Plan Build 3 in detail; Build 4 in general	Yes: Plan Build 4 in detail
5.1.2	Plan for software item qualification testing	No: No software item qual testing in this build	No: No software item qual testing in this build	Yes: Plan for software item qual testing in this build	Yes: Update for software item qual testing in this build
5.1.3	Plan for system qualification testing	No: No system qual testing in this build	No: No system qual testing in this build	Yes: Plan for system qual testing in this build	Yes: Update for system qual testing in this build
5.1.4	Plan for installing software at user sites	No: Let users install on their own	No: Let users install on their own	Yes: Plan to install at user sites	Yes: Update as needed for installation of Bld 4
5.1.5	Plan for transitioning software to the maintenance organization	Yes: Very preliminary planning only	Yes: Update preliminary plans	Yes: Update preliminary plans	Yes: Finalize transition planning
5.1.6	Follow plans; perform management review	Yes: For those plans that are in effect	Yes: For those plans that are in effect	Yes: For those plans that are in effect	Yes: For those plans that are in effect
5.2	ESTABLISHING A SOFTWARE DEVEL ENVIRONMENT				
5.2.1	Establish a software engineering environment	Yes: As needed for Build 1	Yes: Update as needed for Build 2	Yes: Update as needed for Build 3	Yes: Update as needed for Build 4
5.2.2	Establish a software test environment	Yes: As needed for Build 1 testing	Yes: As needed for Build 2 testing	Yes: Set up fully for Build 3 qual testing	Yes: Update as needed for Build 4 qual testing

Figure 8 — Example of build planning

Annex C

(informative)

Guidance on ordering deliverables

C.1 Scope

This annex provides guidance to the acquirer on the deliverables to be required on a software development project. It is informative only, provided to aid in using this standard.

C.2 Ordering deliverables

This standard has been worded to differentiate between the planning/engineering activities that make up a software development project and the generation of deliverables. A key objective of this wording is to eliminate the notion that the acquirer is required to order a given deliverable in order to have planning or engineering work take place. Under this standard, the planning and engineering work takes place regardless of which deliverables are ordered, unless a given activity is tailored out of the standard. In addition, joint technical reviews have been included to review the results of that work in its natural form, without the generation of deliverables. Deliverables are to be ordered only when there is a genuine need to have planning or engineering information transformed into a deliverable (such as deliverables needed for use or maintenance of the software), recognizing that this transformation requires time and effort that would otherwise be spent on the engineering effort. Figure 10 in annex K provides information helpful in deciding whether the corresponding deliverable is to be ordered.

C.3 Scheduling deliverables

This standard has been structured to support a variety of development strategies and to provide the developer flexibility in laying out a software development process that will best suit the work to be done. All of this flexibility can be canceled by rigid scheduling of deliverables in the contract. If the contract lays out a strict "waterfall" sequence of deliverables, little room is left to propose innovative development processes. If the contract forces all software items into lock-step with each other, little room is left to develop the software items in an optimum order. If, to the maximum extent possible, the contract avoids such pre-determination, the door is left open for incremental delivery of software products, staggered development of software items, and other variations to optimize the software development effort. The developer's Software Development Plan will lay out a proposed schedule that meets the constraints in the contract. Final agreement on scheduling can take place at that time.

C.4 Format of deliverables

Traditional deliverables take the form of paper documents exactly following required formats and structures. While this form works well for some deliverables, it is not the only form, and alternatives are to be considered. One variation from paper documents is word processing files containing those documents. This saves paper, is less expensive to duplicate, transport, and change, but still requires the developer to format and structure the information in a particular way. Another variation is specifying that a paper or word processor

document is to include required contents but may be in the developer's format and structure. Yet another variation is allowing deliverables to take forms that are not traditional documents at all, such as data in computer-aided software engineering (CASE) tools. These variations can be specified in the contract.

C.5 Tailoring the content requirements for deliverables

Tailoring the content requirements for deliverables consists of deleting from the software product contents clauses of annexes E through J any requirements for unneeded information, altering requirements to more explicitly reflect the application to a particular effort, or adding requirements as needed. It can also consist of changes such as combining two or more documents under one cover.

Annex D

(informative)

Interpreting this standard for incorporation of reusable software products

D.1 Scope

This annex interprets this standard when applied to the incorporation of reusable software products. It is informative only, provided to aid in using this standard.

D.2 Evaluating reusable software products

The criteria for use in evaluating reusable software products will be described in the developer's SDP. Examples of candidate criteria that may be used include, but are not limited to:

a) Ability to provide required capabilities and meet required constraints
b) Ability to provide required safety, security, and privacy protection
c) Reliability/maturity, as evidenced by established track record
d) Testability
e) Interoperability with other system and system-external elements
f) Distribution issues, including:
    1) Restrictions on copying/distributing the software or documentation
    2) License or other fees applicable to each copy
g) Maintainability, including:
    1) Likelihood the software product will need to be changed
    2) Feasibility of accomplishing that change
    3) Availability and quality of documentation and source files
    4) Likelihood that the current version will continue to be maintained by the developer
    5) Impact on the system if the current version is not maintained
    6) The acquirers usage and ownership rights to the software product
    7) Warranties available
h) Short- and long-term cost impacts of using the software product
i) Technical, cost, and schedule risks and tradeoffs in using the software product

D.3 Interpreting this standard's activities for reusable software products

The following rules can be applied in interpreting this standard:

a) Any requirement that calls for development of a software product may be met by a reusable software product that fulfills the requirement and meets the criteria established in the Software Development Plan. The reusable software product may be used as-is or modified and may be used to satisfy part or all of the requirement. For example, a requirement may be met by using an existing plan, specification, or design.
b) When the reusable software product to be incorporated is the software itself, some of the requirements in this standard require special interpretation. Figure 9 provides this interpretation. Key issues

are whether the software will be modified, whether unmodified software constitutes an entire software item or only one or more software units, and whether unmodified software has a positive performance record (no firm criteria exist for making this determination). The figure is presented in a conditional manner: if an activity in the left column is required for a given type of software, the figure tells how to interpret the activity for reusable software of that type.

If this activity is required:	Interpret the activity as follows for each type of existing, reusable software:				
	For software items to be used unmodified		For software units to be used unmodified		For software units being modified for/ during project
	Positive performance record	No or poor performance record	Positive performance record	No or poor performance record	
5.1 Project planning and oversight	Include the activities in this figure in project plans				
5.2 Establishing software devel environment	Establish and apply a software test environment, software development library, and software development files as appropriate to perform the activities in this figure				Apply full requirements
5.3 System requirements definition	Consider software's capabilities in defining the operational concept & system requirements				
	Use test/ performance records to confirm ability to meet needs	Test to confirm ability to meet needs	Use test/ performance records to confirm ability to meet needs	Test to confirm ability to meet needs	Use tests or records to determine potential to meet needs
5.4.1 System-wide design	Consider the software's capabilities and characteristics in designing system behavior and in making other system-wide design decisions				
5.4.2 System architectural design	Include the software item in the system architecture; allocate system requirements to it		Consider the unit's capabilities and characteristics in designating software items and allocating system requirements to them		
5.5 Software requirements definition	Specify the project-specific requirements the software item is required to meet; verify via records or retest that the software item can meet them		Consider the unit's capabilities and characteristics in specifying the requirements for the software item of which it is a part		
5.6.1 Software item-wide design	No requirement: the software item-wide design decisions have already been made (recording the "as built" design is under 5.13)		Consider the unit's capabilities and characteristics in designing software item behavior and making other software item-wide design decisions		
5.6.2 Software item architectural design	No requirement: the architectural design is already defined (recording the "as built" design is under 5.13)		Include the unit in the software item architecture and allocate software item requirements to it		
5.6.3 Software item detailed design	No requirement: the detailed design is already defined (recording the "as built" design is under 5.13)		No requirement: the unit is already designed (recording the "as built" design is under 5.13)		Modify the unit's design as needed
5.7.1 Software implementation	No requirement: the software for the software item's units is already implemented		No requirement: the software for the unit is already implemented		Modify the software for the unit
5.7.2-5.7.5 Unit testing	No requirement: the software items's units are already tested	Perform selectively if in question and units are accessible	No requirement: the unit is already tested	Perform this testing	

Figure 9 — Interpreting this standard for incorporation of reusable software

If this activity is required:	Interpret the activity as follows for each type of existing, reusable software:				
	For software items to be used unmodified		For software units to be used unmodified		For software units being modified for/ during project
	Positive performance record	No or poor performance record	Positive performance record	No or poor performance record	
5.8 Unit integration and testing	No requirement: the SW items units are already integrated	Perform selectively if in question and units are accessible	Perform except where integration is already tested/proven	Perform this testing	
5.9 Software item qualification testing	No requirement: software item is already tested & proven	Perform this testing	Include the unit in software item qualification testing		
5.10 Software/ hardware item integration and testing	Perform, except where integration is already tested/proven	Include the software item in SW/HW item integration and testing	Include the unit in software/hardware item integration and testing		
5.11 System qualification testing	Include the software item in system qualification testing		Include the unit in system qualification testing		
5.12 Preparing for software use	Include the software for the software item or unit in the executable software; include in version descriptions; handle any license issues; cover use of the software item or unit, as appropriate, via existing, new, or revised user/operator manuals; install the software item or unit as part of the overall system; include its use, as appropriate, in the training offered				
5.13 Preparing for software transition	Include the software for the software item or unit in the executable software; prepare source files for the software item or unit, if available; include in version descriptions; handle any license issues; prepare or provide "as built" design descriptions for software whose design is known; install the software item or unit at the maintenance site; demonstrate regenerability if source is available; include in the training offered				
5.14 Software configuration management	Apply to all software products prepared, modified, or used in incorporating this software				
5.15 Software product evaluation	Apply to all software products prepared or modified in incorporating this software; for software products used unchanged, apply unless a positive performance record or evidence of past evaluations indicates that such an evaluation would be duplicative				
5.16 Software quality assurance	Apply to all activities performed and all software products prepared, modified, or used in incorporating this software				
5.17 Corrective action	Apply to all activities performed and all software products prepared or modified in incorporating this software				
5.18 Joint reviews	Cover the software products prepared or modified in incorporating this software				
5.19 - 5.25 Other activities	Apply the full requirements of each of these 6 clauses, if applicable				

Figure 9 — Interpreting this standard for incorporation of reusable software -- (continued)

Annex E

(normative)

Planning software product descriptions

E.1 Scope

This annex specifies the contents of software products associated with planning in this standard. It applies regardless of whether the software products are deliverable. This annex is a normative (that is, binding) part of this standard, subject to tailoring.

E.2 Software products covered

This following subclauses describe the contents of the software products covered by this annex. The products are listed in the order they are referenced in this standard and include the following:

a) Software Development Plan (SDP)
b) Software Test Plan (STP)
c) Software Installation Plan (SIP)
d) Software Transition Plan (STrP)

E.2.1 Contents of the Software Development Plan (SDP)

SOFTWARE DEVELOPMENT PLAN (SDP)

Contents

1) Scope
   1.1) Identification
   1.2) System overview
   1.3) Document overview
   1.4) Relationship to other plans
2) Referenced documents
3) Overview of required work
4) Plans for performing general software development activities
   4.1) Software development process
   4.2) General plans for software development
      4.2.1)Software development methods
      4.2.2)Standards and practices for software products
      4.2.3)Traceability
      4.2.4)Reusable software products
      4.2.5)Handling of critical requirements
      4.2.6)Computer hardware resource utilization
      4.2.7)Recording rationale
      4.2.8)Access for acquirer review
5) Plans for performing detailed software development activities

5.1) Project planning and oversight
5.1.1)Software development planning (covering updates to this plan)
5.1.2)Software item test planning
5.1.3)System test planning
5.1.4)Software installation planning
5.1.5)Software transition planning
5.1.6)Following and updating plans, including the intervals for management review
5.2) Establishing a software development environment
5.2.1)Software engineering environment
5.2.2)Software test environment
5.2.3)Software development library
5.2.4)Software development files
5.2.5)Non-deliverable software
5.3) System requirements definition
5.3.1)Analysis of user input
5.3.2)Operational concept
5.3.3)System requirements
5.4) System design
5.4.1)System-wide design decisions
5.4.2)System architectural design
5.5) Software requirements definition
5.6) Software design
5.6.1)Software item-wide design decisions
5.6.2)Software item architectural design
5.6.3)Software item detailed design
5.7) Software implementation and unit testing
5.7.1)Software implementation
5.7.2)Preparing for unit testing
5.7.3)Performing unit testing
5.7.4)Revision and retesting
5.7.5)Analyzing and recording unit test results
5.8) Unit integration and testing
5.8.1)Preparing for unit integration and testing
5.8.2)Performing unit integration and testing
5.8.3)Revision and retesting
5.8.4)Analyzing and recording unit integration and test results
5.9) Software item qualification testing
5.9.1)Independence in software item qualification testing
5.9.2)Testing on the target computer system
5.9.3)Preparing for software item qualification testing
5.9.4)Dry run of software item qualification testing
5.9.5)Performing software item qualification testing
5.9.6)Revision and retesting
5.9.7)Analyzing and recording software item qualification test results
5.10) Software/hardware item integration and testing
5.10.1)Preparing for software/hardware item integration and testing
5.10.2)Performing software/hardware item integration and testing
5.10.3)Revision and retesting
5.10.4)Analyzing and recording software/hardware item integration and test results
5.11) System qualification testing
5.11.1)Independence in system qualification testing
5.11.2)Testing on the target computer system
5.11.3)Preparing for system qualification testing
5.11.4)Dry run of system qualification testing

5.11.5)Performing system qualification testing
5.11.6)Revision and retesting
5.11.7)Analyzing and recording system qualification test results
5.12) Preparing for software use
5.12.1)Preparing the executable software
5.12.2)Preparing version descriptions for user sites
5.12.3)Preparing user manuals
5.12.4)Installation at user sites
5.13) Preparing for software transition
5.13.1)Preparing the executable software
5.13.2)Preparing source files
5.13.3)Preparing version descriptions for the maintenance site
5.13.4)Preparing the “as built” software item design and other software maintenance information
5.13.5)Updating the system design description
5.13.6)Updating the software requirements specification
5.13.7)Updating the system/subsystem specification
5.13.8)Preparing maintenance manuals
5.13.9)Transition to the designated maintenance site
5.14) Software configuration management
5.14.1)Configuration identification
5.14.2)Configuration control
5.14.3)Configuration status accounting
5.14.4)Configuration audits
5.14.5)Packaging, storage, handling, and delivery
5.15) Software product evaluation
5.15.1)In-process and final software product evaluations
5.15.2)Software product evaluation records, including items to be recorded
5.15.3)Independence in software product evaluation
5.16) Software quality assurance
5.16.1)Software quality assurance evaluations
5.16.2)Software quality assurance records, including items to be recorded
5.16.3)Independence in software quality assurance
5.17) Corrective action
5.17.1)Problem/change reports, including items to be recorded
5.17.2)Corrective action system
5.18) Joint technical and management reviews
5.18.1)Joint technical reviews, including a proposed set of reviews
5.18.2)Joint management reviews, including a proposed set of reviews
5.19) Risk management
5.20) Software management indicators
5.21) Administrative security and privacy protection
5.22) Managing subcontractors
5.23) Interfacing with software IV&V agents
5.24) Coordinating with associate developers
5.25) Project process improvement
6) Schedules and activity network
7) Project organization and resources
7.1) Project organization
7.2) Project resources
8) Notes
A) Annexes
1) **Scope** . This clause should be divided into the following subclauses.

1.1) **Identification** . This subclause shall contain a full identification of the system and the software to which this document applies, including, as applicable, identification number(s), title(s), abbreviation(s), version number(s), and release number(s).

1.2) **System overview** . This subclause shall briefly state the purpose of the system and the software to which this document applies. It shall describe the general nature of the system and software; summarize the history of system development, operation, and maintenance; identify the project sponsor, acquirer, user, developer, and maintenance organizations; identify current and planned operating sites; and list other relevant documents.

1.3) **Document overview** . This subclause shall summarize the purpose and contents of this document and shall describe any security or privacy protection considerations associated with its use.

1.4) **Relationship to other plans** . This subclause shall describe the relationship, if any, of the SDP to other project management plans.

2) **Referenced documents** . This clause shall list the number, title, revision, date, and source of all documents referenced in this manual.

3) **Overview of required work** . This clause should be divided into subclauses as needed to establish the context for the planning described in later clauses. It shall include, as applicable, an overview of:

a) Requirements and constraints on the system and software to be developed
b) Requirements and constraints on project documentation
c) Position of the project in the system life cycle
d) The selected development/acquisition strategy; any requirements or constraints on it
e) Requirements and constraints on project schedules and resources
f) Other requirements and constraints, such as on project security, privacy protection, methods, standards, interdependencies in hardware and software development, etc.

4) **Plans for performing general software development activities** . This clause should be divided into the following subclauses. Provisions corresponding to non-required activities may be satisfied by the words “Not applicable.” If different builds or different software on the project require different planning, these differences shall be noted in the subclauses. In addition to the content specified below, each subclause shall identify applicable risks/uncertainties, plans for dealing with those risks/uncertainties, and shall cover all contractual clauses regarding the identified topic.

4.1) **Software development process** . This subclause shall describe the software development process to be used. The planning shall identify planned builds, if applicable, their objectives, and the software development activities to be performed in each build.

4.2) **General plans for software development** . This subclause should be divided into the following.

4.2.1) **Software development methods** . This subclause shall describe or reference the software development methods to be used. Included shall be descriptions of the manual and automated tools and procedures to be used in support of these methods. Reference may be made to other subclauses in this plan if the methods are better described in context with the activities to which they will be applied.

4.2.2) **Standards and practices for software products** . This subclause shall describe or reference the standards and practices to be followed for representing requirements, design, code, test cases, test procedures, and test results. Reference may be made to other subclauses in this plan if the standards are better described in context with the activities to which they will be applied. Standards for code shall be provided for each programming language to be used. They shall include at a minimum:

a) Standards for format (such as indentation, spacing, capitalization, and order of information)
b) Standards for header comments (requiring, for example, name/identifier of the code; version identification; modification history; purpose; requirements and design decisions implemented; notes on the processing (such as algorithms used, assumptions, constraints, limitations, and side effects); and notes on the data (inputs, outputs, variables, data structures, etc.)
c) Standards for other comments (such as required number and content expectations)

d) Naming conventions for variables, parameters, packages, procedures, files, etc.
e) Restrictions, if any, on the use of programming language constructs or features
f) Restrictions, if any, on the complexity of code aggregates

4.2.3) **Traceability** . This subclause shall describe the approach to be followed for performing upward and downward traceability.

4.2.4) **Reusable software products** . This subclause shall describe the approach to be followed for identifying, evaluating, and incorporating reusable software products, including the scope of the search for such products and the criteria to be used for their evaluation and incorporation. Candidate or selected reusable software products known at the time this plan is prepared or updated shall be identified and described, together with benefits, drawbacks, and restrictions, as applicable, associated with their use.

4.2.5) **Handling of critical requirements** . This subclause shall describe the approach to be followed for identifying, developing strategies for, and handling safety, security, privacy protection, and other critical requirements.

4.2.6) **Computer hardware resource utilization** . This subclause shall describe the approach to be followed for allocating computer hardware resources and monitoring their utilization.

4.2.7) **Recording rationale** . This subclause shall describe the approach to be followed for recording rationale that will be useful to the maintenance organization for key decisions made on the project. It shall interpret the term "key decisions" for the project and state where the rationale are to be recorded.

4.2.8) **Access for acquirer review** . This subclause shall describe the approach to be followed for providing the acquirer or its authorized representative access to developer and subcontractor facilities for review of software products and activities.

5) **Plans for performing detailed software development activities** . This clause should be divided into the following subclauses. Provisions corresponding to non-required activities may be satisfied by the words "Not applicable." If different builds or different software on the project require different planning, these differences shall be noted in the subclauses. The discussion of each activity shall include the approach (methods/procedures/tools) to be applied to: 1) the analysis or other technical tasks involved, 2) the recording of results, and 3) the preparation of associated deliverables, if applicable. The discussion shall also identify applicable risks/uncertainties, plans for dealing with those risks/uncertainties, and shall cover all contractual clauses regarding the identified topic. Reference may be made to 4.2.1 if applicable methods are described there.

5.1) **Project planning and oversight** . This subclause should be divided into the following to describe the approach to be followed for project planning and oversight.

5.1.1) Software development planning (covering updates to this plan)
5.1.2) Software item test planning
5.1.3) System test planning
5.1.4) Software installation planning
5.1.5) Software transition planning
5.1.6) Following and updating plans, including the intervals for management review

5.2) **Establishing a software development environment** . This subclause should be divided into the following to describe the approach to be followed for establishing, controlling, and maintaining a software development environment.

5.2.1) Software engineering environment
5.2.2) Software test environment
5.2.3) Software development library
5.2.4) Software development files
5.2.5) Non-deliverable software

5.3) **System requirements definition** . This subclause should be divided into the following to describe the approach to be followed for participating in system requirements definition.

5.3.1) Analysis of user input
5.3.2) Operational concept
5.3.3) System requirements

5.4) **System design** . This subclause should be divided into the following to describe the approach to be followed for participating in system design.
5.4.1)System-wide design decisions
5.4.2)System architectural design

5.5) **Software requirements definition** . This subclause shall describe the approach to be followed for software requirements definition.

5.6) **Software design** . This subclause should be divided into the following to describe the approach to be followed for software design.
5.6.1)Software item-wide design decisions
5.6.2)Software item architectural design
5.6.3)Software item detailed design

5.7) **Software implementation and unit testing** . This subclause should be divided into the following to describe the approach to be followed for software implementation and unit testing.
5.7.1)Software implementation
5.7.2)Preparing for unit testing
5.7.3)Performing unit testing
5.7.4)Revision and retesting
5.7.5)Analyzing and recording unit test results

5.8) **Unit integration and testing** . This subclause should be divided into the following to describe the approach to be followed for unit integration and testing.
5.8.1)Preparing for unit integration and testing
5.8.2)Performing unit integration and testing
5.8.3)Revision and retesting
5.8.4)Analyzing and recording unit integration and test results

5.9) **Software item qualification testing** . This subclause should be divided into the following to describe the approach to be followed for software item qualification testing.
5.9.1)Independence in software item qualification testing
5.9.2)Testing on the target computer system
5.9.3)Preparing for software item qualification testing
5.9.4)Dry run of software item qualification testing
5.9.5)Performing software item qualification testing
5.9.6)Revision and retesting
5.9.7)Analyzing and recording software item qualification test results

5.10)**Software/hardware item integration and testing** . This subclause should be divided into the following to describe the approach to be followed for participating in software/hardware item integration and testing.
5.10.1)Preparing for software/hardware item integration and testing
5.10.2)Performing software/hardware item integration and testing
5.10.3)Revision and retesting
5.10.4)Analyzing and recording software/hardware item integration and test results

5.11)**System qualification testing** . This subclause should be divided into the following to describe the approach to be followed for participating in system qualification testing.
5.11.1)Independence in system qualification testing
5.11.2)Testing on the target computer system
5.11.3)Preparing for system qualification testing
5.11.4)Dry run of system qualification testing
5.11.5)Performing system qualification testing
5.11.6)Revision and retesting
5.11.7)Analyzing and recording system qualification test results

5.12)**Preparing for software use** . This subclause should be divided into the following to describe the approach to be followed for preparing for software use.
5.12.1)Preparing the executable software
5.12.2)Preparing version descriptions for user sites
5.12.3)Preparing user manuals

5.12.4)Installation at user sites

5.13)**Preparing for software transition** . This subclause should be divided into the following to describe the approach to be followed for preparing for software transition.

5.13.1)Preparing the executable software

5.13.2)Preparing source files

5.13.3)Preparing version descriptions for the maintenance site

5.13.4)Preparing the “as built” software item design and other software maintenance information

5.13.5)Updating the system design description

5.13.6)Updating the software requirements specification

5.13.7)Updating the system/subsystem specification

5.13.8)Preparing maintenance manuals

5.13.9)Transition to the designated maintenance site

5.14)**Software configuration management** . This subclause should be divided into the following to describe the approach to be followed for software configuration management.

5.14.1)Configuration identification

5.14.2)Configuration control

5.14.3)Configuration status accounting

5.14.4)Configuration audits

5.14.5)Packaging, storage, handling, and delivery

5.15)**Software product evaluation** . This subclause should be divided into the following to describe the approach to be followed for software product evaluation.

5.15.1)In-process and final software product evaluations

5.15.2)Software product evaluation records, including items to be recorded

5.15.3)Independence in software product evaluation

5.16)**Software quality assurance** . This subclause should be divided into the following to describe the approach to be followed for software quality assurance.

5.16.1)Software quality assurance evaluations

5.16.2)Software quality assurance records, including items to be recorded

5.16.3)Independence in software quality assurance

5.17)**Corrective action** . This subclause should be divided into the following to describe the approach to be followed for corrective action.

5.17.1)Problem/change reports, including items to be recorded (candidate items include project name, originator, problem number, problem name, software element or document affected, origination date, category and priority, description, analyst assigned to the problem, date assigned, date completed, analysis time, recommended solution, impacts, problem status, approval of solution, follow-up actions, corrector, correction date, version where corrected, correction time, description of solution implemented)

5.17.2)Corrective action system

5.18)**Joint technical and management reviews** . This subclause should be divided into the following to describe the approach to be followed for joint technical and management reviews.

5.18.1)Joint technical reviews, including a proposed set of reviews

5.18.2)Joint management reviews, including a proposed set of reviews

5.19)**Risk management** . This subclause shall describe the approach to be followed for risk management.

5.20)**Software management indicators** . This subclause shall describe the approach to be followed for use of software management indicators.

5.21)**Administrative security and privacy protection** . This subclause shall describe the approach to be followed for administrative security and privacy protection.

5.22)**Managing subcontractors** . This subclause shall describe the approach to be followed for managing subcontractors.

5.23)**Interfacing with software IV&V agents** . This subclause shall describe the approach to be followed for interfacing with IV&V agents or auditors.

5.24) **Coordinating with associate developers** . This subclause shall describe the approach to be followed for coordinating with associate developers.

5.25) **Project process improvement** . This subclause shall describe the approach to be followed for project process improvement.

6) **Schedules and activity network** . This clause shall present:
   a) Schedule(s) identifying the activities in each build and showing initiation of each activity, availability of draft and final deliverables and other milestones, and completion of each activity
   b) An activity network, depicting sequential relationships and dependencies among activities and identifying those activities that impose the greatest time restrictions on the project

7) **Project organization and resources** . This clause should be divided into the following subclauses to describe the project organization and resources to be applied in each build.

   7.1) **Project organization** . This subclause shall describe the organizational structure to be used on the project, including the organizations involved, their relationships to one another, and the authority and responsibility of each organization for carrying out required activities.

   7.2) **Project resources** . This subclause shall describe the resources to be applied to the project. It shall include, as applicable:
      a) Personnel resources, including:
      1) The estimated staff-loading for the project (number of personnel over time)
      2) The breakdown of the staff-loading numbers by responsibility (for example, management, software engineering, software testing, software configuration management, software product evaluation, software quality assurance)
      3) A breakdown of the skill levels, geographic locations, and security clearances of personnel performing each responsibility
      b) Overview of developer facilities to be used, including geographic locations in which the work will be performed, facilities to be used, and secure areas and other features of the facilities as applicable to the contracted effort.
      c) Acquirer-furnished equipment, software, services, documentation, data, and facilities required for the contracted effort. A schedule detailing when these items will be needed shall also be included.
      d) Other required resources, including a plan for obtaining the resources, dates needed, and availability of each resource item.

8) **Notes** . This clause shall contain any general information that aids in understanding this document (e.g., background information, glossary, rationale). This clause shall include an alphabetical listing of all acronyms, abbreviations, and their meanings as used in this document and a list of any terms and definitions needed to understand this document.

A) **Annexes** . Annexes may be used to provide information published separately for convenience in document maintenance (e.g., charts, classified data). As applicable, each annex shall be referenced in the main body of the document where the data would normally have been provided. Annexes may be bound as separate documents for ease in handling. Annexes shall be lettered alphabetically (A, B, etc.).

E.2.2 Contents of the Software Test Plan (STP)

SOFTWARE TEST PLAN (STP)

Contents

1) Scope
   1.1) Identification
   1.2) System overview
   1.3) Document overview
   1.4) Relationship to other plans
2) Referenced documents

3) Software test environment
   3.x) (Name of test site(s))
      3.x.1)Software
      3.x.2)Hardware and firmware
      3.x.3)Other materials
      3.x.4)Proprietary nature, acquirer's rights, and licensing
      3.x.5)Installation, testing, and control
      3.x.6)Participating organizations
      3.x.7)Personnel
      3.x.8)Orientation plan
      3.x.9)Tests to be performed
4) Test identification
   4.1) General information
      4.1.1)Test levels
      4.1.2)Test classes
      4.1.3)General test conditions
      4.1.4)Test progression
      4.1.5)Data recording, reduction, and analysis
   4.2) Planned tests
      4.2.x)(Item(s) to be tested)
      4.2.x.y)(Project-unique identifier of a test)
5) Test schedules
6) Requirements traceability
7) Notes
A) Annexes
1) **Scope** . This clause should be divided into the following subclauses.
   1.1) **Identification** . This subclause shall contain a full identification of the system and the software to which this document applies, including, as applicable, identification number(s), title(s), abbreviation(s), version number(s), and release number(s).
   1.2) **System overview** . This subclause shall briefly state the purpose of the system and the software to which this document applies. It shall describe the general nature of the system and software; summarize the history of system development, operation, and maintenance; identify the project sponsor, acquirer, user, developer, and maintenance organizations; identify current and planned operating sites; and list other relevant documents.
   1.3) **Document overview** . This subclause shall summarize the purpose and contents of this document and shall describe any security or privacy protection considerations associated with its use.
   1.4) **Relationship to other plans** . This subclause shall describe the relationship, if any, of the STP to related project management plans.
2) **Referenced documents** . This clause shall list the number, title, revision, date, and source of all documents referenced in this manual.
3) **Software test environment** . This clause should be divided into the following subclauses to describe the software test environment at each intended test site. Reference may be made to the Software Development Plan (SDP) for resources that are described there.
   3.x) **(Name of test site(s))** . This subclause shall identify one or more test sites to be used for the testing, and should be divided into the following to describe the software test environment at the site(s). If all tests will be conducted at a single site, this subclause and its subclauses shall be presented only once. If multiple test sites use the same or similar software test environments, they may be discussed together. Duplicative information among test site descriptions may be reduced by referencing earlier descriptions.
      3.x.1)**Software** . This subclause shall identify by name, number, and version, as applicable, the software (e.g., operating systems, compilers, communications software, related applications software, databases, input files, code auditors, dynamic path analyzers, test drivers, preprocessors, test data generators, test control software, other special test software, post-

processors) necessary to perform the planned testing activities at the test site(s). This subclause shall describe the purpose of the software, describe its media (tape, disk, etc.), identify those that are expected to be supplied by the site, and identify any classified processing or other security or privacy protection issues associated with the software.

3.x.2) **Hardware and firmware** . This subclause shall identify by name, number, and version, as applicable, the computer hardware, interfacing equipment, communications equipment, test data reduction equipment, apparatus such as extra peripherals (tape drives, printers, plotters), test message generators, test timing devices, test event records, etc.,and firmware that will be used in the software test environment at the test site(s). This subclause shall describe the purpose of the hardware or firmware, state the period of usage and the number of each needed, identify those that are expected to be supplied by the site, and identify any classified processing or other security or privacy protection issues associated with the hardware or firmware.

3.x.3) **Other materials** . This subclause shall identify and describe any other materials needed for the testing at the test site(s). These materials may include manuals, software listings, media containing the software to be tested, media containing data to be used in the tests, sample listings of output, and other forms or instructions. This subclause shall identify those items that are to be delivered to the site and those that are expected to be supplied by the site. The description shall include the type, layout, and quantity of the materials, as applicable. This subclause shall identify any classified processing or other security or privacy protection issues associated with the items.

3.x.4) **Proprietary nature, acquirer's rights, and licensing** . This subclause shall identify the proprietary nature, acquirer's rights, and licensing issues associated with each element of the software test environment.

3.x.5) **Installation, testing, and control** . This subclause shall identify the developer's plans for performing each of the following, possibly in conjunction with personnel at the test site(s):

a) Acquiring or developing each element of the software test environment
b) Installing and testing each item of the software test environment prior to its use
c) Controlling and maintaining each item of the software test environment

3.x.6) **Participating organizations** . This subclause shall identify the organizations that will participate in the testing at the test sites(s) and the roles and responsibilities of each.

3.x.7) **Personnel** . This subclause shall identify the number, type, and skill level of personnel needed during the test period at the test site(s), the dates and times they will be needed, and any special needs, such as multishift operation and retention of key skills to ensure continuity and consistency in extensive test programs.

3.x.8) **Orientation plan** . This subclause shall describe any orientation and training to be given before and during the testing. This information shall be related to the personnel needs given in 3.x.7. This training may include user instruction, operator instruction, maintenance and control group instruction, and orientation briefings to staff personnel. If extensive training is anticipated, a separate plan may be developed and referenced here.

3.x.9) **Tests to be performed** . This subclause shall identify, by referencing clause 4, the tests to be performed at the test site(s).

4) **Test identification** . This clause should be divided into the following subclauses to identify and describe each test to which this STP applies.

4.1) **General information** . This subclause should be divided into subclauses to present general information applicable to the overall testing to be performed.

4.1.1) **Test levels** . This subclause shall describe the levels at which testing will be performed, for example, software item level or system level.

4.1.2) **Test classes** . This subclause shall describe the types or classes of tests that will be performed (for example, timing tests, erroneous input tests, maximum capacity tests).

4.1.3) **General test conditions** . This subclause shall describe conditions that apply to all of the tests or to a group of tests. For example: "each test shall include nominal, maximum, and minimum values;" "each test of type x shall use live data;" "execution size and time shall be measured for each software item." Included shall be a statement of the extent of testing

to be performed and rationale for the extent selected. The extent of testing shall be expressed as a percentage of some well defined total quantity, such as the number of samples of discrete operating conditions or values, or other sampling approach. Also included shall be the approach to be followed for retesting/regression testing.

4.1.4) **Test progression** . In cases of progressive or cumulative tests, this subclause shall explain the planned sequence or progression of tests.

4.1.5) **Data recording, reduction, and analysis** . This subclause shall identify and describe the data recording, reduction, and analysis procedures to be used during and after the tests identified in this STP. These procedures shall include, as applicable, manual, automatic, and semi-automatic techniques for recording test results, manipulating the raw results into a form suitable for evaluation, and retaining the results of data reduction and analysis.

4.2) **Planned tests** . This subclause should be divided into the following to describe the total scope of the planned testing.

4.2.x) **(Item(s) to be tested)** . This subclause shall identify a software item, subsystem, system, or other entity by name and project-unique identifier, and should be divided into the following to describe the testing planned for the item(s). (Note: the "tests" in this plan are collections of test cases. There is no intent to describe each test case in this document.)

4.2.x.y) **(Project-unique identifier of a test)** . This subclause shall identify a test by project-unique identifier and shall provide the information specified below for the test. Reference may be made as needed to the general information in 4.1.

a) Test objective
b) Test level
c) Test type or class
d) Qualification method(s) as specified in the requirements specification
e) Identifier of the software item requirements and, if applicable, software system requirements addressed by this test. (Alternatively, this information may be provided in clause 6.)
f) Special requirements (for example, 48 hours of continuous facility time, simulation, extent of test, use of a special input or database)
g) Type of data to be recorded
h) Type of data recording/reduction/analysis to be employed
i) Assumptions and constraints, such as anticipated limitations on the test due to system or test conditions—timing, interfaces, equipment, personnel, database, etc.
j) Safety, security, and privacy protection considerations associated with the test

5) **Test schedules** . This clause shall contain or reference the schedules for conducting the tests identified in this plan. It shall include:

a) A listing or chart depicting the sites at which the testing will be scheduled and the time frames during which the testing will be conducted
b) A schedule for each test site depicting the activities and events listed below, as applicable, in chronological order with supporting narrative as necessary:
   1) On-site test period and periods assigned to major portions of the testing
   2) Pretest on-site period needed for setting up the software test environment and other equipment, system debugging, orientation, and familiarization
   3) Collection of database/data file values, input values, and other operational data needed for the testing
   4) Conducting the tests, including planned retesting
   5) Preparation, review, and approval of the Software Test Report (STR)

6) **Requirements traceability** . This subclause shall contain:

a) Traceability from each test identified in this plan to the software item requirements and, if applicable, software system requirements it addresses. (Alternatively, this traceability may be provided in 4.2.x.y and referenced from this subclause.)
b) Traceability from each software item requirement and, if applicable, each software system requirement covered by this test plan to the test(s) that address it. The traceability shall cover the software item requirements in all applicable Software Requirements Specifications (SRSs) and associated Interface Requirements Specifications (IRSs), and, for software systems, the

system requirements in all applicable System/Subsystem Specifications (SSS) and associated system-level IRSs.

7) **Notes** . This clause shall contain any general information that aids in understanding this document (e.g., background information, glossary, rationale). This clause shall include an alphabetical listing of all acronyms, abbreviations, and their meanings as used in this document and a list of any terms and definitions needed to understand this document.

A) **Annexes** . Annexes may be used to provide information published separately for convenience in document maintenance (e.g., charts, classified data). As applicable, each annex shall be referenced in the main body of the document where the data would normally have been provided. Annexes may be bound as separate documents for ease in handling. Annexes shall be lettered alphabetically (A, B, etc.).

E.2.3 Contents of the Software Installation Plan (SIP)

SOFTWARE INSTALLATION PLAN (SIP)

Contents

1) Scope
   1.1) Identification
   1.2) System overview
   1.3) Document overview
   1.4) Relationship to other plans
2) Referenced documents
3) Installation overview
   3.1) Description
   3.2) Contact point
   3.3) Support materials
   3.4) Training
   3.5) Tasks
   3.6) Personnel
   3.7) Security and privacy protection
4) Site-specific information for software center operations staff
   4.x) (Site name)
      4.x.1)Schedule
      4.x.2)Software inventory
      4.x.3)Facilities
      4.x.4)Installation team
      4.x.5)Installation procedures
      4.x.6)Data update procedures
5) Site-specific information for software users
   5.x) (Site name)
      5.x.1)Schedule
      5.x.2)Installation procedures
      5.x.3)Data update procedures
6) Notes

A) Annexes

1) **Scope** . This clause should be divided into the following subclauses.
   1.1) **Identification** . This subclause shall contain a full identification of the system and the software to which this document applies, including, as applicable, identification number(s), title(s), abbreviation(s), version number(s), and release number(s).
   1.2) **System overview** . This subclause shall briefly state the purpose of the system and the software to which this document applies. It shall describe the general nature of the system and software;

summarize the history of system development, operation, and maintenance; identify the project sponsor, acquirer, user, developer, and maintenance organizations; identify current and planned operating sites; and list other relevant documents.

1.3) **Document overview** . This subclause shall summarize the purpose and contents of this plan and shall describe any security or privacy protection considerations associated with its use.

1.4) **Relationship to other plans** . This subclause shall describe the relationship, if any, of the SIP to other project management plans.

2) **Referenced documents** . This clause shall list the number, title, revision, date, and source of all documents referenced in this manual.

3) **Installation overview** . This clause should be divided into the following subclauses to provide an overview of the installation process.

3.1) **Description** . This subclause shall provide a general description of the installation process to provide a frame of reference for the remainder of the document. A list of sites for software installation, the schedule dates, and the method of installation shall be included.

3.2) **Contact point** . This subclause shall provide the organizational name, department/division, and telephone number of a point of contact for questions relating to this installation.

3.3) **Support materials** . This subclause shall list the type, source, and quantity of support materials needed for the installation. Included shall be items such as magnetic tapes, disk packs, computer printer paper, and special forms.

3.4) **Training** . This subclause shall describe the developer's plans for training personnel who will operate and/or use the software installed at user sites. Included shall be the delineation between general orientation, classroom training, and "hands-on" training.

3.5) **Tasks** . This subclause shall list and describe in general terms each task involved in the software installation. Each task description shall identify the organization that will accomplish the task, usually either the user, computer operations, or the developer. The task list shall include such items as:

a) Providing overall planning, coordination, and preparation for installation
b) Providing personnel for the installation team
c) Arranging lodging, transportation, and office facilities for the installation team
d) Ensuring that all manuals applicable to the installation are available when needed
e) Ensuring that all other prerequisites have been fulfilled prior to the installation
f) Planning and conducting training activities
g) Providing students for the training
h) Providing computer support and technical assistance for the installation
i) Providing for conversion from the current system

3.6) **Personnel** . This subclause shall describe the number, type, and skill level of the personnel needed during the installation period, including the need for multishift operation, clerical support, etc.

3.7) **Security and privacy protection** . This subclause shall contain an overview of the security and privacy protection considerations associated with the system.

4) **Site-specific information for software center operations staff** . This clause applies if the software will be installed in computer center(s) or other centralized or networked software installations for users to access via terminals or using batch input/output. If this type of installation does not apply, this clause shall contain the words "Not applicable."

4.x) **(Site name)** . This subclause shall identify a site or set of sites and should be divided into the following to discuss those sites. Multiple sites may be discussed together when the information for those sites is generally the same.

4.x.1)**Schedule** . This subclause shall present a schedule of tasks to be accomplished during installation. It shall depict the tasks in chronological order with beginning and ending dates of each task and supporting narrative as necessary.

4.x.2)**Software inventory** . This subclause shall provide an inventory of the software needed to support the installation. The software shall be identified by name, identification number, version number, release number, configuration, and security classification, as applicable. This subclause shall indicate whether the software is expected to be on site or will be

delivered for the installation and shall identify any software to be used only to facilitate the installation process.

4.x.3)**Facilities** . This subclause shall detail the physical facilities and accommodations needed during the installation period. This description shall include the following, as applicable:

a) Classroom, work space, and training aids needed, specifying hours per day, number of days, and shifts
b) Hardware that is required to be operational and available
c) Transportation and lodging for the installation team

4.x.4)**Installation team** . This subclause shall describe the composition of the installation team. Each team member's tasks shall be defined.

4.x.5)**Installation procedures** . This subclause shall provide step-by-step procedures for accomplishing the installation. References may be made to other documents, such as operator manuals. Safety precautions, marked by WARNING or CAUTION, shall be included where applicable. The procedures shall include the following, as applicable:

a) Installing the software
b) Checking out the software once installed
c) Initializing databases and other software with site-specific data
d) Conversion from the current system, possibly involving running in parallel
e) Dry run of the procedures in operator and user manuals

4.x.6)**Data update procedures** . This subclause shall present the data update procedures to be followed during the installation period. When the data update procedures are the same as normal updating or processing procedures, reference may be made to other documents, such as operator manuals.

5) **Site-specific information for software users** . This clause shall provide installation planning pertinent to users of the software. When more than one type of user is involved, for example, users at different positions, performing different functions, or in different organizations, a separate clause (clauses 5 through n) may be written for each type of user and the clause titles modified to reflect each user.

5.x) **(Site name)** . This subclause shall identify a site or set of sites and should be divided into the following to discuss those sites. Multiple sites may be discussed together when the information for those sites is generally the same.

5.x.1)**Schedule** . This subclause shall present a schedule of tasks to be accomplished by the user during installation. It shall depict the tasks in chronological order including beginning and ending dates for each task and supporting narrative as necessary.

5.x.2)**Installation procedures** . This subclause shall provide step-by-step procedures for accomplishing the installation. Reference may be made to other documents, such as user manuals. Safety precautions, marked by WARNING or CAUTION, shall be included where applicable. The procedures shall include the following, as applicable:

a) Performing the tasks under 4.x.5 if not performed by operations staff
b) Initializing user-specific data
c) Setting up queries and other user inputs
d) Performing sample processing
e) Generating sample reports
f) Conversion from the current system, possibly involving running in parallel
g) Dry run of procedures in user manuals

5.x.3)**Data update procedures** . This subclause should be divided into subclauses to present the user's data update procedures to be followed during the installation period. When update procedures are the same as normal processing, reference may be made to other documents, such as user manuals, and to clause 4 of this document

6) **Notes** . This clause shall contain any general information that aids in understanding this document (e.g., background information, glossary, rationale). This clause shall include an alphabetical listing of all acronyms, abbreviations, and their meanings as used in this document and a list of terms and definitions needed to understand this document. If clause 5 has been expanded into clause(s) 6, ...n, this clause shall be numbered as the next clause following clause n.A.

A) **Annexes** . Annexes may be used to provide information published separately for convenience in document maintenance (e.g., charts, classified data). As applicable, each annex shall be referenced in the main body of the document where the data would normally have been provided. Annexes may be bound as separate documents for ease in handling. Annexes shall be lettered alphabetically (A, B, etc.).

E.2.4 Contents of the Software Transition Plan (STrP)

SOFTWARE TRANSITION PLAN (STrP)

Contents

1) Scope
   1.1) Identification
   1.2) System overview
   1.3) Document overview
   1.4) Relationship to other plans
2) Referenced documents
3) Software maintenance resources
   3.1) Facilities
   3.2) Hardware
   3.3) Software
   3.4) Other documentation
   3.5) Personnel
   3.6) Other resources
   3.7) Interrelationship of components
4) Recommended procedures
5) Training
6) Anticipated areas of change
7) Transition planning
8) Notes

A) Annexes

1) **Scope** This clause should be divided into the following subclauses.
   1.1) **Scope Identification** .This subclause shall contain a full identification of the system and the software to which this document applies, including, as applicable, identification number(s), title(s), abbreviation(s), version number(s), and release number(s).
   1.2) **System overview** .This subclause shall briefly state the purpose of the system and the software to which this document applies. It shall describe the general nature of the system and software; summarize the history of system development, operation, and maintenance; identify the project sponsor, acquirer, user, developer, and maintenance organizations; identify current and planned operating sites; and list other relevant documents.
   1.3) **Document overview** .This subclause shall summarize the purpose and contents of this document and shall describe any security or privacy protection considerations associated with its use.
   1.4) **Relationship to other plans** .This subclause shall describe the relationship, if any, of the STrP to other project management plans.
2) **Referenced documents** .This clause shall list the number, title, revision, date, and source of all documents referenced in this manual.
3) **Software maintenance resources** .This clause should be divided into subclauses to identify and describe the resources needed to maintain the deliverable software. These resources shall include items needed to control, copy, and distribute the software and its documentation, and to specify, design, implement, document, test, evaluate, control, copy, and distribute modifications to the software.

3.1) **Facilities** .This subclause shall describe the facilities needed to maintain the deliverable software. These facilities may include special buildings, rooms, mock-ups, building features such as raised flooring or cabling; building features to support security and privacy protection requirements (electromagnetic shielding, vaults, etc.), building features to support safety requirements (smoke alarms, safety glass, etc.), special power requirements, and so on. The purpose of each item shall be described. Diagrams may be included as applicable.

3.2) **Hardware** .This subclause shall identify and describe the hardware and associated documentation needed to maintain the deliverable software. This hardware may include computers, peripheral equipment, hardware simulators, stimulators, emulators, diagnostic equipment, and non-computer equipment. The description shall include:

a) Specific models, versions, and configurations
b) Rationale for the selected hardware
c) Reference to user/operator manuals or instructions for each item, as applicable
d) Identification of each hardware item and document as acquirer-furnished, an item that will be delivered to the maintenance organization, an item the maintenance organization is known to have, an item the maintenance organization is required to acquire, or other description of status
e) If items are required to be acquired, information about a current source of supply, including whether the item is currently available and whether it is expected to be available at the time of delivery
f) Information about manufacturer support, licensing, and usage and ownership rights, including whether the item is currently supported by the manufacturer, whether it is expected to be supported at the time of delivery, whether licenses will be assigned to the maintenance organization, and the terms of such licenses
g) Security and privacy protection considerations, limitations, or other items of interest

3.3) **Software** .This subclause shall identify and describe the software and associated documentation needed to maintain the deliverable software. This software may include computer-aided software engineering (CASE) tools, data in these tools, compilers, test tools, test data, simulations, emulations, utilities, configuration management tools, databases and data files, and other software. The description shall include:

a) Specific names, identification numbers, version numbers, release numbers, and configurations, as applicable
b) Rationale for the selected software
c) Reference to user/operator manuals or instructions for each item, as applicable
d) Identification of each item of software and document as acquirer-furnished, an item that will be delivered to the maintenance organization, an item the maintenance organization is known to have, an item the maintenance organization is required to acquire, or other description of status
e) If items are required to be acquired, information about a current source of supply, including whether the item is currently available and whether it is expected to be available at the time of delivery
f) Information about vendor support, licensing, and usage and ownership rights, including whether the item is currently supported by the vendor, whether it is expected to be supported at the time of delivery, whether licenses will be assigned to the maintenance organization, and the terms of such licenses
g) Security and privacy protection considerations, limitations, or other items of interest

3.4) **Other documentation** .This subclause shall identify any other documentation needed to maintain the deliverable software. The list will include, for example, plans, reports, studies, specifications, design descriptions, test cases/procedures, test reports, user/operator manuals, and maintenance manuals for the deliverable software. This subclause shall provide:

a) Names, identification numbers, version numbers, and release numbers, as applicable
b) Rationale for including each document in the list

c) Identification of each document as acquirer-furnished, an item that will be delivered to the maintenance organization, an item the maintenance organization is known to have, an item the maintenance organization is required to acquire, or other description of status
d) If a document is required to be acquired, information about where to acquire it
e) Information about licensing and usage and ownership rights
f) Security and privacy protection considerations, limitations, or other items of interest

3.5) **Personnel** .This subclause shall describe the personnel needed to maintain the deliverable software, including anticipated number of personnel, types and levels of skills and expertise, and security clearances. This subclause shall cite, as applicable, actual staffing on the development project as a basis for the staffing needs cited.

3.6) **Other resources** .This subclause shall identify any other resources needed to maintain the deliverable software. Included may be consumable such as magnetic tapes and diskettes, together with an estimate of the type and number that should be acquired.

3.7) **Interrelationship of components** .This subclause shall identify the interrelationships of the components identified in the preceding subclauses. A figure may be used to show the interrelationships.

4) **Recommended procedures** .This clause should be divided into subclauses as needed to describe any procedures, including advice and lessons learned, that the developer may wish to recommend to the maintenance organization for maintaining the deliverable software and associated maintenance environment.

5) **Training** .This clause should be divided into subclauses as appropriate to describe the developer's plans for training maintenance personnel to maintain the deliverable software. This clause shall include:
a) The schedule, duration, and location for the training
b) The delineation between classroom training and "hands-on" training
c) Provision (either directly or by reference) for:
1) Familiarization with the operational software and target computer(s)
2) Familiarization with the maintenance software and host system

6) **Anticipated areas of change** .This clause shall describe anticipated areas of change to the deliverable software.

7) **Transition planning.** This clause should be divided into subclauses as needed to describe the developer's plans for transitioning the deliverable software to the maintenance organization. This clause shall address the following:
a) All activities to be performed to transition the deliverable software to the maintenance organization. These activities may include planning/coordination meetings; preparation of items to be delivered to the maintenance organization; packaging, shipment, installation, and checkout of the software maintenance environment; packaging, shipment, installation, and checkout of the operational software; and training of maintenance personnel.
b) Roles and responsibilities for each activity
c) The resources needed to carry out the transition activities and the source from which each resource will be provided
d) Schedules and milestones for conducting the transition activities. These schedules and milestones shall be compatible with the contract master schedule.
e) Procedures for installation and checkout of deliverable items in the maintenance environment

8) **Notes** .This clause shall contain any general information that aids in understanding this document (e.g., background information, glossary, rationale). This clause shall include an alphabetical listing of all acronyms, abbreviations, and their meanings as used in this document and a list of any terms and definitions needed to understand this document.

A) **Annexes** . Annexes may be used to provide information published separately for convenience in document maintenance (e.g., charts, classified data). As applicable, each annex shall be referenced in the main body of the document where the data would normally have been provided. Annexes may be bound as separate documents for ease in handling. Annexes shall be lettered alphabetically (A, B, etc.).

Annex F

(normative)

Concept and requirements software product descriptions

F.1 Scope

This annex specifies the contents of software products associated with concept description and requirements specification in this standard. It applies regardless of whether the software products are deliverable. This annex is a normative (that is, binding) part of this standard, subject to tailoring.

F.2 Software products covered

This following subclauses describe the contents of the software products covered by this annex. The products are listed in the order they are referenced in this standard and include the following:

a) Operational Concept Description (OCD)
b) System/Subsystem Specification (SSS)
c) Interface Requirements Specification (IRS)
d) Software Requirements Specification (SRS)

F.2.1 Contents of the Operational Concept Description (OCD)

OPERATIONAL CONCEPT DESCRIPTION (OCD)

Contents

1) Scope
   1.1) Identification
   1.2) System overview
   1.3) Document overview
2) Referenced documents
3) Current system or situation
   3.1) Background, objectives, and scope
   3.2) Operational policies and constraints
   3.3) Description of current system or situation
   3.4) Users or involved personnel
   3.5) Support strategy
4) Justification for and nature of changes
   4.1) Justification for change
   4.2) Description of needed changes
   4.3) Priorities among the changes
   4.4) Changes considered but not included
   4.5) Assumptions and constraints
5) Concept for a new or modified system

5.1) Background, objectives, and scope
5.2) Operational policies and constraints
5.3) Description of the new or modified system
5.4) Users/affected personnel
5.5) Support strategy
6) Operational scenarios
7) Summary of impacts
7.1) Operational impacts
7.2) Organizational impacts
7.3) Impacts during development
8) Analysis of the proposed system
8.1) Summary of advantages
8.2) Summary of disadvantages/limitations
8.3) Alternatives and trade-offs considered
9) Notes
A) Annexes
1) **Scope** . This clause should be divided into the following subclauses.
1.1) **Identification** . This subclause shall contain a full identification of the system to which this document applies, including, as applicable, identification number(s), title(s), abbreviations), version number(s), and release number(s).
1.2) **System overview** . This subclause shall briefly state the purpose of the system to which this document applies. It shall describe the general nature of the system; summarize the history of system development, operation, and maintenance; identify the project sponsor, acquirer, user, developer, and maintenance organizations; identify current and planned operating sites; and list other relevant documents.
1.3) **Document overview** . This subclause shall summarize the purpose and contents of this document and shall describe any security or privacy protection considerations associated with its use.
2) **Referenced documents** . This clause shall list the number, title, revision, date, and source of all documents referenced in this manual.
3) **Current system or situation** . This clause should be divided into the following subclauses to describe the system or situation as it currently exists.
3.1) **Back-ground, objectives, and scope** . This subclause shall describe the background, mission or objectives, and scope of the current system or situation.
3.2) **Operational policies and constraints** . This subclause shall describe any operational policies and constraints that apply to the current system or situation.
3.3) **Description of current system or situation** . This subclause shall provide a description of the current system or situation, identifying differences associated with different states or modes of operation (for example, regular, maintenance, training, degraded, emergency, alternative-site, wartime, peacetime). The distinction between states and modes is arbitrary. A system may be described in terms of states only, modes only, states within modes, modes within states, or any other scheme that is useful. If the system operates without states or modes, this subclause shall so state, without the need to create artificial distinctions. The description shall include, as applicable:
a) The operational environment and its characteristics
b) Major system components and the interconnections among these components
c) Interfaces to external systems or procedures
d) Capabilities/functions of the current system
e) Charts and accompanying descriptions depicting input, output, data flow, and manual and automated processes sufficient to understand the current system or situation from the user's point of view
f) Performance characteristics, such as speed, throughput, volume, frequency
g) Quality attributes, such as reliability, maintainability, availability, flexibility, portability, usability, efficiency

h) Provisions for safety, security, privacy protection, and continuity of operations in emergencies

3.4) **Users or involved personnel** . This subclause shall describe the types of users of the system, or personnel involved in the current situation, including, as applicable, organizational structures, training/skills, responsibilities, activities, and interactions with one another.

3.5) **Support strategy** . This subclause shall provide an overview of the support strategy for the current system, including, as applicable to this document, maintenance organization(s); facilities; equipment; maintenance software; repair/replacement criteria; maintenance levels and cycles; and storage, distribution, and supply methods.

4) **Justification for and nature of changes** . This clause should be divided into the following subclauses.

4.1) **Justification for change** . This subclause shall:

a) Describe new or modified aspects of user needs, threats, missions, objectives, environments, interfaces, personnel or other factors that require a new or modified system

b) Summarize deficiencies or limitations in the current system or situation that make it unable to respond to these factors

4.2) **Description of needed changes** . This subclause shall summarize new or modified capabilities/functions, processes, interfaces, or other changes needed to respond to the factors identified in 4.1.

4.3) **Priorities among the changes** . This subclause shall identify priorities among the needed changes. It shall, for example, identify each change as essential, desirable, or optional, and prioritize the desirable and optional changes.

4.4) **Changes considered but not included** . This subclause shall identify changes considered but not included in 4.2, and rationale for not including them.

4.5) **Assumptions and constraints** . This subclause shall identify any assumptions and constraints applicable to the changes identified in this clause.

5) **Concept for a new or modified system** . This clause should be divided into the following subclauses to describe a new or modified system.

5.1) **Background, objectives, and scope** . This subclause shall describe the background, mission or objectives, and scope of the new or modified system.

5.2) **Operational policies and constraints** . This subclause shall describe any operational policies and constraints that apply to the new or modified system.

5.3) **Description of the new or modified system** . This subclause shall provide a description of the new or modified system, identifying differences associated with different states or modes of operation (for example, regular, maintenance, training, degraded, emergency, alternative-site, wartime, peacetime). The distinction between states and modes is arbitrary. A system may be described in terms of states only, modes only, states within modes, modes within states, or any other scheme that is useful. If the system operates without states or modes, this subclause shall so state, without the need to create artificial distinctions. The description shall include, as applicable:

a) The operational environment and its characteristics

b) Major system components and the interconnections among these components

c) Interfaces to external systems or procedures

d) Capabilities/functions of the new or modified system

e) Charts and accompanying descriptions depicting input, output, data flow, and manual and automated processes sufficient to understand the new or modified system or situation from the user's point of view

f) Performance characteristics, such as speed, throughput, volume, frequency

g) Quality attributes, such as reliability, maintainability, availability, flexibility, portability, usability, efficiency

h) Provisions for safety, security, privacy protection, and continuity of operations in emergencies

5.4) **Users/affected personnel** . This subclause shall describe the types of users of the new or modified system, including, as applicable, organizational structures, training/skills, responsibilities, and interactions with one another.

5.5) **Support strategy** . This subclause shall provide an overview of the support strategy for the new or modified system, including, as applicable, maintenance organizations); facilities; equipment; maintenance software; repair/replacement criteria; maintenance levels and cycles; and storage, distribution, and supply methods.

6) **Operational scenarios** . This clause shall describe one or more operational scenarios that illustrate the role of the new or modified system, its interaction with users, its interface to other systems, and all states or modes identified for the system. The scenarios shall include events, actions, stimuli, information, interactions, etc., as applicable. Reference may be made to other media, such as videos, to provide part or all of this information.

7) **Summary of impacts** . This clause should be divided into the following subclauses.

7.1) **Operational impacts** . This subclause shall describe anticipated operational impacts on the user, acquirer, developer, and maintenance organizations. These impacts may include changes in interfaces with computer operating centers; change in procedures; use of new data sources; changes in quantity, type, and timing of data to be input to the system; changes in data retention requirements; and new modes of operation based on peacetime, alert, wartime, or emergency conditions.

7.2) **Organizational impacts** . This subclause shall describe anticipated organizational impacts on the user, acquirer, developer, and maintenance organizations. These impacts may include modification of responsibilities; addition or elimination of responsibilities or positions; need for training or retraining; and changes in number, skill levels, position identifiers, or location of personnel in various modes of operation.

7.3) **Impacts during development** . This subclause shall describe anticipated impacts on the user, acquirer, developer, and maintenance organizations during the development effort. These impacts may include meetings/discussions regarding the new system; development or modification of databases; training; parallel operation of the new and existing systems; impacts during testing of the new system; and other activities needed to aid or monitor development.

8) **Analysis of the proposed system** . This clause should be divided into the following subclauses.

8.1) **Summary of advantages** . This subclause shall provide a qualitative and quantitative summary of the advantages to be obtained from the new or modified system. This summary shall include new capabilities, enhanced capabilities, and improved performance, as applicable, and their relationship to deficiencies identified in 4.1.

8.2) **Summary of disadvantages/limitations** . This subclause shall provide a qualitative and quantitative summary of disadvantages or limitations of the new or modified system. These disadvantages and limitations shall include, as applicable, degraded or missing capabilities, degraded or less-than-desired performance, greater-than-desired use of computer hardware resources, undesirable operational impacts, conflicts with user assumptions, and other constraints.

8.3) **Alternatives and trade-offs considered** . This subclause shall identify and describe major alternatives considered to the system or its characteristics, the trade-offs among them, and rationale for the decisions reached.

9) **Notes** . This clause shall contain any general information that aids in understanding this document (e.g., background information, glossary, rationale). This clause shall include an alphabetical listing of all acronyms, abbreviations, and their meanings as used in this document and a list of any terms and definitions needed to understand this document.

A) **Annexes** . Annexes may be used to provide information published separately for convenience in document maintenance (e.g., charts, classified data). As applicable, each annex shall be referenced in the main body of the document where the data would normally have been provided. Annexes may be bound as separate documents for ease in handling. Annexes shall be lettered alphabetically (A, B, etc.).

F.2.2 Contents of the System/Subsystem Specification (SSS)

SYSTEM/SUBSYSTEM SPECIFICATION (SSS)

Contents

1) Scope
   1.1) Identification
   1.2) System overview
   1.3) Document overview
2) Referenced documents
3) Requirements
   3.1) Required states and modes
   3.2) System capability requirements
      3.2.x)(System capability)
   3.3) System external interface requirements
      3.3.1)Interface identification and diagrams
      3.3.2)(Project-unique identifier of interface)
   3.4) System internal interface requirements
   3.5) System internal data requirements
   3.6) Adaptation requirements
   3.7) Safety requirements
   3.8) Security and privacy protection requirements
   3.9) System environment requirements
   3.10)Computer resource requirements
      3.10.1)Computer hardware requirements
      3.10.2)Computer hardware resource utilization requirements
      3.10.3)Computer software requirements
      3.10.4)Computer communications requirements
   3.11)System quality factors
   3.12)Design and construction constraints
   3.13)Personnel-related requirements
   3.14)Training-related requirements
   3.15)Logistics-related requirements
   3.16)Other requirements
   3.17)Packaging requirements
   3.18)Precedence and criticality of requirements
4) Qualification provisions
5) Requirements traceability
6) Notes

A) Annexes

1) **Scope** .This clause should be divided into the following subclauses.
   1.1) **Identification** .This subclause shall contain a full identification of the system to which this document applies, including, as applicable, identification number(s), title(s), abbreviation(s), version number(s), and release number(s).
   1.2) **System overview** .This subclause shall briefly state the purpose of the system to which this document applies. It shall describe the general nature of the system; summarize the history of system development, operation, and maintenance; identify the project sponsor, acquirer, user, developer, and maintenance organizations; identify current and planned operating sites; and list other relevant documents.
   1.3) **Document overview** .This subclause shall summarize the purpose and contents of this document and shall describe any security or privacy protection considerations associated with its use.

2) **Referenced documents** .This clause shall list the number, title, revision, date, and source of all documents referenced in this manual.

3) **Requirements** .This clause should be divided into the following subclauses to specify the system requirements, that is, those characteristics of the system that are conditions for its acceptance. Each requirement shall be assigned a project-unique identifier to support testing and traceability and shall be stated in such a way that an objective test can be defined for it. Each requirement shall be annotated with associated qualification method(s) (see clause 4) and, for subsystems, traceability to system requirements (see 5.a), if not provided in those clauses. The degree of detail to be provided shall be guided by the following rule: include those characteristics of the system that are conditions for system acceptance; defer to design descriptions those characteristics that the acquirer is willing to leave up to the developer. If there are no requirements in a given subclause, the subclause shall so state. If a given requirement fits into more than one subclause, it may be stated once and referenced from the other subclauses. Conventions needed to understand the requirements shall be presented or referenced.

   3.1) **Required states and modes** .If the system is required to operate in more than one state or mode having requirements distinct from other states or modes, this subclause shall identify and define each state and mode. Examples of states and modes include: idle, ready, active, post-use analysis, training, degraded, emergency, backup, wartime, peacetime. The distinction between states and modes is arbitrary. A system may be described in terms of states only, modes only, states within modes, modes within states, or any other scheme that is useful. If no states or modes are required, this subclause shall so state, without the need to create artificial distinctions. If states and/or modes are required, each requirement or group of requirements in this specification shall be correlated to the states and modes. The correlation may be indicated by a table or other method in this subclause, in an annex referenced from this subclause, or by annotation of the requirements in the subclauses where they appear.

   3.2) **System capability requirements** .This subclause should be divided into subclauses to itemize the requirements associated with each capability of the system. A “capability” is defined as a group of related requirements. The word “capability” may be replaced with “function,” “subject,” “object,” or other term useful for presenting the requirements.

      3.2.x)**(System capability)** .This subclause shall identify a required system capability and shall itemize the requirements associated with the capability. If the capability can be more clearly specified by dividing it into constituent capabilities, the constituent capabilities shall be specified in subclauses. The requirements shall specify required behavior of the system and shall include applicable parameters, such as response times, throughput times, other timing constraints, sequencing, accuracy, capacities (how much/how many), priorities, continuous operation requirements, and allowable deviations based on operating conditions. The requirements shall include, as applicable, required behavior under unexpected, unallowed, or “out of bounds” conditions, requirements for error handling, and any provisions to be incorporated into the system to provide continuity of operations in the event of emergencies. Subclause 3.3.x of the SSS provides a list of topics to be considered when specifying requirements regarding input the system is required to accept and output it is required to produce.

   3.3) **System external interface requirements** .This subclause should be divided into subclauses to specify the requirements, if any, for the system’s external interfaces. This subclause may reference one or more Interface Requirements Specifications (IRSs) or other documents containing these requirements.

      3.3.1)**Interface identification and diagrams** .This subclause shall identify the required external interfaces of the system. The identification of each interface shall include a project-unique identifier and shall designate the interfacing entities (systems, hardware items, software items, users, etc.) by name, number, version, and documentation references, as applicable. The identification shall state which entities have fixed interface characteristics (and therefore impose interface requirements on interfacing entities) and which are being developed or modified (thus having interface requirements imposed on them). One or more interface diagrams shall be provided to depict the interfaces.

3.3.2)(**Project-unique identifier of interface)** .This subclause (beginning with 3.3.2) shall identify a system external interface by project-unique identifier, shall briefly identify the interfacing entities, and should be divided into subclauses as needed to state the requirements imposed on the system to achieve the interface. Interface characteristics of the other entities involved in the interface shall be stated as assumptions or as "When [the entity not covered] does this, the system shall ...," not as requirements on the other entities. This subclause may reference other documents (such as data dictionaries, standards for communication protocols, and standards for user interfaces) in place of stating the information here. The requirements shall include the following, as applicable, presented in any order suited to the requirements, and shall note any differences in these characteristics from the point of view of the interfacing entities (such as different expectations about the size, frequency, or other characteristics of data elements):

a) Priority that the system is required to assign the interface
b) Requirements on the type of interface (such as real-time data transfer, storage-and-retrieval of data, etc.) to be implemented
c) Required characteristics of individual data elements that the system is required to provide, store, send, access, receive, etc., such as:

1) Names/identifiers
a) Project-unique identifier
b) Non-technical (natural language) name
c) Standard data element name
d) Technical name (e.g., variable or field name in code or database)
e) Abbreviation or synonymous names
2) Data type (alphanumeric, integer, etc.)
3) Size and format (such as length and punctuation of a character string)
4) Units of measurement (such as meters, dollars, nanoseconds)
5) Range or enumeration of possible values (such as 0-99)
6) Accuracy (how correct) and precision (number of significant digits)
7) Priority, timing, frequency, volume, sequencing, and other constraints, such as whether the data element may be updated and whether business rules apply
8) Security and privacy protection constraints
9) Sources (setting/sending entities) and recipients (using/receiving entities)

d) Required characteristics of data element assemblies (records, messages, files, arrays, displays, reports, etc.) that the system is required to provide, store, send, access, receive, etc., such as:

1) Names/identifiers
a) Project-unique identifier
b) Non-technical (natural language) name
c) Technical name (e.g., record or data structure name in code or database)
d) Abbreviations or synonymous names
2) Data elements in the assembly and their structure (number, order, grouping)
3) Medium (such as disk) and structure of data elements/assemblies on the medium
4) Visual and auditory characteristics of displays and other outputs (such as colors, layouts, fonts, icons and other display elements, beeps, lights)
5) Relationships among assemblies, such as sorting/access characteristics
6) Priority, timing, frequency, volume, sequencing, and other constraints, such as whether the assembly may be updated and whether business rules apply
7) Security and privacy protection constraints
8) Sources (setting/sending entities) and recipients (using/receiving entities)

e) Required characteristics of communication methods that the system is required to use for the interface, such as:

1) Project-unique identifiers)
2) Communication links/bands/frequencies/media and their characteristics
3) Message formatting

4) Flow control (such as sequence numbering and buffer allocation)
5) Data transfer rate, whether periodic/periodic, and interval between transfers
6) Routing, addressing, and naming conventions
7) Transmission services, including priority and grade
8) Safety/security/privacy protection considerations, such as encryption, user authentication, compartmentalization, and auditing

f) Required characteristics of protocols the system is required to use for the interface, such as:

1) Project-unique identifier(s)
2) Priority/layer of the protocol
3) Packeting, including fragmentation and reassembly, routing, and addressing
4) Legality checks, error control, and recovery procedures
5) Synchronization, including connection establishment, maintenance, termination
6) Status, identification, and any other reporting features

g) Other required characteristics, such as physical compatibility of the interfacing entity(ies) (dimensions, tolerances, loads, voltages, plug compatibility, etc.)

3.4) **System internal interface requirements** .This subclause shall specify the requirements, if any, imposed on interfaces internal to the system. If all internal interfaces are left to the design or to requirement specifications for system components, this fact shall be so stated. If such requirements are to be imposed, subclause 3.3 of the SSS provides a list of topics to be considered.

3.5) **System internal data requirements** .This subclause shall specify the requirements, if any, imposed on data internal to the system. Included shall be requirements, if any, on databases and data files to be included in the system. If all decisions about internal data are left to the design or to requirements specifications for system components, this fact shall be so stated. If such requirements are to be imposed, subclauses 3.3.x.c and 3.3.x.d of the SSS provide a list of topics to be considered.

3.6) **Adaptation requirements** .This subclause shall specify the requirements, if any, concerning installation-dependent data that the system is required to provide (such as site-dependent latitude and longitude or site-dependent state tax codes) and parameters that the system is required to use that may vary according to operational needs (such as operation-dependent targeting constants or site-dependent month-end dates).

3.7) **Safety requirements** .This subclause shall specify the system requirements, if any, concerned with preventing or minimizing unintended hazards to personnel, property, and the physical environment. Examples include restricting the use of dangerous materials; classifying explosives for purposes of shipping, handling, and storing; abort/escape provisions from enclosures; gas detection and warning devices; grounding of electrical systems; decontamination; and explosion proofing. This subclause shall include the system requirements, if any, for nuclear components, including, as applicable, requirements for component design, prevention of inadvertent detonation, and compliance with nuclear safety rules.

3.8) **Security and privacy protection requirements** .This subclause shall specify the system requirements, if any, concerned with maintaining security and privacy protection. The requirements shall include, as applicable, the security/privacy protection environment in which the system is required to operate, the type and degree of security or privacy protection to be provided, the security/privacy protection risks the system is required to withstand, required safeguards to reduce those risks, the security/privacy protection policy that is required to be met, the security/privacy protection accountability the system is required to provide, and the criteria that are required to be met for security/privacy protection certification/accreditation.

3.9) **System environment requirements** .This subclause shall specify the requirements, if any, regarding the environment in which the system is required to operate. Examples for a software system are the computer hardware and operating system on which the software is required to run. (Additional requirements concerning computer resources are given in the next subclause). Examples for a hardware-software system include the environmental conditions that the system is required to withstand during transportation, storage, and operation, such as conditions in the natural environment (wind, rain, temperature, geographic location), the induced environment

(motion, shock, noise, electromagnetic radiation), and environments due to hostile action (explosions, radiation).

3.10) **Computer resource requirements** .This subclause should be divided into the following. Depending upon the nature of the system, the computer resources covered in these subclauses may constitute the environment of the system (as for a software system) or components of the system (as for a hardware-software system).

3.10.1) **Computer hardware requirements** .This subclause shall specify the requirements, if any, regarding computer hardware that is required to be used by, or incorporated into, the system. The requirements shall include, as applicable, number of each type of equipment, type, size, capacity, and other required characteristics of processors, memory, input/output devices, auxiliary storage, communications/network equipment, and other required equipment.

3.10.2) **Computer hardware resource utilization requirements** .This subclause shall specify the requirements, if any, on the system's computer hardware resource utilization, such as maximum allowable use of processor capacity, memory capacity, input/output device capacity, auxiliary storage device capacity, and communications/network equipment capacity. The requirements (stated, for example, as percentages of the capacity of each computer hardware resource) shall include the conditions, if any, under which the resource utilization is to be measured.

3.10.3) **Computer software requirements** .This subclause shall specify the requirements, if any, regarding computer software that is required to be used by, or incorporated into, the system. Examples include operating systems, database management systems, communications/ network software, utility software, input and equipment simulators, test software, and manufacturing software. The correct nomenclature, version, and documentation references of each such item of software shall be provided.

3.10.4) **Computer communications requirements** .This subclause shall specify the additional requirements, if any, concerning the computer communications that are required to be used by, or incorporated into, the system. Examples include geographic locations to be linked; configuration and network topology; transmission techniques; data transfer rates; gateways; required system use times; type and volume of data to be transmitted/received; time boundaries for transmission/reception/response; peak volumes of data; and diagnostic features.

3.11) **System quality factors** .This subclause shall specify the requirements, if any, pertaining to system quality factors. Examples include quantitative requirements concerning system functionality (the ability to perform all required functions), reliability (the ability to perform with correct, consistent results — such as mean time between failure for equipment), maintainability (the ability to be easily serviced, repaired, or corrected), availability (the ability to be accessed and operated when needed), flexibility (the ability to be easily adapted to changing requirements), portability of software (the ability to be easily modified for a new environment), reusability (the ability to be used in multiple applications), testability (the ability to be easily and thoroughly tested), usability (the ability to be easily learned and used), and other attributes.

3.12) **Design and construction constraints** .This subclause shall specify the requirements, if any, that constrain the design and construction of the system. For hardware-software systems, this subclause shall include the physical requirements imposed on the system. These requirements may be specified by reference to appropriate commercial or government standards and specifications. Examples include requirements concerning:

a) Use of a particular system architecture or requirements on the architecture, such as required subsystems; use of standard, military, or existing components; or use of acquirer-furnished property (equipment, information, or software)

b) Use of particular design or construction standards; use of particular data standards; use of a particular programming language; workmanship requirements and production techniques

c) Physical characteristics of the system (such as weight limits, dimensional limits, color, protective coatings); interchangeability of parts; ability to be transported from one location to another; ability to be carried or set up by one, or a given number of, persons
d) Materials that can and cannot be used; requirements on the handling of toxic materials; limits on the electromagnetic radiation that the system is permitted to generate
e) Use of nameplates, part marking, serial and lot number marking, and other identifying markings
f) Flexibility and expandability that are required to be provided to support anticipated areas of growth or changes in technology, threat, or mission

3.13) **Personnel-related requirements** .This subclause shall specify the system requirements, if any, included to accommodate the number, skill levels, duty cycles, training needs, or other information about the personnel who will use or support the system. Examples include requirements for the number of work stations to be provided and for built-in help and training features. Also included shall be the human factors engineering requirements, if any, imposed on the system. These requirements shall include, as applicable, considerations for the capabilities and limitations of humans, foreseeable human errors under both normal and extreme conditions, and specific areas where the effects of human error would be particularly serious. Examples include requirements for adjustable-height work stations, color and duration of error messages, physical placement of critical indicators or buttons, and use of auditory signals.

3.14) **Training-related requirements** .This subclause shall specify the system requirements, if any, pertaining to training. Examples include training devices and training materials to be included in the system.

3.15) **Logistics-related requirements** .This subclause shall specify the system requirements, if any, concerned with logistics considerations. These considerations may include: system maintenance, software maintenance, system transportation modes, supply-system requirements, impact on existing facilities, and impact on existing equipment.

3.16) **Other requirements** .This subclause shall specify additional system requirements, if any, not covered in the previous subclauses. Examples include requirements for system documentation, such as specifications, drawings, technical manuals, test plans and procedures, and installation instruction data, if not covered in other contractual documents.

3.17) **Packaging requirements** .This clause shall specify the requirements, if any, for packaging, labeling, and handling the system and its components for delivery. Applicable commercial or government specifications and standards may be referenced if appropriate.

3.18) **Precedence and criticality of requirements** .This subclause shall specify, if applicable, the order of precedence, criticality, or assigned weights indicating the relative importance of the requirements in this specification. Examples include identifying those requirements deemed critical to safety, to security, or to privacy protection for purposes of singling them out for special treatment. If all requirements have equal weight, this subclause shall so state.

4) **Qualification provisions** .This clause shall define a set of qualification methods and shall specify for each requirement in clause 3 the method(s) to be used to ensure that the requirement has been met. A table may be used to present this information, or each requirement in clause 3 may be annotated with the method(s) to be used. Qualification methods may include:

a) Demonstration: The operation of the system, or a part of the system, that relies on observable functional operation not requiring the use of instrumentation, special test equipment, or subsequent analysis.
b) Test: The operation of the system, or a part of the system, using instrumentation or other special test equipment to collect data for later analysis.
c) Analysis: The processing of accumulated data obtained from other qualification methods. Examples are reduction, interpolation, or extrapolation of test results.
d) Inspection: The visual examination of system components, documentation, etc.
e) Special qualification methods: Any special qualification methods for the system, such as special tools, techniques, procedures, facilities, acceptance limits, use of standard samples, preprocessing or periodic production samples, pilot models, or pilot lots.

5) **Requirements traceability** .For system-level specifications, this subclause does not apply. For subsystem-level specifications, this subclause shall contain:
   a) Traceability from each subsystem requirement in this specification to the system requirements it addresses. (Alternatively, this traceability may be provided by annotating each requirement in clause 3.)Note: Each level of system refinement may result in requirements not directly traceable to higher-level requirements. For example, a system architectural design that creates two subsystems may result in requirements about how the subsystems will interface, even though these interfaces are not covered in system requirements. Such requirements may be traced to a general requirement such as "system implementation" or to the system design decisions that resulted in their generation.
   b) Traceability from each system requirement that has been allocated to the subsystem covered by this specification to the subsystem requirements that address it. All system requirements allocated to the subsystem shall be accounted for. Those that trace to subsystem requirements contained in IRSs shall reference those IRSs.

6) **Notes** .This clause shall contain any general information that aids in understanding this document (e.g., background information, glossary, rationale). This clause shall contain an alphabetical listing of all acronyms, abbreviations, and their meanings as used in this document and a list of any terms and definitions needed to understand this document.

A) **Annexes** . Annexes may be used to provide information published separately for convenience in document maintenance (e.g., charts, classified data). As applicable, each annex shall be referenced in the main body of the document where the data would normally have been provided. Annexes may be bound as separate documents for ease in handling. Annexes shall be lettered alphabetically (A, B, etc.).

F.2.3 Contents of the Interface Requirements Specification (IRS)

INTERFACE REQUIREMENTS SPECIFICATION (IRS)

Contents

1) Scope
   1.1) Identification
   1.2) System overview
   1.3) Document overview
2) Referenced documents
3) Requirements
   3.1) Interface identification and diagrams
   3.2) (Project-unique identifier of interface)
   3.3) Precedence and criticality of requirements
4) Qualification provisions
5) Requirements traceability
6) Notes

A) Annexes

1) **Scope** .This clause should be divided into the following subclauses.
   1.1) **Identification** .This subclause shall contain a full identification of the interfacing entities (systems, subsystems, hardware items, software items, manual operations, or other system components) and the interfaces to which this document applies, including, as applicable, identification number(s), title(s), abbreviations), version number(s), and release number(s).
   1.2) **System overview** .This subclause shall briefly state the purpose of the system(s) and software to which this document applies. It shall describe the general nature of the system and software; summarize the history of system development, operation, and maintenance; identify the project sponsor, acquirer, user, developer, and maintenance organizations; identify current and planned operating sites; and list other relevant documents.

1.3) **Document overview** .This subclause shall summarize the purpose and contents of this document and shall describe any security or privacy protection considerations associated with its use.

2) **Referenced documents** .This clause shall list the number, title, revision, date, and source of all documents referenced in this manual.

3) **Requirements** .This clause should be divided into the following subclauses to specify the requirements imposed on one or more systems, subsystems, hardware items, software items, manual operations, or other system components to achieve one or more interfaces among these entities. Each requirement shall be assigned a project-unique identifier to support testing and traceability and shall be stated in such a way that an objective test can be defined for it. Each requirement shall be annotated with associated qualification method(s) (see clause 4) and traceability to system (or subsystem, if applicable) requirements (see 5.a) if not provided in those clauses. The degree of detail to be provided shall be guided by the following rule: include those characteristics of the interfacing entities that are conditions for their acceptance; defer to design descriptions those characteristics that the acquirer is willing to leave up to the developer. If a given requirement fits into more than one subclause, it may be stated once and referenced from the other subclauses. If an interfacing entity included in this specification will operate in states and/or modes having interface requirements different from other states and modes, each requirement or group of requirements for that entity shall be correlated to the states and modes. The correlation may be indicated by a table or other method in this subclause, in an annex referenced from this subclause, or by annotation of the requirements in the subclauses where they appear. Conventions needed to understand the requirements shall be presented or referenced.

3.1) **Interface identification and diagrams** .For each interface identified in 1.1, this subclause shall include a project-unique identifier and shall designate the interfacing entities (systems, hardware items, software items, users, etc.) by name, number, version, and documentation references, as applicable. The identification shall state which entities have fixed interface characteristics (and therefore impose interface requirements on interfacing entities) and which are being developed or modified (thus having interface requirements imposed on them). One or more interface diagrams shall be provided to depict the interfaces.

3.x) **(Project-unique identifier of interface)** .This subclause (beginning with 3.2) shall identify an interface by project-unique identifier, shall briefly identify the interfacing entities, and should be divided as needed to state the requirements imposed on one or more of the interfacing entities to achieve the interface. If the interface characteristics of an entity are not covered by this IRS but need to be mentioned to specify the requirements for entities that are, those characteristics shall be stated as assumptions or as "When [the entity not covered] does this, the [entity being specified] shall ...," rather than as requirements on the entities not covered by this IRS. This subclause may reference other documents (such as data dictionaries, standards for communication protocols, and standards for user interfaces) in place of stating the information here. The requirements shall include the following, as applicable, presented in any order suited to the requirements, and shall note any differences in these characteristics from the point of view of the interfacing entities (such as different expectations about the size, frequency, or other characteristics of data elements):

a) Priority that the interfacing entity(ies) is required to assign the interface

b) Requirements on the type of interface (such as real-time data transfer, storage-and-retrieval of data, etc.) to be implemented

c) Required characteristics of individual data elements that the interfacing entity(ies) is required to provide, store, send, access, receive, etc., such as:

1) Names/identifiers

a) Project-unique identifier

b) Non-technical (natural language) name

c) Standard data element name

d) Technical name (e.g., variable or field name in code or database)

e) Abbreviation or synonymous names

2) Data type (alphanumeric, integer, etc.)

3) Size and format (such as length and punctuation of a character string)
4) Units of measurement (such as meters, dollars, nanoseconds)
5) Range or enumeration of possible values (such as 0–99)
6) Accuracy (how correct) and precision (number of significant digits)
7) Priority, timing, frequency, volume, sequencing, and other constraints, such as whether the data element may be updated and whether business rules apply
8) Security and privacy protection constraints
9) Sources (setting/sending entities) and recipients (using/receiving entities)

d) Required characteristics of data element assemblies (records, messages, files, arrays, displays, reports, etc.) that the interfacing entity(ies) is required to provide, store, send, access, receive, etc., such as:

1) Names/identifiers
a) Project-unique identifier
b) Non-technical (natural language) name
c) Technical name (e.g., record or data structure name in code or database)
d) Abbreviations or synonymous names
2) Data elements in the assembly and their structure (number, order, grouping)
3) Medium (such as disk) and structure of data elements/assemblies on the medium
4) Visual and auditory characteristics of displays and other outputs (such as colors, layouts, fonts, icons and other display elements, beeps, lights)
5) Relationships among assemblies, such as sorting/access characteristics
6) Priority, timing, frequency, volume, sequencing, and other constraints, such as whether the assembly may be updated and whether business rules apply
7) Security and privacy protection constraints
8) Sources (setting/sending entities) and recipients (using/receiving entities)

e) Required characteristics of communication methods that the interfacing entity(ies) is required to use for the interface, such as:

1) Project-unique identifier(s)
2) Communication links/bands/frequencies/media and their characteristics
3) Message formatting
4) Flow control (such as sequence numbering and buffer allocation)
5) Data transfer rate, whether periodic/aperiodic, and interval between transfers
6) Routing, addressing, and naming conventions
7) Transmission services, including priority and grade
8) Safety/security/privacy protection considerations, such as encryption, user authentication, compartmentalization, and auditing

f) Required characteristics of protocols the interfacing entity(ies) is required to use for the interface, such as:

1) Project-unique identifier(s)
2) Priority/layer of the protocol
3) Packeting, including fragmentation and reassembly, routing, and addressing
4) Legality checks, error control, and recovery procedures
5) Synchronization, including connection establishment, maintenance, termination
6) Status, identification, and any other reporting features

g) Other required characteristics, such as physical compatibility of the interfacing entity(ies) (dimensions, tolerances, loads, voltages, plug compatibility, etc.)

3.y) **Precedence and criticality of requirements** .This subclause shall be numbered as the last subclause in clause 3 and shall specify, if applicable, the order of precedence, criticality, or assigned weights indicating the relative importance of the requirements in this specification. Examples include identifying those requirements deemed critical to safety, to security, or to privacy protection for purposes of singling them out for special treatment. If all requirements have equal weight, this subclause shall so state.

4) **Qualification provisions** .This clause shall define a set of qualification methods and shall specify, for each requirement in clause 3, the qualification method(s) to be used to ensure that the require-

ment has been met. A table may be used to present this information, or each requirement in clause 3 may be annotated with the method(s) to be used. Qualification methods may include:

a) Demonstration: The operation of interfacing entities that relies on observable functional operation not requiring the use of instrumentation, special test equipment, or subsequent analysis.
b) Test: The operation of interfacing entities using instrumentation or special test equipment to collect data for later analysis.
c) Analysis: The processing of accumulated data obtained from other qualification methods. Examples are reduction, interpretation, or extrapolation of test results.
d) Inspection: The visual examination of interfacing entities, documentation, etc.
e) Special qualification methods: Any special qualification methods for the interfacing entities, such as special tools, techniques, procedures, facilities, and acceptance limits.

5) **Requirements traceability** .For system-level interfacing entities, this subclause does not apply. For each subsystem- or lower-level interfacing entity covered by this IRS, this subclause shall contain:
   a) Traceability from each requirement imposed on the entity in this specification to the system (or subsystem, if applicable) requirements it addresses. (Alternatively, this traceability may be provided by annotating each requirement in clause 3.)Note: Each level of system refinement may result in requirements not directly traceable to higher-level requirements. For example, a system architectural design that creates multiple software items may result in requirements about how the software items will interface, even though these interfaces are not covered in system requirements. Such requirements may be traced to a general requirement such as "system implementation" or to the system design decisions that resulted in their generation.
   b) Traceability from each system (or subsystem, if applicable) requirement that has been allocated to the interfacing entity and that affects an interface covered in this specification to the requirements in this specification that address it.
6) **Notes** .This clause shall contain any general information that aids in understanding this document (e.g., background information, glossary, rationale). This clause shall include an alphabetical listing of all acronyms, abbreviations, and their meanings as used in this document and a list of any terms and definitions needed to understand this document.

A) **Annexes** . Annexes may be used to provide information published separately for convenience in document maintenance (e.g., charts, classified data). As applicable, each annex shall be referenced in the main body of the document where the data would normally have been provided. Annexes may be bound as separate documents for ease in handling. Annexes shall be lettered alphabetically (A, B, etc.).

F.2.4 Contents of the Software Requirements Specification (SRS)

SOFTWARE REQUIREMENTS SPECIFICATION (SRS)

Contents

1) Scope
   1.1) Identification
   1.2) System overview
   1.3) Document overview
2) Referenced documents
3) Requirements
   3.1) Required states and modes
   3.2) Software item capability requirements
      3.2.x)Software item capability)
   3.3) Software item external interface requirements
      3.3.1)Interface identification and diagrams
      3.3.x)Project-unique identifier of interface)
   3.4) Software item internal interface requirements

3.5) Software item internal data requirements
3.6) Adaptation requirements
3.7) Safety requirements
3.8) Security and privacy protection requirements
3.9) Software item environment requirements
3.10)Computer resource requirements
3.10.1)Computer hardware requirements
3.10.2)Computer hardware resource utilization requirements
3.10.3)Computer software requirements
3.10.4)Computer communications requirements
3.11)Software quality factors
3.12)Design and implementation constraints
3.13)Personnel-related requirements
3.14)Training-related requirements
3.15)Logistics-related requirements
3.16)Other requirements
3.17)Packaging requirements
3.18)Precedence and criticality of requirements

4) Qualification provisions
5) Requirements traceability
6) Notes

A) Annexes

1) **Scope** .This clause should be divided into the following subclauses.
1.1) **Identification** .This subclause shall contain a full identification of the system and the software to which this document applies, including, as applicable, identification number(s), title(s), abbreviations), version number(s), and release number(s).
1.2) **System overview** .This subclause shall briefly state the purpose of the system and the software to which this document applies. It shall describe the general nature of the system and software; summarize the history of system development, operation, and maintenance; identify the project sponsor, acquirer, user, developer, and maintenance organizations; identify current and planned operating sites; and list other relevant documents.
1.3) **Document overview** .This subclause shall summarize the purpose and contents of this document and shall describe any security or privacy protection considerations associated with its use.

2) **Referenced documents** .This clause shall list the number, title, revision, date, and source of all documents referenced in this manual.

3) **Requirements** .This clause should be divided into the following subclauses to specify the software item requirements, that is, those characteristics of the software item that are conditions for its acceptance. Software item requirements are software requirements generated to satisfy the system requirements allocated to this software item. Each requirement shall be assigned a project-unique identifier to support testing and traceability and shall be stated in such a way that an objective test can be defined for it. Each requirement shall be annotated with associated qualification method(s) (see clause 4) and traceability to system (or subsystem, if applicable) requirements (see 5.a) if not provided in those clauses. The degree of detail to be provided shall be guided by the following rule: include those characteristics of the software item that are conditions for software item acceptance; defer to design descriptions those characteristics that the acquirer is willing to leave up to the developer. If there are no requirements in a given subclause, the subclause shall so state. If a given requirement fits into more than one subclause, it may be stated once and referenced from the other subclauses. Conventions needed to understand the requirements shall be presented or referenced.
3.1) **Required states and modes** .If the software item is required to operate in more than one state or mode having requirements distinct from other states or modes, this subclause shall identify and define each state and mode. Examples of states and modes include: idle, ready, active, post-use analysis, training, degraded, emergency, backup, wartime, peacetime. The distinction between states and modes is arbitrary. A software item may be described in terms of states

only, modes only, states within modes, modes within states, or any other scheme that is useful. If no states or modes are required, this subclause shall so state, without the need to create artificial distinctions. If states and/or modes are required, each requirement or group of requirements in this specification shall be correlated to the states and modes. The correlation may be indicated by a table or other method in this subclause, in an annex referenced from this subclause, or by annotation of the requirements in the subclauses where they appear.

3.2) **Software item capability requirements** .This subclause should be divided into subclauses to itemize the requirements associated with each capability of the software item. A "capability" is defined as a group of related requirements. The word "capability" may be replaced with "function," "subject," "object," or other term useful for presenting the requirements.

3.2.x)**(Software item capability)** .This subclause shall identify a required software item capability and shall itemize the requirements associated with the capability. If the capability can be more clearly specified by dividing it into constituent capabilities, the constituent capabilities shall be specified in subclauses. The requirements shall specify required behavior of the software item and shall include applicable parameters, such as response times, throughput times, other timing constraints, sequencing, accuracy, capacities (how much/how many), priorities, continuous operation requirements, and allowable deviations based on operating conditions. The requirements shall include, as applicable, required behavior under unexpected, unallowed, or "out of bounds" conditions, requirements for error handling, and any provisions to be incorporated into the software item to provide continuity of operations in the event of emergencies. Subclause 3.3.x of the SRS provides a list of topics to be considered when specifying requirements regarding input the software item is required to accept and output it is required to produce.

3.3) **Software item external interface requirements** .This subclause should be divided into subclauses to specify the requirements, if any, for the software item's external interfaces. This subclause may reference one or more Interface Requirements Specifications (IRSs) or other documents containing these requirements.

3.3.1)**Interface identification and diagrams** .This subclause shall identify the required external interfaces of the software item (that is, relationships with other entities that involve sharing, providing or exchanging data). The identification of each interface shall include a project-unique identifier and shall designate the interfacing entities (systems, hardware items, software items, users, etc.) by name, number, version, and documentation references, as applicable. The identification shall state which entities have fixed interface characteristics (and therefore impose interface requirements on interfacing entities) and which are being developed or modified (thus having interface requirements imposed on them). One or more interface diagrams shall be provided to depict the interfaces.

3.3.x)**(Project-unique identifier of interface)** .This subclause (beginning with 3.3.2) shall identify a software item external interface by project-unique identifier, shall briefly identify the interfacing entities, and should be divided into subclauses as needed to state the requirements imposed on the software item to achieve the interface. Interface characteristics of the other entities involved in the interface shall be stated as assumptions or as "When [the entity not covered] does this, the software item shall...," not as requirements on the other entities. This subclause may reference other documents (such as data dictionaries, standards for communication protocols, and standards for user interfaces) in place of stating the information here. The requirements shall include the following, as applicable, presented in any order suited to the requirements, and shall note any differences in these characteristics from the point of view of the interfacing entities (such as different expectations about the size, frequency, or other characteristics of data elements):

a) Priority that the software item is required to assign the interface

b) Requirements on the type of interface (such as real-time data transfer, storage-and-retrieval of data, etc.) to be implemented

c) Required characteristics of individual data elements that the software item is required to provide, store, send, access, receive, etc., such as:

1) Names/identifiers

a) Project-unique identifier
b) Non-technical (natural language) name
c) Standard data element name
d) Technical name (e.g., variable or field name in code or database)
e) Abbreviation or synonymous names
2) Data type (alphanumeric, integer, etc.)
3) Size and format (such as length and punctuation of a character string)
4) Units of measurement (such as meters, dollars, nanoseconds)
5) Range or enumeration of possible values (such as 0–99)
6) Accuracy (how correct) and precision (number of significant digits)
7) Priority, timing, frequency, volume, sequencing, and other constraints, such as whether the data element may be updated and whether business rules apply
8) Security and privacy protection constraints
9) Sources (setting/sending entities) and recipients (using/receiving entities)
d) Required characteristics of data element assemblies (records, messages, files, arrays, displays, reports, etc.) that the software item is required to provide, store, send, access, receive, etc., such as:
1) Names/identifiers
a) Project-unique identifier
b) Non-technical (natural language) name
c) Technical name (e.g., record or data structure name in code or database)
d) Abbreviations or synonymous names
2) Data elements in the assembly and their structure (number, order, grouping)
3) Medium (such as disk) and structure of data elements/assemblies on the medium
4) Visual and auditory characteristics of displays and other outputs (such as colors, layouts, fonts, icons and other display elements, beeps, lights)
5) Relationships among assemblies, such as sorting/access characteristics
6) Priority, timing, frequency, volume, sequencing, and other constraints, such as whether the assembly may be updated and whether business rules apply
7) Security and privacy protection constraints
8) Sources (setting/sending entities) and recipients (using/receiving entities)
e) Required characteristics of communication methods that the software item is required to use for the interface, such as:
1) Project-unique identifiers)
2) Communication links/bands/frequencies/media and their characteristics
3) Message formatting
4) Flow control (such as sequence numbering and buffer allocation)
5) Data transfer rate, whether periodic/aperiodic, and interval between transfers
6) Routing, addressing, and naming conventions
7) Transmission services, including priority and grade
8) Safety/security/privacy protection considerations, such as encryption, user authentication, compartmentalization, and auditing
f) Required characteristics of protocols the software item is required to use for the interface, such as:
1) Project-unique identifier(s)
2) Priority/layer of the protocol
3) Packeting, including fragmentation and reassembly, routing, and addressing
4) Legality checks, error control, and recovery procedures
5) Synchronization, including connection establishment, maintenance, termination
6) Status, identification, and any other reporting features
g) Other required characteristics, such as physical compatibility of the interfacing entity(ies) (dimensions, tolerances, loads, voltages, plug compatibility, etc.)

3.4) **Software item internal interface requirements** .This subclause shall specify the requirements, if any, imposed on interfaces internal to the software item. If all internal interfaces are

left to the design, this fact shall be so stated. If such requirements are to be imposed, subclause 3.3 of the SRS provides a list of topics to be considered.

3.5) **Software item internal data requirements** .This subclause shall specify the requirements, if any, imposed on data internal to the software item. Included shall be requirements, if any, on databases and data files to be included in the software item. If all decisions about internal data are left to the design, this fact shall be so stated. If such requirements are to be imposed, subclauses 3.3.x.c and 3.3.x.d of the SRS provide a list of topics to be considered.

3.6) **Adaptation requirements** .This subclause shall specify the requirements, if any, concerning installation-dependent data to be provided by the software item (such as site-dependent latitude and longitude or site-dependent state tax codes) and parameters that the software item is required to use that may vary according to operational needs (such as operation-dependent targeting constants or site-dependent month-end dates).

3.7) **Safety requirements** .This subclause shall specify the software item requirements, if any, concerned with preventing or minimizing unintended hazards to personnel, property, and the physical environment. Examples include safeguards the software item is required to provide to prevent inadvertent actions (such as accidentally issuing an "auto pilot off" command) and non-actions (such as failure to issue an intended "auto pilot off" command). This subclause shall include the software item requirements, if any, regarding nuclear components of the system, including, as applicable, prevention of inadvertent detonation and compliance with nuclear safety rules.

3.8) **Security and privacy protection requirements** .This subclause shall specify the software item requirements, if any, concerned with maintaining security and privacy protection. These requirements shall include, as applicable, the security/privacy protection environment in which the software item is required to operate, the type and degree of security or privacy protection to be provided, the security/privacy protection risks the software item is required to withstand, required safeguards to reduce those risks, the security/privacy protection policy that is required to be met, the security/privacy protection accountability the software item is required to provide, and the criteria that are required to be met for security/privacy protection certification/ accreditation.

3.9) **Software item environment requirements** .This subclause shall specify the requirements, if any, regarding the environment in which the software item is required to operate. Examples include the computer hardware and operating system on which the software item is required to run. (Additional requirements concerning computer resources are given in the next subclause.)

3.10) **Computer resource requirements** .This subclause should be divided into the following.

3.10.1) **Computer hardware requirements** .This subclause shall specify the requirements, if any, regarding computer hardware that is required to be used by the software item. The requirements shall include, as applicable, number of each type of equipment, type, size, capacity, and other required characteristics of processors, memory, input/output devices, auxiliary storage, communications/network equipment, and other required equipment.

3.10.2) **Computer hardware resource utilization requirements** .This subclause shall specify the requirements, if any, on the software item's computer hardware resource utilization, such as maximum allowable use of processor capacity, memory capacity, input/output device capacity, auxiliary storage device capacity, and communications/ network equipment capacity. The requirements (stated, for example, as percentages of the capacity of each computer hardware resource) shall include the conditions, if any, under which the resource utilization is to be measured.

3.10.3) **Computer software requirements** .This subclause shall specify the requirements, if any, regarding computer software that is required to be used by, or incorporated into, the software item. Examples include operating systems, database management systems, communications/ network software, utility software, input and equipment simulators, test software, and manufacturing software. The correct nomenclature, version, and documentation references of each such item of software shall be provided.

3.10.4) **Computer communications requirements** .This subclause shall specify the additional requirements, if any, concerning the computer communications that are required to be

used by the software item. Examples include geographic locations to be linked; configuration and network topology; transmission techniques; data transfer rates; gateways; required system use times; type and volume of data to be transmitted/received; time boundaries for transmission/reception/response; peak volumes of data; and diagnostic features.

3.11) **Software quality factors** .This subclause shall specify the software item requirements, if any, concerned with software quality factors identified in the contract or derived from a higher level specification. Examples include quantitative requirements regarding software item functionality (the ability to perform all required functions), reliability (the ability to perform with correct, consistent results), maintainability (the ability to be easily corrected), availability (the ability to be accessed and operated when needed), flexibility (the ability to be easily adapted to changing requirements), portability (the ability to be easily modified for a new environment), reusability (the ability to be used in multiple applications), testability (the ability to be easily and thoroughly tested), usability (the ability to be easily learned and used), and other attributes.

3.12) **Design and implementation constraints** .This subclause shall specify the requirements, if any, that constrain the design and implementation of the software item. These requirements may be specified by reference to appropriate commercial or government standards and specifications. Examples include requirements concerning:

a) Use of a particular software item architecture or requirements on the architecture, such as required databases or other software units; use of standard, military, or existing components; or use of acquirer-furnished property (equipment, information, or software)

b) Use of particular design or implementation standards; use of particular data standards; use of a particular programming language

c) Flexibility and expandability that are required to be provided to support anticipated areas of growth or changes in technology, threat, or mission

3.13) **Personnel-related requirements** .This subclause shall specify the software item requirements, if any, included to accommodate the number, skill levels, duty cycles, training needs, or other information about the personnel who will use or maintain the software item. Examples include requirements for number of simultaneous users and for built-in help or training features. Also included shall be the human factors engineering requirements, if any, imposed on the software item. These requirements shall include, as applicable, considerations for the capabilities and limitations of humans; foreseeable human errors under both normal and extreme conditions; and specific areas where the effects of human error would be particularly serious. Examples include requirements for color and duration of error messages, physical placement of critical indicators or keys, and use of auditory signals.

3.14) **Training-related requirements** .This subclause shall specify the software item requirements, if any, pertaining to training. Examples include training software to be included in the software item.

3.15) **Logistics-related requirements** .This subclause shall specify the software item requirements, if any, concerned with logistics considerations. These considerations may include: system maintenance, software maintenance, system transportation modes, supply-system requirements, impact on existing facilities, and impact on existing equipment.

3.16) **Other requirements** .This subclause shall specify additional software item requirements, if any, not covered in the previous subclauses.

3.17) **Packaging requirements** .This clause shall specify the requirements, if any, for packaging, labeling, and handling the software item for delivery (for example, delivery on 8 track magnetic tape labelled and packaged in a certain way). Applicable commercial or government specifications and standards may be referenced if appropriate.

3.18) **Precedence and criticality of requirements** .This subclause shall specify, if applicable, the order of precedence, criticality, or assigned weights indicating the relative importance of the requirements in this specification. Examples include identifying those requirements deemed critical to safety, to security, or to privacy protection for purposes of singling them out for special treatment. If all requirements have equal weight, this subclause shall so state.

4) **Qualification provisions** .This clause shall define a set of qualification methods and shall specify for each requirement in clause 3 the method(s) to be used to ensure that the requirement has been met. A table may be used to present this information, or each requirement in clause 3 may be annotated with the method(s) to be used. Qualification methods may include:
   a) Demonstration: The operation of the software item, or a part of the software item, that relies on observable functional operation not requiring the use of instrumentation, special test equipment, or subsequent analysis.
   b) Test: The operation of the software item, or a part of the software item, using instrumentation or other special test equipment to collect data for later analysis.
   c) Analysis: The processing of accumulated data obtained from other qualification methods. Examples are reduction, interpolation, or extrapolation of test results.
   d) Inspection: The visual examination of software item code, documentation, etc.
   e) Special qualification methods: Any special qualification methods for the software item, such as special tools, techniques, procedures, facilities, and acceptance limits.
5) **Requirements traceability** .This subclause shall contain:
   a) Traceability from each software item requirement in this specification to the system (or subsystem, if applicable) requirements it addresses. (Alternatively, this traceability may be provided by annotating each requirement in clause 3.)Note: Each level of system refinement may result in requirements not directly traceable to higher-level requirements. For example, a system architectural design that creates multiple software items may result in requirements about how the software items will interface, even though these interfaces are not covered in system requirements. Such requirements may be traced to a general requirement such as “system implementation” or to the system design decisions that resulted in their generation.
   b) Traceability from each system (or subsystem, if applicable) requirement allocated to this software item to the software item requirements that address it. All system (subsystem) requirements allocated to this software item shall be accounted for. Those that trace to software item requirements contained in IRSs shall reference those IRSs.
6) **Notes** .This clause shall contain any general information that aids in understanding this specification (e.g., background information, glossary, rationale). This clause shall include an alphabetical listing of all acronyms, abbreviations, and their meanings as used in this document and a list of any terms and definitions needed to understand this document.

A) **Annexes** . Annexes may be used to provide information published separately for convenience in document maintenance (e.g., charts, classified data). As applicable, each annex shall be referenced in the main body of the document where the data would normally have been provided. Annexes may be bound as separate documents for ease in handling. Annexes shall be lettered alphabetically (A, B, etc.).

Annex G

(normative)

Design software product descriptions

G.1 Scope

This annex specifies the contents of software products associated with design in this standard. It applies regardless of whether the software products are deliverable. This annex is a normative (that is, binding) part of this standard, subject to tailoring.

G.2 Software products covered

This following subclauses describe the contents of the software products covered by this annex. The products are listed in the order they are referenced in this standard and include the following:

a)) System/Subsystem Design Description (SSDD)
b)) Interface Design Description (IDD)
c)) Database Design Description (DBDD)
d)) Software Design Description (SDD)

G.2.1 Contents of the System/Subsystem Design Description (SSDD)

SYSTEM/SUBSYSTEM DESIGN DESCRIPTION (SSDD)

Contents

1) Scope
   1.1) Identification
   1.2) System overview
   1.3) Document overview
2) Referenced documents
3) System-wide design decisions
4) System architectural design
   4.1) System components
   4.2) Concept of execution
   4.3) Interface design
      4.3.1)Interface identification and diagrams
      4.3.x)(Project-unique identifier of interface)
5) Requirements traceability
6) Notes

A) Annexes

1) **Scope** . This clause should be divided into the following subclauses.

1.1) **Identification** . This subclause shall contain a full identification of the system to which this document applies, including, as applicable, identification number(s), title(s), abbreviation(s), version number(s), and release number(s).

1.2) **System overview** . This subclause shall briefly state the purpose of the system to which this document applies. It shall describe the general nature of the system; summarize the history of system development, operation, and maintenance; identify the project sponsor, acquirer, user, developer, and maintenance organizations; identify current and planned operating sites; and list other relevant documents.

1.3) **Document overview** . This subclause shall summarize the purpose and contents of this document and shall describe any security or privacy protection considerations associated with its use.

2) **Referenced documents** . This clause shall list the number, title, revision, date, and source of all documents referenced in this manual.

3) **System-wide design decisions** . This clause should be divided into subclauses as needed to present system-wide design decisions, that is, decisions about the system's behavioral design (how it will behave, from a user's point of view, in meeting its requirements, ignoring internal implementation) and other decisions affecting the selection and design of system components. If all such decisions are explicit in the requirements or are deferred to the design of the system components, this clause shall so state. Design decisions that respond to requirements designated critical, such as those for safety, security, or privacy protection, shall be placed in separate subclauses. If a design decision depends upon system states or modes, this dependency shall be indicated. Design conventions needed to understand the design shall be presented or referenced. Examples of system-wide design decisions are the following:

a) Design decisions regarding input the system will accept and output it will produce, including interfaces with other systems, hardware items, software items, and users (4.3.x of the SSDD identifies topics to be considered in this description). If part or all of this information is given in Interface Design Descriptions (IDDs), they may be referenced.

b) Design decisions on system behavior in response to each input or condition, including actions the system will perform, response times and other performance characteristics, description of physical systems modeled, selected equations/algorithms/rules, and handling of unallowed inputs or conditions.

c) Design decisions on how system databases/data files will appear to the user (4.3.x of the SSDD identifies topics to be considered in this description). If part or all of this information is given in Database Design Descriptions (DBDDs), they may be referenced.

d) Selected approach to meeting safety, security, and privacy protection requirements.

e) Design and construction choices for hardware or hardware-software systems, such as physical size, color, shape, weight, materials, and markings.

f) Other system-wide design decisions made in response to requirements, such as selected approach to providing required flexibility, availability, and maintainability.

4) **System architectural design** . This clause should be divided into the following subclauses to describe the system architectural design. If part or all of the design depends upon system states or modes, this dependency shall be indicated. If design information falls into more than one subclause, it may be presented once and referenced from the other subclauses. Design conventions needed to understand the design shall be presented or referenced.Note: For brevity, this clause is written in terms of organizing a system directly into hardware items, software items, and manual operations, but is interpreted to cover organizing a system into subsystems, organizing a subsystem into hardware items, software items, and manual operations, or other variations as appropriate.

4.1) **System components** . This subclause shall:

a) Identify the components of the system (hardware items, software items, and manual operations). Each component shall be assigned a project-unique identifier. Note: A database may be treated as a software item or as part of a software item.

b) Show the static (such as "consists of") relationship(s) of the components. Multiple relationships may be presented, depending on the selected design methodology.

c) State the purpose of each component and identify the system requirements and system-wide design decisions allocated to it. (Alternatively, the allocation of requirements may be provided in 5.a.)

d) Identify each component's development type, if known (such as new development, existing component to be reused as is, existing design to be reused as is, existing design or component to be reengineered, component to be developed for reuse, component planned for Build N, etc.) For existing design or components, the description shall provide identifying information, such as name, version, documentation references, location, etc.

e) For each computer system or other aggregate of computer hardware resources identified for use in the system, describe its computer hardware resources (such as processors, memory, input/output devices, auxiliary storage, and communications/network equipment). Each description shall, as applicable, identify the hardware and software items that will use the resource, describe the allocation of resource utilization to each software item that will use the resource (for example, 20% of the resource's capacity allocated to software item 1, 30% to software item 2), describe the conditions under which utilization will be measured, and describe the characteristics of the resource:

1) Descriptions of computer processors shall include, as applicable, manufacturer name and model number, processor speed/capacity, identification of instruction set architecture, applicable compiler(s), word size (number of bits in each computer word), character set standard (such as ASCII, EBCDIC), and interrupt capabilities.

2) Descriptions of memory shall include, as applicable, manufacturer name and model number and memory size, type, speed, and configuration (such as 256K cache memory, 16MB RAM (4MB x 4)).

3) Descriptions of input/output devices shall include, as applicable, manufacturer name and model number, type of device, and device speed/capacity.

4) Descriptions of auxiliary storage shall include, as applicable, manufacturer name and model number, type of storage, amount of installed storage, and storage speed.

5) Descriptions of communications/network equipment, such as modems, network interface cards, hubs, gateways, cabling, high speed data lines, or aggregates of these or other components, shall include, as applicable, manufacturer name and model number, data transfer rates/capacities, network topologies, transmission techniques, and protocols used.

6) Each description shall also include, as applicable, growth capabilities, diagnostic capabilities, and any additional hardware capabilities relevant to the description.

f) Present a specification tree for the system, that is, a diagram that identifies and shows the relationships among the planned specifications for the system components.

4.2) **Concept of execution** . This subclause shall describe the concept of execution among the system components. It shall include diagrams and descriptions showing the dynamic relationship of the components, that is, how they will interact during system operation, including, as applicable, flow of execution control, data flow, dynamically controlled sequencing, state transition diagrams, timing diagrams, priorities among components, handling of interrupts, timing/sequencing relationships, exception handling, concurrent execution, dynamic allocation/deallocation, dynamic creation/deletion of objects, processes, tasks, and other aspects of dynamic behavior.

4.3) **Interface design** . This subclause should be divided into the following to describe the interface characteristics of the system components. It shall include both interfaces among the components and their interfaces with external entities such as other systems, hardware items, software items, and users. Note: There is no requirement for these interfaces to be completely designed at this level; this subclause is provided to allow the recording of interface design decisions made as part of system architectural design. If part or all of this information is contained in Interface Design Descriptions (IDDs) or elsewhere, these sources may be referenced.

4.3.1)**Interface identification and diagrams** .This subclause shall state the project-unique identifier assigned to each interface and shall identify the interfacing entities (systems, hardware items, software items, users, etc.) by name, number, version, and documentation references, as applicable. The identification shall state which entities have fixed interface

characteristics (and therefore impose interface requirements on interfacing entities) and which are being developed or modified (thus having interface requirements imposed on them). One or more interface diagrams shall be provided, as appropriate, to depict the interfaces.

4.3.x)**(Project-unique identifier of interfaces)** .This subclause (beginning with 4.3.2) shall identify an interface by project-unique identifier, shall briefly identify the interfacing entities, and should be divided into subclauses as needed to describe the interface characteristics of one or both of the interfacing entities. If a given interfacing entity is not covered by this SSDD (for example, an external system) but its interface characteristics need to be mentioned to describe interfacing entities that are, these characteristics shall be stated as assumptions or as "When [the entity not covered] does this, [the entity that is covered] will ... ." This subclause may reference other documents (such as data dictionaries, standards for protocols, and standards for user interfaces) in place of stating the information here. The design description shall include the following, as applicable, presented in any order suited to the information to be provided, and shall note any differences in these characteristics from the point of view of the interfacing entities (such as different expectations about the size, frequency, or other characteristics of data elements):

a) Priority assigned to the interface by the interfacing entity(ies)
b) Type of interface (such as real-time data transfer, storage-and-retrieval of data, etc.) to be implemented
c) Characteristics of individual data elements that the interfacing entity(ies) will provide, store, send, access, receive, etc., such as:

1) Names/identifiers
a) Project-unique identifier
b) Non-technical (natural language) name
c) Standard data element name
d) Technical name (e.g., variable or field name in code or database)
e) Abbreviation or synonymous names
2) Data type (alphanumeric, integer, etc.)
3) Size and format (such as length and punctuation of a character string)
4) Units of measurement (such as meters, dollars, nanoseconds)
5) Range or enumeration of possible values (such as 0-99)
6) Accuracy (how correct) and precision (number of significant digits)
7) Priority, timing, frequency, volume, sequencing, and other constraints, such as whether the data element may be updated and whether business rules apply
8) Security and privacy protection constraints
9) Sources (setting/sending entities) and recipients (using/receiving entities)

d) Characteristics of data element assemblies (records, messages, files, arrays, displays, reports, etc.) that the interfacing entity(ies) will provide, store, send, access, receive, etc., such as:

1) Names/identifiers
a) Project-unique identifier to be used for traceability
b) Non-technical (natural language) name
c) Technical name (e.g., record or data structure name in code or database)
d) Abbreviations or synonymous names
2) Data elements in the assembly and their structure (number, order, grouping)
3) Medium (such as disk) and structure of data elements/assemblies on the medium
4) Visual and auditory characteristics of displays and other outputs (such as colors, layouts, fonts, icons and other display elements, beeps, lights)
5) Relationships among assemblies, such as sorting/access characteristics
6) Priority, timing, frequency, volume, sequencing, and other constraints, such as whether the assembly may be updated and whether business rules apply
7) Security and privacy protection constraints
8) Sources (setting/sending entities) and recipients (using/receiving entities)

e) Characteristics of communication methods that the interfacing entity(ies) will use for the interface, such as:
1) Project-unique identifier(s)
2) Communication links/bands/frequencies/media and their characteristics
3) Message formatting
4) Flow control (such as sequence numbering and buffer allocation)
5) Data transfer rate, whether periodic/aperiodic, and interval between transfers
6) Routing, addressing, and naming conventions
7) Transmission services, including priority and grade
8) Safety/security/privacy protection considerations, such as encryption, user authentication, compartmentalization, and auditing
f) Characteristics of protocols that the interfacing entity(ies) will use for the interface, such as:
1) Project-unique identifier(s)
2) Priority/layer of the protocol
3) Packeting, including fragmentation and reassembly, routing, and addressing
4) Legality checks, error control, and recovery procedures
5) Synchronization, including connection establishment, maintenance, termination
6) Status, identification, and any other reporting features
g) Other characteristics, such as physical compatibility of the interfacing entity(ies) (dimensions, tolerances, loads, voltages, plug compatibility, etc.)

5) **Requirements traceability** .This subclause shall contain:
a) Traceability from each system component identified in this SSDD to the system requirements allocated to it. (Alternatively, this traceability may be provided in 4.1.)Note: Each level of system refinement may result in requirements not directly traceable to higher-level requirements. For example, a system architectural design that creates two subsystems may result in requirements about how the subsystems will interface, even though these interfaces are not covered in system requirements. Such requirements may be traced to a general requirement such as “system implementation” or to the system design decisions that resulted in their generation.
b) Traceability from each system requirement to the system components to which it is allocated.

6) **Notes** .This clause shall contain any general information that aids in understanding this document (e.g., background information, glossary, rationale). This clause shall contain an alphabetical listing of all acronyms, abbreviations, and their meanings as used in this document and a list of any terms and definitions needed to understand this document.

A) **Annexes** . Annexes may be used to provide information published separately for convenience in document maintenance (e.g., charts, classified data). As applicable, each annex shall be referenced in the main body of the document where the data would normally have been provided. Annexes may be bound as separate documents for ease in handling. Annexes shall be lettered alphabetically (A, B, etc.).

G.2.2 Contents of the Interface Design Description (IDD)

INTERFACE DESIGN DESCRIPTION (IDD)

Contents

1) Scope
1.1) Identification
1.2) System overview
1.3) Document overview
2) Referenced documents
3) Interface design
3.1) Interface identification and diagrams

3.x) (Project-unique identifier of interface)
4) Requirements traceability
5) Notes
A) Annexes
1) **Scope** . This clause should be divided into the following subclauses.
1.1) **Identification** . This subclause shall contain a full identification of the interfacing entities (systems, subsystems, hardware items, software items, manual operations, or other system components) and interfaces to which this document applies, including, as applicable, identification number(s), title(s), abbreviations), version number(s), and release number(s).
1.2) **System overview** . This subclause shall briefly state the purpose of the system(s) and software to which this document applies. It shall describe the general nature of the system and software; summarize the history of system development, operation, and maintenance; identify the project sponsor, acquirer, user, developer, and maintenance organizations; identify current and planned operating sites; and list other relevant documents.
1.3) **Document overview** . This subclause shall summarize the purpose and contents of this document and shall describe any security or privacy protection considerations associated with its use.
2) **Referenced documents** . This clause shall list the number, title, revision, date, and source of all documents referenced in this manual.
3) **Interface design** . This clause should be divided into the following subclauses to describe the interface characteristics of one or more systems, subsystems, hardware items, software items, manual operations, or other system components. If part or all of the design depends upon system states or modes, this dependency shall be indicated. If design information falls into more than one subclause, it may be presented once and referenced from the other subclauses. If part or all of this information is documented elsewhere, it may be referenced. Design conventions needed to understand the design shall be presented or referenced.
3.1) **Interface identification and diagrams** . For each interface identified in 1.1, this subclause shall state the project-unique identifier assigned to the interface and shall identify the interfacing entities (systems, hardware items, software items, users, etc.) by name, number, version, and documentation references, as applicable. The identification shall state which entities have fixed interface characteristics (and therefore impose interface requirements on interfacing entities) and which are being developed or modified (thus having interface requirements imposed on them). One or more interface diagrams shall be provided, as appropriate, to depict the interfaces.
3.x) **(Project-unique identifier of interface)** . This subclause (beginning with 3.2) shall identify an interface by project-unique identifier, shall briefly identify the interfacing entities, and should be divided as needed to describe the interface characteristics of one or both of the interfacing entities. If a given interfacing entity is not covered by this IDD (for example, an external system) but its interface characteristics need to be mentioned to describe interfacing entities that are, these characteristics shall be stated as assumptions or as “When [the entity not covered] does this, [the entity that is covered] will... .” This subclause may reference other documents (such as data dictionaries, standards for protocols, and standards for user interfaces) in place of stating the information here. The design description shall include the following, as applicable, presented in any order suited to the information to be provided, and shall note any differences in these characteristics from the point of view of the interfacing entities (such as different expectations about the size, frequency, or other characteristics of data elements):
a) Priority assigned to the interface by the interfacing entity(ies)
b) Type of interface (such as real-time data transfer, storage-and-retrieval of data, etc.) to be implemented
c) Characteristics of individual data elements that the interfacing entity(ies) will provide, store, send, access, receive, etc., such as:
1) Names/identifiers
a) Project-unique identifier
b) Non-technical (natural language) name

c) Standard data element name
d) Technical name (e.g., variable or field name in code or database)
e) Abbreviation or synonymous names
2) Data type (alphanumeric, integer, etc.)
3) Size and format (such as length and punctuation of a character string)
4) Units of measurement (such as meters, dollars, nanoseconds)
5) Range or enumeration of possible values (such as 0-99)
6) Accuracy (how correct) and precision (number of significant digits)
7) Priority, timing, frequency, volume, sequencing, and other constraints, such as whether the data element may be updated and whether business rules apply
8) Security and privacy protection constraints
9) Sources (setting/sending entities) and recipients (using/receiving entities)
d) Characteristics of data element assemblies (records, messages, files, arrays, displays, reports, etc.) that the interfacing entity(ies) will provide, store, send, access, receive, etc., such as:
1) Names/identifiers
a) Project-unique identifier
b) Non-technical (natural language) name
c) Technical name (e.g., record or data structure name in code or database)
d) Abbreviations or synonymous names
2) Data elements in the assembly and their structure (number, order, grouping)
3) Medium (such as disk) and structure of data elements/assemblies on the medium
4) Visual and auditory characteristics of displays and other outputs (such as colors, layouts, fonts, icons and other display elements, beeps, lights)
5) Relationships among assemblies, such as sorting/access characteristics
6) Priority, timing, frequency, volume, sequencing, and other constraints, such as whether the assembly may be updated and whether business rules apply
7) Security and privacy protection constraints
8) Sources (setting/sending entities) and recipients (using/receiving entities)
e) Characteristics of communication methods that the interfacing entity(ies) will use for the interface, such as:
1) Project-unique identifier(s)
2) Communication links/bands/frequencies/media and their characteristics
3) Message formatting
4) Flow control (such as sequence numbering and buffer allocation)
5) Data transfer rate, whether periodic/aperiodic, and interval between transfers
6) Routing, addressing, and naming conventions
7) Transmission services, including priority and grade
8) Safety/security/privacy protection considerations, such as encryption, user authentication, compartmentalization, and auditing
f) Characteristics of protocols the interfacing entity(ies) will use for the interface, such as:
1) Project-unique identifier(s)
2) Priority/layer of the protocol
3) Packeting, including fragmentation and reassembly, routing, and addressing
4) Legality checks, error control, and recovery procedures
5) Synchronization, including connection establishment, maintenance, termination
6) Status, identification, and any other reporting features
g) Other characteristics, such as physical compatibility of the interfacing entity(ies) (dimensions, tolerances, loads, voltages, plug compatibility, etc.)

4) **Requirements traceability** .This subclause shall contain:
a) Traceability from each interfacing entity covered by this IDD to the system or software item requirements addressed by the entity's interface design.
Note: Each level of system or software item refinement may result in requirements not directly traceable to higher-level requirements. For example, a system or software architectural design

that creates two subsystems or two software units may result in requirements about how the subsystems or software units will interface, even though these interfaces are not covered in system or software item requirements. Such requirements may be traced to a general requirement such as “system implementation” or “software item” or to the system or software design decisions (e.g., in the SDD) that resulted in their generation.

b) Traceability from each system or software item requirement that affects an interface covered in this IDD to the interfacing entities that address it.

5) **Notes** . This clause shall contain any general information that aids in understanding this document (e.g., background information, glossary, rationale). This clause shall include an alphabetical listing of all acronyms, abbreviations, and their meanings as used in this document and a list of any terms and definitions needed to understand this document.

A) **Annexes** . Annexes may be used to provide information published separately for convenience in document maintenance (e.g., charts, classified data). As applicable, each annex shall be referenced in the main body of the document where the data would normally have been provided. Annexes may be bound as separate documents for ease in handling. Annexes shall be lettered alphabetically (A, B, etc.).

G.2.3 Contents of the Database Design Description (DBDD)

DATABASE DESIGN DESCRIPTION (DBDD)

Contents

1) Scope
   1.1) Identification
   1.2) Database overview
   1.3) Document overview
2) Referenced documents
3) Database-wide design decisions
4) Design of the database
   4.x) (Name of database design level)
5) Detailed design of software units used for database access or manipulation
   5.x) (Project-unique identifier of a software unit, or designator of a group of software units)
6) Requirements traceability
7) Notes

A) Annexes

1) **Scope** . This clause should be divided into the following subclauses.
   1.1) **Identification** . This subclause shall contain a full identification of the database to which this document applies, including, as applicable, identification number(s), title(s), abbreviation(s), version number(s), and release number(s).
   1.2) **Database overview** .This subclause shall briefly state the purpose of the database to which this document applies. It shall describe the general nature of the database; summarize the history of its development, use, and maintenance; identify the project sponsor, acquirer, user, developer, and maintenance organizations; identify current and planned operating sites; and list other relevant documents.
   1.3) **Document overview** .This subclause shall summarize the purpose and contents of this document and shall describe any security or privacy protection considerations associated with its use.
2) **Referenced documents** .This clause shall list the number, title, revision, date, and source of all documents referenced in this manual.
3) **Database-wide design decisions** .This clause should be divided into subclauses as needed to present database-wide design decisions, that is, decisions about the database’s behavioral design (how it will behave, from a user’s point of view, in meeting its requirements, ignoring internal

implementation) and other decisions affecting further design of the database. If all such decisions are explicit in the system or software item requirements, this clause shall so state. Design decisions that respond to requirements designated critical, such as those for safety, security, or privacy protection, shall be placed in separate subclauses. If a design decision depends upon system states or modes, this dependency shall be indicated. If some or all of the design decisions are described in the documentation of a custom or commercial database management system (DBMS), they may be referenced from this clause. Design conventions needed to understand the design shall be presented or referenced. Examples of database-wide design decisions are the following:

a) Design decisions regarding queries or other input the database will accept and output (displays, reports, messages, responses, etc.) it will produce, including interfaces with other systems, hardware items, software items, and users (5.x.d of the DBDD identifies topics to be considered in this description). If part or all of this information is given in Interface Design Descriptions (IDDs), they may be referenced.
b) Design decisions on database behavior in response to each input or query, including actions, response times and other performance characteristics, selected equations/algorithms/rules, disposition, and handling of unallowed inputs
c) Design decisions on how databases/data files will appear to the user (4.x of the DBDD identifies topics to be considered in this description)
d) Design decisions on the database management system to be used (including name, version/ release) and the type of flexibility to be built into the database for adapting to changing requirements
e) Design decisions on the levels and types of availability, security, privacy protection, and continuity of operations to be offered by the database
f) Design decisions on database distribution (such as client/server), master database file updates and maintenance, including maintaining consistency, establishing/ re-establishing and maintaining synchronization, enforcing integrity and business rules
g) Design decisions on backup and restoration including data and process distribution strategies, permissible actions during backup and restoration, and special considerations for new or non-standard technologies such as video and sound
h) Design decisions on repacking, sorting, indexing, synchronization, and consistency including automated disk management and space reclamation considerations, optimizing strategies and considerations, storage and size considerations, and population of the database and capture of legacy data

4) **Design of the database** .This clause should be divided into subclauses as needed to describe the design of the database. The number of levels of design and the names of those levels shall be based on the design methodology used. Examples of database design levels include conceptual, internal, logical, and physical. If part or all of the design depends upon system states or modes, this dependency shall be indicated. Design conventions needed to understand the design shall be presented or referenced.

Note: The term “data element assembly” is used to mean any entity, relation, schema, field, table, array, etc., that has structure (number/order/grouping of data elements) at a given design level (e.g., conceptual, internal, logical, physical) and the term “data element” to mean any relation, attribute, field, cell, data element, etc. that does not have structure at that level.

4.x) **(Name of database design level)** .This subclause shall identify a database design level and shall describe the data elements and data element assemblies of the database in the terminology of the selected design method. The information shall include the following, as applicable, presented in any order suited to the information to be provided:

a) Characteristics of individual data elements in the database design, such as:
1) Names/identifiers
a) Project-unique identifier
b) Non-technical (natural language) name
c) Standard data element name
d) Technical name (e.g., field name in the database)
e) Abbreviation or synonymous names

2) Data type (alphanumeric, integer, etc.)
3) Size and format (such as length and punctuation of a character string)
4) Units of measurement (such as meters, dollars, nanoseconds)
5) Range or enumeration of possible values (such as 0–99)
6) Accuracy (how correct) and precision (number of significant digits)
7) Priority, timing, frequency, volume, sequencing, and other constraints, such as whether the data element may be updated and whether business rules apply
8) Security and privacy protection constraints
9) Sources (setting/sending entities) and recipients (using/receiving entities)

b) Characteristics of data element assemblies (records, messages, files, arrays, displays, reports, etc.) in the database design, such as:

1) Names/identifiers
a) Project-unique identifier
b) Non-technical (natural language) name
c) Technical name (e.g., record or data structure name in code or database)
d) Abbreviations or synonymous names
2) Data elements in the assembly and their structure (number, order, grouping)
3) Medium (such as disk) and structure of data elements/assemblies on the medium
4) Visual and auditory characteristics of displays and other outputs (such as colors, layouts, fonts, icons and other display elements, beeps, lights)
5) Relationships among assemblies, such as sorting/access characteristics
6) Priority, timing, frequency, volume, sequencing, and other constraints, such as whether the assembly may be updated and whether business rules apply
7) Security and privacy protection constraints
8) Sources (setting/sending entities) and recipients (using/receiving entities)

5) **Detailed design of software units used for database access or manipulation** .This clause should be divided into the following subclauses to describe each software unit used for database access or manipulation. If part or all of this information is provided elsewhere, such as in a Software Design Description (SDD), the SDD for a customized DBMS, or the user manual of a commercial DBMS, that information may be referenced rather than repeated here. If part or all of the design depends upon system states or modes, this dependency shall be indicated. If design information falls into more than one subclause, it may be presented once and referenced from the other subclauses. Design conventions needed to understand the design shall be presented or referenced.

5.x) **(Project-unique identifier of a software unit, or designator of a group of software units)** .This subclause shall identify a software unit by project-unique identifier and shall describe the unit. The description shall include the following information, as applicable. Alternatively, this subclause may designate a group of software units and identify and describe the software units in subordinate subclauses. Software units that contain other software units may reference the descriptions of those units rather than repeating information.

a) Unit design decisions, if any, such as algorithms to be used, if not previously selected.
b) Any constraints, limitations, or unusual features in the design of the software unit
c) The programming language to be used and rationale for its use if other than the specified language for the software item
d) If the software unit consists of or contains procedural commands (such as menu selections in a DBMS for defining forms and reports, on-line DBMS queries for database access and manipulation, input to a graphical user interface (GUI) builder for automated code generation, commands to the operating system, or shell scripts), a list of the procedural commands and a reference to user manuals or other documents that explain them
e) If the software unit contains, receives, or outputs data, a description of its inputs, outputs, and other data elements and data element assemblies, as applicable. Data local to the software unit shall be described separately from data input to or output from the software unit. Interface characteristics may be provided here or by referencing Interface Design Description(s). If a given interfacing entity is not covered by this DBDD (for example, an external system) but its interface characteristics need to be mentioned to describe soft-

ware units that are, these characteristics shall be stated as assumptions or as "When [the entity not covered] does this, [the software unit] will... ." This subclause may reference other documents (such as data dictionaries, standards for protocols, and standards for user interfaces) in place of stating the information here. The design description shall include the following, as applicable, presented in any order suited to the information to be provided, and shall note any differences in these characteristics from the point of view of the interfacing entities (such as different expectations about the size, frequency, or other characteristics of data elements):

1) Project-unique identifier for the interface
2) Identification of the interfacing entities (software units, software items, hardware items, users, etc.) by name, number, version, and documentation references, as applicable
3) Priority assigned to the interface by the interfacing entity(ies)
4) Type of interface (such as real-time data transfer, storage-and-retrieval of data, etc.) to be implemented
5) Characteristics of individual data elements that the interfacing entity(ies) will provide, store, send, access, receive, etc. Subclause 4.x.a of the DBDD identifies topics to be covered in this description.
6) Characteristics of data element assemblies (records, messages, files, arrays, displays, reports, etc.) that the interfacing entity(ies) will provide, store, send, access, receive, etc. Subclause 4.x.b of the DBDD identifies topics to be covered in this description.
7) Characteristics of communication methods that the interfacing entity(ies) will use for the interface, such as:

a) Project-unique identifiers)
b) Communication links/bands/frequencies/media and their characteristics
c) Message formatting
d) Flow control (such as sequence numbering and buffer allocation)
e) Data transfer rate, whether periodic/aperiodic, and interval between transfers
f) Routing, addressing, and naming conventions
g) Transmission services, including priority and grade
h) Safety/security/privacy protection considerations, such as encryption, user authentication, compartmentalization, and auditing

8) Characteristics of protocols that the interfacing entity(ies) will use for the interface, such as:

a) Project-unique identifier(s)
b) Priority/layer of the protocol
c) Packeting, including fragmentation and reassembly, routing, and addressing
d) Legality checks, error control, and recovery procedures
e) Synchronization, including connection establishment, maintenance, termination
f) Status, identification, and any other reporting features

9) Other characteristics, such as physical compatibility of the interfacing entity(ies) (dimensions, tolerances, loads, voltages, plug compatibility, etc.)

f) If the software unit contains logic, the logic to be used by the software unit, including, as applicable:

1) Conditions in effect within the software unit when its execution is initiated
2) Conditions under which control is passed to other software units
3) Response and response time to each input, including data conversion, renaming, and data transfer operations
4) Sequence of operations and dynamically controlled sequencing during the software unit's operation, including:

a) The method for sequence control
b) The logic and input conditions of that method, such as timing variations, priority assignments
c) Data transfer in and out of memory

d) The sensing of discrete input signals, and timing relationships between interrupt operations within the software unit
5) Exception and error handling

6) **Requirements traceability** . This clause shall contain:
a) Traceability from each database or other software unit covered by this DBDD to the system or software item requirements it addresses.
Note: Each level of system refinement may result in requirements not directly traceable to higher-level requirements. For example, a system architectural design that creates two subsystems may result in requirements about how the subsystems will interface, even though these interfaces are not covered in system requirements. Such requirements may be traced to a general requirement such as "system implementation" or to the system design decisions that resulted in their generation.
b) Traceability from each system or software item requirement that has been allocated to a database or other software unit covered in this DBDD to the database or other software units that address it.

7) **Notes** .This clause shall contain any general information that aids in understanding this document (e.g., background information, glossary, rationale). This clause shall include an alphabetical listing of all acronyms, abbreviations, and their meanings as used in this document and a list of any terms and definitions needed to understand this document.

A) **Annexes** . Annexes may be used to provide information published separately for convenience in document maintenance (e.g., charts, classified data). As applicable, each annex shall be referenced in the main body of the document where the data would normally have been provided. Annexes may be bound as separate documents for ease in handling. Annexes shall be lettered alphabetically (A, B, etc.).

G.2.4 Contents of the Software Design Description (SDD)

SOFTWARE DESIGN DESCRIPTION (SDD)

Contents

1) Scope
1.1) Identification
1.2) System overview
1.3) Document overview
2) Referenced documents
3) System item-wide design decisions
4) Software item architectural design
4.1) Software item components
4.2) Concept of execution
4.3) Interface design
4.3.1)Interface identification and diagrams
4.3.x)(Project-unique identifier of interface)
5) Software item detailed design
5.x) (Project-unique identifier of a software unit, or designator of a group of software units)
6) Requirements traceability
7) Notes
A) Annexes

1) **Scope** .This clause should be divided into the following subclauses.
1.1) **Identification** .This subclause shall contain a full identification of the system and the software to which this document applies, including, as applicable, identification number(s), title(s), abbreviation(s), version number(s), and release number(s).

1.2) **System overview** .This subclause shall briefly state the purpose of the system and the software to which this document applies. It shall describe the general nature of the system and software; summarize the history of system development, operation, and maintenance; identify the project sponsor, acquirer, user, developer, and maintenance organizations; identify current and planned operating sites; and list other relevant documents.

1.3) **Document overview** .This subclause shall summarize the purpose and contents of this document and shall describe any security or privacy protection considerations associated with its use.

2) **Referenced documents** .This clause shall list the number, title, revision, date, and source of all documents referenced in this manual.

3) **Software item-wide design decisions** .This clause should be divided into subclauses as needed to present software item-wide design decisions, that is, decisions about the software item's behavioral design (how it will behave, from a user's point of view, in meeting its requirements, ignoring internal implementation) and other decisions affecting the selection and design of the software units that make up the software item. If all such decisions are explicit in the software item requirements or are deferred to the design of the software item's software units, this clause shall so state. Design decisions that respond to requirements designated critical, such as those for safety, security, or privacy protection, shall be placed in separate subclauses. If a design decision depends upon system states or modes, this dependency shall be indicated. Design conventions needed to understand the design shall be presented or referenced. Examples of software item-wide design decisions are the following:

   a) Design decisions regarding input the software item will accept and output it will produce, including interfaces with other systems, hardware items, software items, and users (4.3.x of the SDD identifies topics to be considered in this description). If part or all of this information is given in Interface Design Descriptions (IDDs), they may be referenced.
   b) Design decisions on software item behavior in response to each input or condition, including actions the software item will perform, response times and other performance characteristics, description of physical systems modeled, selected equations/algorithms/rules, and handling of unallowed inputs or conditions.
   c) Design decisions on how databases/data files will appear to the user (4.3.x of the SDD identifies topics to be considered in this description). If part or all of this information is given in Database Design Descriptions (DBDDs), they may be referenced.
   d) Selected approach to meeting safety, security, and privacy protection requirements.
   e) Other software item-wide design decisions made in response to requirements, such as selected approach to providing required flexibility, availability, and maintainability.

4) **Software item architectural design** .This clause should be divided into the following subclauses to describe the software item architectural design. If part or all of the design depends upon system states or modes, this dependency shall be indicated. If design information falls into more than one subclause, it may be presented once and referenced from the other subclauses. Design conventions needed to understand the design shall be presented or referenced.

   4.1) **Software item components** .This subclause shall:

      a) Identify the software units that make up the software item. Each software unit shall be assigned a project-unique identifier.

         Note: A software unit is an element in the design of a software item; for example, a major subdivision of a software item, a component of that subdivision, a class, object, module, function, routine, or database. Software units may occur at different levels of a hierarchy and may consist of other software units. Software units in the design may or may not have a one-to-one relationship with the code and data entities (routines, procedures, databases, data files, etc.) that implement them or with the computer files containing those entities. A database may be treated as a software item or as a software unit. The SDD may refer to software units by any name(s) consistent with the design methodology being used.
      b) Show the static (such as "consists of") relationships) of the software units. Multiple relationships may be presented, depending on the selected software design methodology (for

example, in an object-oriented design, this subclause may present the class and object structures as well as the module and process architectures of the software item).

c) State the purpose of each software unit and identify the software item requirements and software item-wide design decisions allocated to it. (Alternatively, the allocation of requirements may be provided in 6.a.)

d) Identify each software unit's development type (such as new development, existing design or software to be reused as is, existing design or software to be reengineered, software to be developed for reuse, software planned for Build N, etc.) For existing design or software, the description shall provide identifying information, such as name, version, documentation references, library, etc.

e) Describe the software item's (and as applicable, each software unit's) planned utilization of computer hardware resources (such as processor capacity, memory capacity, input/output device capacity, auxiliary storage capacity, and communications/network equipment capacity). The description shall cover all computer hardware resources included in resource utilization requirements for the software item, in system-level resource allocations affecting the softwareitem, and in resource utilization measurement planning in the Software Development Plan. If all utilization data for a given computer hardware resource are presented in a single location, such as in one SDD, this subclause may reference that source. Included for each computer hardware resource shall be:

1) The software item requirements or system-level resource allocations being satisfied
2) The assumptions and conditions on which the utilization data are based (for example, typical usage, worst-case usage, assumption of certain events)
3) Any special considerations affecting the utilization (such as use of virtual memory, overlays, or multiprocessors or the impacts of operating system overhead, library software, or other implementation overhead)
4) The units of measure used (such as percentage of processor capacity, cycles per second, bytes of memory, kilobytes per second)
5) The level(s) at which the estimates or measures will be made (such as software unit, software item, or executable program)

f) Identify the program library in which the software that implements each software unit is to be placed

4.2) **Concept of execution** .This subclause shall describe the concept of execution among the software units. It shall include diagrams and descriptions showing the dynamic relationship of the software units, that is, how they will interact during software item operation, including, as applicable, flow of execution control, data flow, dynamically controlled sequencing, state transition diagrams, timing diagrams, priorities among units, handling of interrupts, timing/sequencing relationships, exception handling, concurrent execution, dynamic allocation/deallocation, dynamic creation/deletion of objects, processes, tasks, and other aspects of dynamic behavior.

4.3) **Interface design** .This subclause should be divided as follows to describe the interface characteristics of the software units. It shall include both interfaces among the software units and their interfaces with external entities such as systems, hardware items, software items, and users. If part or all of this information is contained in Interface Design Descriptions (IDDs), in clause 5 of the SDD, or elsewhere, these sources may be referenced.

4.3.1)**Interface identification and diagrams** .This subclause shall state the project-unique identifier assigned to each interface and shall identify the interfacing entities (software units, systems, hardware items, software items, users, etc.) by name, number, version, and documentation references, as applicable. The identification shall state which entities have fixed interface characteristics (and therefore impose interface requirements on interfacing entities) and which are being developed or modified (thus having interface requirements imposed on them). One or more interface diagrams shall be provided, as appropriate, to depict the interfaces.

4.3.x)**(Project-unique identifier of interface)** .This subclause (beginning with 4.3.x) shall identify an interface by project-unique identifier, shall briefly identify the interfacing enti-

ties, and should be divided as needed to describe the interface characteristics of one or both of the interfacing entities. If a given interfacing entity is not covered by this SDD (for example, an external system) but its interface characteristics need to be mentioned to describe interfacing entities that are, these characteristics shall be stated as assumptions or as "When [the entity not covered] does this, [the entity that is covered] will ... ." This subclause may reference other documents (such as data dictionaries, standards for protocols, and standards for user interfaces) in place of stating the information here. The design description shall include the following, as applicable, presented in any order suited to the information to be provided, and shall note any differences in these characteristics from the point of view of the interfacing entities (such as different expectations about the size, frequency, or other characteristics of data elements):

a) Priority assigned to the interface by the interfacing entity(ies)
b) Type of interface (such as real-time data transfer, storage-and-retrieval of data, etc.) to be implemented
c) Characteristics of individual data elements that the interfacing entity(ies) will provide, store, send, access, receive, etc., such as:
1) Names/identifiers
a) Project-unique identifier
b) Non-technical (natural language) name
c) Standard data element name
d) Technical name (e.g., variable or field name in code or database)
e) Abbreviation or synonymous names
2) Data type (alphanumeric, integer, etc.)
3) Size and format (such as length and punctuation of a character string)
4) Units of measurement (such as meters, dollars, nanoseconds)
5) Range or enumeration of possible values (such as 0-99)
6) Accuracy (how correct) and precision (number of significant digits)
7) Priority, timing, frequency, volume, sequencing, and other constraints, such as whether the data element may be updated and whether business rules apply
8) Security and privacy protection constraints
9) Sources (setting/sending entities) and recipients (using/receiving entities)
d) Characteristics of data element assemblies (records, messages, files, arrays, displays, reports, etc.) that the interfacing entity(ies) will provide, store, send, access, receive, etc., such as:
1) Names/identifiers
a) Project-unique identifier
b) Non-technical (natural language) name
c) Technical name (e.g., record or data structure name in code or database)
d) Abbreviations or synonymous names
2) Data elements in the assembly and their structure (number, order, grouping)
3) Medium (such as disk) and structure of data elements/assemblies on the medium
4) Visual and auditory characteristics of displays and other outputs (such as colors, layouts, fonts, icons and other display elements, beeps, lights)
5) Relationships among assemblies, such as sorting/access characteristics
6) Priority, timing, frequency, volume, sequencing, and other constraints, such as whether the assembly may be updated and whether business rules apply
7) Security and privacy protection constraints
8) Sources (setting/sending entities) and recipients (using/receiving entities)
e) Characteristics of communication methods that the interfacing entity(ies) will use for the interface, such as:
1) Project-unique identifier(s)
2) Communication links/bands/frequencies/media and their characteristics
3) Message formatting
4) Flow control (such as sequence numbering and buffer allocation)

5) Data transfer rate, whether periodic/aperiodic, and interval between transfers
6) Routing, addressing, and naming conventions
7) Transmission services, including priority and grade
8) Safety/security/privacy protection considerations, such as encryption, user authentication, compartmentalization, and auditing

f) Characteristics of protocols that the interfacing entity(ies) will use for the interface, such as:

1) Project-unique identifier(s)
2) Priority/layer of the protocol
3) Packeting, including fragmentation and reassembly, routing, and addressing
4) Legality checks, error control, and recovery procedures
5) Synchronization, including connection establishment, maintenance, termination
6) Status, identification, and any other reporting features

g) Other characteristics, such as physical compatibility of the interfacing entity(ies) (dimensions, tolerances, loads, voltages, plug compatibility, etc.)

5) **Software item detailed design** .This clause should be divided into the following subclauses to describe each software unit of the software item. If part or all of the design depends upon system states or modes, this dependency shall be indicated. If design information falls into more than one subclause, it may be presented once and referenced from the other subclauses. Design conventions needed to understand the design shall be presented or referenced. Interface characteristics of software units may be described here, in clause 4, or in Interface Design Descriptions (IDDs). Software units that are databases, or that are used to access or manipulate databases, may be described here or in Database Design Descriptions (DBDDs).

5.x) **(Project-unique identifier of a software unit, or designator of a group of software units)** .This subclause shall identify a software unit by project-unique identifier and shall describe the unit. The description shall include the following information, as applicable. Alternatively, this subclause may designate a group of software units and identify and describe the software units in subordinate subclauses. Software units that contain other software units may reference the descriptions of those units rather than repeating information.

a) Unit design decisions, if any, such as algorithms to be used, if not previously selected
b) Any constraints, limitations, or unusual features in the design of the software unit
c) The programming language to be used and rationale for its use if other than the specified software item language
d) If the software unit consists of or contains procedural commands (such as menu selections in a database management system (DBMS) for defining forms and reports, on-line DBMS queries for database access and manipulation, input to a graphical user interface (GUI) builder for automated code generation, commands to the operating system, or shell scripts), a list of the procedural commands and reference to user manuals or other documents that explain them
e) If the software unit contains, receives, or outputs data, a description of its inputs, outputs, and other data elements and data element assemblies, as applicable. Subclause 4.3.x of the SDD provides a list of topics to be covered, as applicable. Data local to the software unit may be described separately from data input to or output from the software unit. If the software unit is a database, a corresponding Database Design Description (DBDD) may be referenced; interface characteristics may be provided here or by referencing clause 4 or the corresponding Interface Design Description(s).
f) If the software unit contains logic, the logic to be used by the software unit, including, as applicable:

1) Conditions in effect within the software unit when its execution is initiated
2) Conditions under which control is passed to other software units
3) Response and response time to each input, including data conversion, renaming, and data transfer operations
4) Sequence of operations and dynamically controlled sequencing during the software unit's operation, including:

a) The method for sequence control
b) The logic and input conditions of that method, such as timing variations, priority assignments
c) Data transfer in and out of memory
d) The sensing of discrete input signals, and timing relationships between interrupt operations within the software unit

5) Exception and error handling

6) **Requirements traceability** . This clause shall contain:
   a) Traceability from each software unit identified in this SDD to the software item requirements allocated to it. (Alternatively, this traceability may be provided in 4.1.)
      Note: Each level of software item refinement may result in requirements not directly traceable to higher-level requirements. For example, a software architectural design that creates two software units may result in requirements about how the software units will interface, even though these interfaces are not covered in software item requirements. Such requirements may be traced to a general requirement such as “software item” or to the software design decisions that resulted in their generation.
   b) Traceability from each software item requirement to the software units to which it is allocated.

7) **Notes** .This clause shall contain any general information that aids in understanding this document (e.g., background information, glossary, rationale). This clause shall include an alphabetical listing of all acronyms, abbreviations, and their meanings as used in this document and a list of any terms and definitions needed to understand this document.

A) **Annexes** . Annexes may be used to provide information published separately for convenience in document maintenance (e.g., charts, classified data). As applicable, each annex shall be referenced in the main body of the document where the data would normally have been provided. Annexes may be bound as separate documents for ease in handling. Annexes shall be lettered alphabetically (A, B, etc.).

Annex H

(normative)

Annex H Qualification testing software product descriptions

H.1)Scope

This annex specifies the contents of software products associated with qualification testing in this standard (the Software Test Plan is found together with other plans in annex E). It applies regardless of whether the software products are deliverable. This annex is a normative (that is, binding) part of this standard, subject to tailoring.

H.2)Software products covered

This following subclauses describe the contents of the software products covered by this annex. The products are listed in the order they are referenced in this standard and include the following:

a)) Software Test Description (STD)
b)) Software Test Report (STR)

H.2.1 Contents of the Software Test Description (STD)

SOFTWARE TEST DESCRIPTION (STD)

Contents

1) Scope
   1.1) Identification
   1.2) System overview
   1.3) Document overview
2) Referenced documents
3) Test preparations
   3.x) (project-unique identifier of a test)
      3.x.1)Hardware preparation
      3.x.2)Software preparation
      3.x.3)Other pre-test preparations
4) Test descriptions
   4.x) (Project-unique identifier of a test)
      4.x.y)(Project-unique identifier of a test case)
      4.x.y.1)Requirements addressed
      4.x.y.2)Prerequisite conditions
      4.x.y.3)Test input
      4.x.y.4)Expected test results
      4.x.y.5)Criteria for evaluating results
      4.x.y.6)Test procedure
      4.x.y.7)Assumptions and constraints

5) Requirements traceability
6) Notes
A) Annexes
1) **Scope** . This clause should be divided into the following subclauses.
   1.1) **Identification** .This subclause shall contain a full identification of the system and the software to which this document applies, including, as applicable, identification number(s), title(s), abbreviation(s), version number(s), and release number(s).
   1.2) **System overview** .This subclause shall briefly state the purpose of the system and the software to which this document applies. It shall describe the general nature of the system and software; summarize the history of system development, operation, and maintenance; identify the project sponsor, acquirer, user, developer, and maintenance organizations; identify current and planned operating sites; and list other relevant documents.
   1.3) **Document overview** .This subclause shall summarize the purpose and contents of this document and shall describe any security or privacy protection considerations associated with its use.
2) **Referenced documents** .This clause shall list the number, title, revision, date, and source of all documents referenced in this manual.
3) **Test preparations** . This clause should be divided into the following subclauses. Safety precautions, marked by WARNING or CAUTION, and security and privacy protection considerations shall be included as applicable.
   3.x) **(Project-unique identifier of a test)** . This subclause shall identify a test by project-unique identifier, shall provide a brief description, and should be divided into the following. When the information required duplicates information previously specified for another test, that information may be referenced rather than repeated.
      3.x.1)**Hardware preparation** . This subclause shall describe the procedures necessary to prepare the hardware for the test. Reference may be made to published operating manuals for these procedures. The following shall be provided, as applicable:
      a) The specific hardware to be used, identified by name and, if applicable, number
      b) Any switch settings and cabling necessary to connect the hardware
      c) One or more diagrams to show hardware, interconnecting control, and data paths
      d) Step-by-step instructions for placing the hardware in a state of readiness
      3.x.2)**Software preparation** . This subclause shall describe the procedures necessary to prepare the item(s) under test and any related software, including data, for the test. Reference may be made to published software manuals for these procedures. The following information shall be provided, as applicable:
      a) The specific software to be used in the test
      b) The storage medium of the item(s) under test (e.g., magnetic tape, diskette)
      c) The storage medium of any related software (e.g., simulators, test drivers, databases)
      d) Instructions for loading the software, including required sequence
      e) Instructions for software initialization common to more than one test case
      3.x.3)**Other pre-test preparations** .This subclause shall describe any other pre-test personnel actions, preparations, or procedures necessary to perform the test.
4) **Test descriptions** . This clause should be divided into the following subclauses. Safety precautions, marked by WARNING or CAUTION, and security and privacy protection considerations shall be included as applicable.
   4.x) **(Project-unique identifier of a test)** .This subclause shall identify a test by project-unique identifier and should be divided into the following. When the required information duplicates information previously provided, that information may be referenced rather than repeated.
      4.x.y)**(Project-unique identifier of a test case)** .This subclause shall identify a test case by project-unique identifier, state its purpose, and provide a brief description. The following shall provide a detailed description of the test case.
      4.x.y.1)**Requirements addressed** .This subclause shall identify the software item or system requirements addressed by the test case. (Alternatively, this information may be provided in 5.a.)

4.x.y.2)**Prerequisite conditions** . This subclause shall identify any prerequisite conditions that are required to be established prior to performing the test case. The following considerations shall be discussed, as applicable:

a) Hardware and software configuration
b) Flags, initial breakpoints, pointers, control parameters, or initial data to be set/reset prior to test commencement
c) Preset hardware conditions or electrical states necessary to run the test case
d) Initial conditions to be used in making timing measurements
e) Conditioning of the simulated environment
f) Other special conditions peculiar to the test case

4.x.y.3)**Test input** . This subclause shall describe the test input necessary for the test case. The following shall be provided, as applicable:

a) Name, purpose, and description (e.g., range of values, accuracy) of each test input
b) Source of the test input and the method to be used for selecting the test input
c) Whether the test input is real or simulated
d) Time or event sequence of test input
e) The manner in which the input data will be controlled to:

1) Test the item(s) with a minimum/reasonable number of data types and values
2) Exercise the item(s) with a range of valid data types and values that test for overload, saturation, and other “worst case” effects
3) Exercise the item(s) with invalid data types and values to test for appropriate handling of irregular inputs
4) Permit retesting, if necessary

4.x.y.4)**Expected test results** .This subclause shall identify all expected test results for the test case. Both intermediate and final test results shall be provided, as applicable.

4.x.y.5)**Criteria for evaluating results** .This subclause shall identify the criteria to be used for evaluating the intermediate and final results of the test case. For each test result, the following information shall be provided, as applicable:

a) The range or accuracy over which an output can vary and still be acceptable
b) Minimum number of combinations or alternatives of input and output conditions that constitute an acceptable test result
c) Maximum/minimum allowable test duration, in terms of time or number of events
d) Maximum number of interrupts, halts, or other system breaks that may occur
e) Allowable severity of processing errors
f) Conditions under which the result is inconclusive and re-testing is to be performed
g) Conditions under which the output is to be interpreted as indicating irregularities in input test data, in the test database/data files, or in test procedures
h) Allowable indications of the control, status, and results of the test and the readiness for the next test case (may be output of auxiliary test software)
i) Additional criteria not mentioned above.

4.x.y.6)**Test procedure** .This subclause shall define the test procedure for the test case. The test procedure shall be defined as a series of individually numbered steps listed sequentially in the order in which the steps are to be performed. For convenience in document maintenance, the test procedures may be included as an annex and referenced in this subclause. The appropriate level of detail in each test procedure depends on the type of software being tested. For some software, each keystroke may be a separate test procedure step; for most software, each step may include a logically related series of keystrokes or other actions. The appropriate level of detail is the level at which it is useful to specify expected results and compare them to actual results. The following shall be provided for each test procedure, as applicable:

a) Test operator actions and equipment operation required for each step, including commands, as applicable, to:

1) Initiate the test case and apply test input
2) Inspect test conditions

3) Perform interim evaluations of test results
4) Record data
5) Halt or interrupt the test case
6) Request data dumps or other aids, if needed
7) Modify the database/data files
8) Repeat the test case if unsuccessful
9) Apply alternate modes as required by the test case
10) Terminate the test case

b) Expected result and evaluation criteria for each step

c) If the test case addresses multiple requirements, identification of which test procedure step(s) address which requirements. (Alternatively, this information may be provided in 5.)

d) Actions to follow in the event of a program stop or indicated error, such as:

1) Recording of critical data from indicators for reference purposes
2) Halting or pausing time-sensitive test-support software and test apparatus
3) Collection of system and operator records of test results

e) Procedures to be used to reduce and analyze test results to accomplish the following, as applicable:

1) Detect whether an output has been produced
2) Identify media and location of data produced by the test case
3) Evaluate output as a basis for continuation of test sequence
4) Evaluate test output against required output

4.x.y.7) **Assumptions and constraints** .This subclause shall identify any assumptions made and constraints or limitations imposed in the description of the test case due to system or test conditions, such as limitations on timing, interfaces, equipment, personnel, and database/ data files. If waivers or exceptions to specified limits and parameters are approved, they shall be identified and this subclause shall address their effects and impacts upon the test case.

5) **Requirements traceability** .This subclause shall contain:

a) Traceability from each test case in this STD to the system or software item requirements it addresses. If a test case addresses multiple requirements, traceability from each set of test procedure steps to the requirements addressed. (Alternatively, this traceability may be provided in 4.x.y.1.)

b) Traceability from each system or software item requirement covered by this STD to the test case(s) that address it. For software item testing, traceability from each software item requirement in the software item's Software Requirements Specification (SRS) and associated Interface Requirements Specifications (IRSs). For system testing, traceability from each system requirement in the system's System/Subsystem Specification (SSS) and associated IRSs. If a test case addresses multiple requirements, the traceability shall indicate the particular test procedure steps that address each requirement.

6) **Notes** .This clause shall contain any general information that aids in understanding this document (e.g., background information, glossary, rationale). This clause shall include an alphabetical listing of all acronyms, abbreviations, and their meanings as used in this document and a list of any terms and definitions needed to understand this document.

A) **Annexes** . Annexes may be used to provide information published separately for convenience in document maintenance (e.g., charts, classified data). As applicable, each annex shall be referenced in the main body of the document where the data would normally have been provided. Annexes may be bound as separate documents for ease in handling. Annexes shall be lettered alphabetically (A, B, etc.).

H.2.2 Contents of the Software Test Report (STR)

SOFTWARE TEST REPORT (STR)

Contents

1) Scope
   1.1) Identification
   1.2) System overview
   1.3) Document overview
2) Referenced documents
3) Overview of test results
   3.1) Overall assessment of the software tested
   3.2) Impact of test environment
   3.3) Recommended improvements
4) Detailed test results
   4.x) (Project-unique identifier of a test)
      4.x.1)Summary of test results
      4.x.2)Problems encountered
      4.x.2.y)(Project-unique identifier of a test case)
      4.x.3)Deviations from test cases/procedures
      4.x.3.y)(Project-unique identifier of a test case)
5) Test log
6) Notes

A) Annexes

1) **Scope** . This clause should be divided into the following subclauses.
   1.1) **Identification** . This subclause shall contain a full identification of the system and the software to which this document applies, including, as applicable, identification number(s), title(s), abbreviation(s), version number(s), and release number(s).
   1.2) **System overview** .This subclause shall briefly state the purpose of the system and the software to which this document applies. It shall describe the general nature of the system and software; summarize the history of system development, operation, and maintenance; identify the project sponsor, acquirer, user, developer, and maintenance organizations; identify current and planned operating sites; and list other relevant documents.
   1.3) **Document overview** .This subclause shall summarize the purpose and contents of this document and shall describe any security or privacy protection considerations associated with its use.
2) **Referenced documents** .This clause shall list the number, title, revision, date, and source of all documents referenced in this manual.
3) **Overview of test results** . This clause should be divided into the following subclauses to provide an overview of test results.
   3.1) **Overall assessment of the software tested** .This subclause shall:
      a) Provide an overall assessment of the software as demonstrated by the test results in this report
      b) Identify any remaining deficiencies, limitations, or constraints that were detected by the testing performed. Problem/change reports may be used to provide deficiency information.
      c) For each remaining deficiency, limitation, or constraint, describe:
      1) Its impact on software and system performance, including identification of requirements not met
      2) The impact on software and system design to correct it
      3) A recommended solution/approach for correcting it
   3.2) **Impact of test environment** .This subclause shall provide an assessment of the manner in which the test environment may be different from the operational environment and the effect of this difference on the test results.
   3.3) **Recommended improvements** .This subclause shall provide any recommended improvements in the design, operation, or testing of the software tested. A discussion of each recommenda-

tion and its impact on the software may be provided. If no recommended improvements are provided, this subclause shall state "None."

4) **Detailed test results** .This clause should be divided into the following subclauses to describe the detailed results for each test. Note: The word "test" means a related collection of test cases.

4.x) **(Project-unique identifier of a test)** .This subclause shall identify a test by project-unique identifier and should be divided into the following to describe the test results.

4.x.1)**Summary of test results** .This subclause shall summarize the results of the test. The summary shall include, possibly in a table, the completion status of each test case associated with the test (for example, "all results as expected," "problems encountered," "deviations required"). When the completion status is not "as expected," this subclause shall reference the following subclauses for details.

4.x.2)**Problems encountered** .This subclause should be divided into subclauses that identify each test case in which one or more problems occurred.

4.x.2.y)**(Project-unique identifier of a test case)** .This subclause shall identify by project-unique identifier a test case in which one or more problems occurred, and shall provide:

a) A brief description of the problem(s) that occurred
b) Identification of the test procedure step(s) in which they occurred
c) Reference(s) to the associated problem/change report(s) and backup data, as applicable
d) The number of times the procedure or step was repeated in attempting to correct the problem(s) and the outcome of each attempt
e) Back-up points or test steps where tests were resumed for retesting

4.x.3)**Deviations from test cases/procedures** .This subclause should be divided into subclauses that identify each test case in which deviations from test case/test procedures occurred.

4.x.3.y)**(Project-unique identifier of a test case)** .This subclause shall identify by project-unique identifier a test case in which one or more deviations occurred, and shall provide:

a) A description of the deviations) (for example, test case run in which the deviation occurred and nature of the deviation, such as substitution of required equipment, procedural steps not followed, schedule deviations). (Red-lined test procedures may be used to show the deviations)
b) The rationale for the deviation(s)
c) An assessment of the deviations' impact on the validity of the test case

5) **Test log .** This clause shall present, possibly in a figure or annex, a chronological record of the test events covered by this report. This test log shall include:

a) The date(s), time(s), and location(s) of the tests performed
b) The hardware and software configurations used for each test including, as applicable, part/model/serial number, manufacturer, revision level, and calibration date of all hardware, and version number and name for the software components used
c) The date and time of each test-related activity, the identity of the individual(s) who performed the activity, and the identities of witnesses, as applicable

6) **Notes .** This clause shall contain any general information that aids in understanding this document (e.g., background information, glossary, rationale). This clause shall include an alphabetical listing of all acronyms, abbreviations, and their meanings as used in this document and a list of any terms and definitions needed to understand this document.

A) **Annexes** . Annexes may be used to provide information published separately for convenience in document maintenance (e.g., charts, classified data). As applicable, each annex shall be referenced in the main body of the document where the data would normally have been provided. Annexes may be bound as separate documents for ease in handling. Annexes shall be lettered alphabetically (A, B, etc.).

Annex I

(normative)

Maintenance software product descriptions

I.1 Scope

This annex specifies the contents of software products associated with maintenance in this standard. It applies regardless of whether the software products are deliverable. This annex is a normative (that is, binding) part of this standard, subject to tailoring.

I.2 Software products covered

This following subclauses describe the contents of the software products covered by this annex. The products are listed in the order they are referenced in this standard and include the following:

a)) Software Product Specification (SPS)
b)) Software Version Description (SVD)
c)) Computer Programming Manual (CPM)
d)) Firmware Support Manual (FSM)

I.2.1 Contents of the Software Product Specification (SPS)

SOFTWARE PRODUCT SPECIFICATION (SPS)

Contents

1) Scope
   1.1) Identification
   1.2) System overview
   1.3) Document overview
2) Referenced documents
3) Requirements
   3.1) Executable software
   3.2) Source files
   3.3) Packaging requirements
4) Qualification provisions
5) Software maintenance information
   5.1) “As built” software design
   5.2) Compilation/build procedures
   5.3) Modification procedures
   5.4) Computer hardware resource utilization
6) Requirements traceability
7) Notes
A) Annexes

1) **Scope** .This clause should be divided into the following subclauses.
   1.1) **Identification** .This subclause shall contain a full identification of the system and the software to which this document applies, including, as applicable, identification number(s), title(s), abbreviation(s), version number(s), and release number(s).
   1.2) **System overview** .This subclause shall briefly state the purpose of the system and the software to which this document applies. It shall describe the general nature of the system and software; summarize the history of system development, operation, and maintenance; identify the project sponsor, acquirer, user, developer, and maintenance organizations; identify current and planned operating sites; and list other relevant documents.
   1.3) **Document overview** .This subclause shall summarize the purpose and contents of this document and shall describe any security or privacy protection considerations associated with its use.
2) **Referenced documents** .This clause shall list the number, title, revision, date, and source of all documents referenced in this manual.
3) **Requirements** .This clause should be divided into the following subclauses to achieve delivery of the software and to establish the requirements that another body of software is required to meet to be considered a valid copy of the software item.Note: In past versions of the SPS, clause 3 required a presentation of the software design describing the "as built" software. That approach was modeled on hardware development, in which the final product is a design to which hardware items are required to be manufactured. For software, however, this approach does not apply. Software "manufacturing" consists of electronic duplication of the software itself, not recreation from design, and the validity of a "manufactured" copy is determined by comparison to the software itself, not to a design description. This clause therefore establishes the software itself as the criterion that is required to be matched for a body of software to be considered a valid copy of the software item. The updated software design has been placed in clause 5 below, not as a requirement, but as information to be used to modify, enhance, or otherwise maintain the software. Clause 3 is the only portion of this specification to be placed under acquirer configuration control. It is the software itself that establishes the product baseline, not a description of the software's design.
   3.1) **Executable software** .This subclause shall provide, by reference to enclosed or otherwise provided electronic media, the executable software for the software item, including any batch files, command files, data files, or other software files needed to install and operate the software on its target computer(s). In order for a body of software to be considered a valid copy of the software item's executable software, it is required to be shown to match these files exactly.
   3.2) **Source files** .This subclause shall provide, by reference to enclosed or otherwise provided electronic media, the source files for the software item, including any batch files, command files, data files, or other files needed to regenerate the executable software for the software item. In order for a body of software to be considered a valid copy of the software item's source files, it is required to be shown to match these files exactly.
   3.3) **Packaging requirements** .This subclause shall state the requirements, if any, for packaging and marking copies of the software item.
4) **Qualification provisions** .This subclause shall state the method(s) to be used to demonstrate that a given body of software is a valid copy of the software item. For example, the method for executable files might be to establish that each executable file referenced in 3.1 has an identically-named counterpart in the software in question and that each such counterpart can be shown, via bit-for-bit comparison, check sum, or other method, to be identical to the corresponding executable file. The method for source files might be comparable, using the source files referenced in 3.2.
5) **Software maintenance information** .This clause should be divided into the following subclauses to provide information needed to maintain the software item.
   5.1) **"As built" software design** .This subclause shall contain, or reference an annex or other deliverable document that contains, information describing the design of the "as built" software item. The information shall be the same as that required in a Software Design Description (SDD), Interface Design Description (IDD), and Database Design Description (DBDD), as applicable. If these documents or their equivalents are to be delivered for the "as built" software item, this subclause shall reference them. If not, the information shall be provided in this

document. Information provided in the headers, comments, and code of the source code listings may be referenced and need not be repeated in this clause. If the SDD, IDD, or DBDD is included in an annex, the subclause numbers and page numbers need not be changed.

5.2) **Compilation/build procedures** .This subclause shall describe, or reference an annex that describes, the compilation/build process to be used to create the executable files from the source files and to prepare the executable files to be loaded into firmware or other distribution media. It shall specify the compiler(s)/assembler(s) to be used, including version numbers; other hardware and software needed, including version numbers; any settings, options, or conventions to be used; and procedures for compiling/assembling, linking, and building the software item and the software system/subsystem containing the software item, including variations for different sites, configurations, versions, etc. Build procedures above the software item level may be presented in one SPS and referenced from the others.

5.3) **Modification procedures** .This subclause shall describe procedures that are required to be followed to modify the software item. It shall include or reference information on the following, as applicable:

a) Maintenance facilities, equipment, and software, and procedures for their use
b) Databases/data files used by the software item and procedures for using and modifying them
c) Design, coding, and other conventions to be followed
d) Compilation/build procedures if different from those above
e) Integration and testing procedures to be followed

5.4) **Computer hardware resource utilization** .This subclause shall describe the “as built” software item’s measured utilization of computer hardware resources (such as processor capacity, memory capacity, input/output device capacity, auxiliary storage capacity, and communications/network equipment capacity). It shall cover all computer hardware resources included in utilization requirements for the software item, in system-level resource allocations affecting the software item, or in the Software Development Plan. If all utilization data for a given computer hardware resource is presented in a single location, such as in one SPS, this subclause may reference that source. Included for each computer hardware resource shall be:

a) The software item requirements or system-level resource allocations being satisfied. (Alternatively, the traceability to software item requirements may be provided in 6.c.)
b) The assumptions and conditions on which the utilization data are based (for example, typical usage, worst-case usage, assumption of certain events)
c) Any special considerations affecting the utilization (such as use of virtual memory, overlays, or multiprocessors or the impacts of operating system overhead, library software, or other implementation overhead)
d) The units of measure used (such as percentage of processor capacity, cycles per second, bytes of memory, kilobytes per second)
e) The level(s) at which the estimates or measures have been made (such as software unit, software item, or executable program)

6) **Requirements traceability** .This clause shall provide:

a) Traceability from each software item source file to the software unit(s) that it implements.
b) Traceability from each software unit to the source files that implement it.
c) Traceability from each computer hardware resource utilization measurement given in 5.4 to the software item requirements it addresses. (Alternatively, this traceability may be provided in 5.4.)
d) Traceability from each software item requirement regarding computer hardware resource utilization to the utilization measurements given in 5.4.

7) **Notes** .This clause shall contain any general information that aids in understanding this specification (e.g., background information, glossary, rationale). This clause shall include an alphabetical listing of all acronyms, abbreviations, and their meanings as used in this document and a list of any terms and definitions needed to understand this document.

A) **Annexes** . Annexes may be used to provide information published separately for convenience in document maintenance (e.g., charts, classified data). As applicable, each annex shall be referenced

in the main body of the document where the data would normally have been provided. Annexes may be bound as separate documents for ease in handling. Annexes shall be lettered alphabetically (A, B, etc.).

I.2.2 Contents of the Software Version Description (SVD)

SOFTWARE VERSION DESCRIPTION (SVD)

Contents

1) Scope
   1.1) Identification
   1.2) System overview
   1.3) Document overview
2) Referenced documents
3) Version description
   3.1) Inventory of materials released
   3.2) Inventory of software contents
   3.3) Changes installed
   3.4) Adaptation data
   3.5) Related documents
   3.6) Installation instructions
   3.7) Possible problems and known errors
4) Notes

A) Annexes

1) **Scope** .This clause should be divided into the following subclauses.
   1.1) **Identification** .This subclause shall contain a full identification of the system and the software to which this document applies, including, as applicable, identification number(s), title(s), abbreviation(s), version number(s), and release number(s). It shall also identify the intended recipients of the SVD to the extent that this identification affects the contents of the software released (for example, source code may not be released to all recipients.)
   1.2) **System overview** .This subclause shall briefly state the purpose of the system and the software to which this document applies. It shall describe the general nature of the system and software; summarize the history of system development, operation, and maintenance; identify the project sponsor, acquirer, user, developer, and maintenance organizations; identify current and planned operating sites; and list other relevant documents.
   1.3) **Document overview** .This subclause shall summarize the purpose and contents of this document and shall describe any security or privacy protection considerations associated with its use.
2) **Referenced documents** .This clause shall list the number, title, revision, date, and source of all documents referenced in this manual.
3) **Version description** .This clause should be divided into the following subclauses.
   3.1) **Inventory of materials released** .This subclause shall list by identifying numbers, titles, abbreviations, dates, version numbers, and release numbers, as applicable, all physical media (for example, listings, tapes, disks) and associated documentation that make up the software version being released. It shall include applicable security and privacy protection considerations for these items, safeguards for handling them, such as concerns for static and magnetic fields, and instructions and restrictions regarding duplication and license provisions.
   3.2) **Inventory of software contents** .This subclause shall list by identifying numbers, titles, abbreviations, dates, version numbers, and release numbers, as applicable, all computer files that make up the software version being released. Any applicable security and privacy protection considerations shall be included.

3.3) **Changes installed** .This subclause shall contain a list of all changes incorporated into the software version since the previous version. If classes or categories of changes have been used, the changes shall be separated into these classes or categories. This subclause shall identify, as applicable, the problem reports, change proposals, and change notices associated with each change and the effects, if any, of each change on system operation and on interfaces with other hardware and software. This subclause does not apply to the initial software version.

3.4) **Adaptation data** .This subclause shall identify or reference all unique-to-site data contained in the software version. For software versions after the first, this subclause shall describe changes made to the adaptation data.

3.5) **Related documents** .This subclause shall list by identifying numbers, titles, abbreviations, dates, version numbers, and release numbers, as applicable, all documents pertinent to the software version being released but not included in the release.

3.6) **Installation instructions** .This subclause shall provide or reference the following information, as applicable:

a) Instructions for installing the software version
b) Identification of other changes that have to be installed for this version to be used, including site-unique adaptation data not included in the software version
c) Security, privacy protection, or safety precautions relevant to the installation
d) Procedures for determining whether the version has been installed properly
e) A point of contact to be consulted if there are problems or questions with the installation

3.7) **Possible problems and known errors** .This subclause shall identify any possible problems or known errors with the software version at the time of release, any steps being taken to resolve the problems or errors, and instructions (either directly or by reference) for recognizing, avoiding, correcting, or otherwise handling each one. The information presented shall be appropriate to the intended recipient of the SVD (for example, a user organization may need advice on avoiding errors, a maintenance organization on correcting them).

4) **Notes** .This clause shall contain any general information that aids in understanding this document (e.g., background information, glossary, rationale). This clause shall include an alphabetical listing of all acronyms, abbreviations, and their meanings as used in this document and a list of any terms and definitions needed to understand this document.

A) **Annexes** . Annexes may be used to provide information published separately for convenience in document maintenance (e.g., charts, classified data). As applicable, each annex shall be referenced in the main body of the document where the data would normally have been provided. Annexes may be bound as separate documents for ease in handling. Annexes shall be lettered alphabetically (A, B, etc.).

I.2.3 Contents of the Computer Programming Manual (CPM)

COMPUTER PROGRAMMING MANUAL (CPM)

Contents

1) Scope
   1.1) Identification
   1.2) Computer system overview
   1.3) Document overview
2) Referenced documents
3) Programming environment
4) Programming information
5) Notes

A) Annexes

1) **Scope** .This clause should be divided into the following subclauses.

1.1) **Identification** .This subclause shall contain the manufacturer's name, model number, and any other identifying information for the computer system to which this document applies.

1.2) **Computer system overview** .This subclause shall briefly state the purpose of the computer system to which this document applies.

1.3) **Document overview** .This subclause shall summarize the purpose and contents of this manual and shall describe any security or privacy protection considerations associated with its use.

2) **Referenced documents** .This clause shall list the number, title, revision, date, and source of all documents referenced in this manual.

3) **Programming environment** .This clause should be divided into subclauses as appropriate to provide the following information.

a) The components and configuration of the computer system

b) Operating characteristics, capabilities, and limitations, including, as applicable:

1) Machine cycle time
2) Word length
3) Memory capacity and characteristics
4) Instruction set characteristics
5) Interrupt capabilities
6) Modes of operation (e.g., batch, interactive, privileged, non-privileged)
7) Operational registers
8) Error indicators
9) Input/output characteristics
10) Special features

c) Description of the equipment (e.g., tapes, disks, other peripheral equipment) necessary to perform compilations and assemblies on the computer system. Identify (as applicable) by name and version number the editor, linker, link-editor, compiler, assembler, cross-compilers, cross-assemblers, and other utilities used, and reference appropriate manuals describing their use. Highlight any special flags or instructions necessary for loading, executing, or recording the results.

4) **Programming information** .This clause should be divided into subclauses as appropriate to provide the following information.

a) Description of the programming features of the computer's instruction set architecture, including, as applicable:

1) Data representation (e.g., byte, word, integer, floating-point, double precision)
2) Instruction formats and addressing modes
3) Special registers and words (e.g., stack pointer, program counter)
4) Control instructions (e.g., branch, jump, subroutine and procedure call instructions, privileged instructions, and the modes they operate in)
5) Subroutines and procedures (e.g., non-reentrant, reentrant, macrocode routines, argument lists, parameter passing conventions)
6) Interrupt processing
7) Timers and clocks
8) Memory protection features (e.g., read-only memory)
9) Additional features, such as instruction or data cache architecture

b) Description of each instruction, including, as applicable:

1) Use
2) Syntax
3) Condition codes set
4) Execution time
5) Machine-code format
6) Mnemonic conventions
7) Other characteristics

c) Description of input and output control programming, including, as applicable:

1) Initial loading and verification of computer memory
2) Serial and parallel data channels

3) Discrete input and output
4) Interface components
5) Device numbers, operational codes, and memory locations for peripheral equipment

d) Additional, restricted, or special programming techniques associated with the computer system (e.g., a concise description of the microprogram control clause)
e) Examples that demonstrate the programming features described above, including examples of the proper use of all categories of instructions on the computer system
f) Error detection and diagnostic features associated with the computer system, including condition codes, overflow and addressing exception interrupts, and input and output error status indicators

5) **Notes** .This clause shall contain any general information that aids in understanding this document (e.g., background information, glossary, rationale). This clause shall include an alphabetical listing of all acronyms, abbreviations, and their meanings as used in this document and a list of terms and definitions needed to understand this document.

A) **Annexes** . Annexes may be used to provide information published separately for convenience in document maintenance (e.g., charts, classified data). As applicable, each annex shall be referenced in the main body of the document where the data would normally have been provided. Annexes may be bound as separate documents for ease in handling. Annexes shall be lettered alphabetically (A, B, etc.).

I.2.4 Contents of the Firmware Support Manual (FSM)

FIRMWARE SUPPORT MANUAL (FSM)

Contents

1) Scope
   1.1) Identification
   1.2) System overview
   1.3) Document overview
2) Referenced documents
3) Firmware programming instructions
   3.x) (identifier of programmed firmware device)
      3.x.1)Description of pre-programmed device
      3.x.2)Software to be programmed into the device
      3.x.3)Programming equipment
      3.x.4)Programming software
      3.x.5)Programming procedures
      3.x.6)Installation and repair procedures
      3.x.7)Vendor information
4) Notes

A) Annexes

1) **Scope** .This clause should be divided into the following subclauses.

1.1) **Identification** .This subclause shall contain a full identification of the system, software, and firmware devices to which this document applies, including, as applicable, identification number(s), title(s), abbreviations), version number(s), and release number(s) of the system and software and manufacturer's name and model number for each firmware device.

1.2) **System overview** .This subclause shall briefly state the purpose of the system and the software to which this document applies. It shall describe the general nature of the system and software; summarize the history of system development, operation, and maintenance; identify the project sponsor, acquirer, user, developer, and maintenance organizations; identify current and planned operating sites; and list other relevant documents.

1.3) **Document overview** .This subclause shall summarize the purpose and contents of this manual and shall describe any security or privacy protection considerations associated with its use.

2) **Referenced documents** .This clause shall list the number, title, revision, date, and source of all documents referenced in this manual.

3) **Firmware programming instructions** .This clause should be divided into the following subclauses.

3.x) **(Identifier of programmed firmware device)** .This subclause shall state the project-unique identifier of a programmed firmware device to be used in the system and should be divided into the following.

3.x.1)**Description of pre-programmed device** .This subclause shall:

a) Identify by manufacturer's name and model number the firmware device to be programmed

b) Provide a complete physical description of the firmware device, including the following, as applicable:

1) Memory size, type, speed, and configuration (such as 64Kx1, 8Kx8)
2) Operating characteristics (such as access time, power requirements, logic levels)
3) Pin functional descriptions
4) Logical interfaces (such as addressing scheme, chip selection)
5) Internal and external identification scheme used
6) Timing diagrams

c) Describe the operational and environmental limits to which the firmware device may be subjected and still maintain satisfactory operation

3.x.2)**Software to be programmed into the device** .This subclause shall identify by project-unique identifier(s) the software to be programmed into the firmware device.

3.x.3)**Programming equipment** .This subclause shall describe the equipment to be used for programming and reprogramming the firmware device. It shall include computer equipment, general purpose equipment, and special equipment to be used for device erasure, loading, verification, and marking, as applicable. Each piece of equipment shall be identified by manufacturer's name, model number, and any other information that is necessary to uniquely identify that piece of equipment. A description of each piece of equipment shall be provided, including its purpose, usage, and major capabilities.

3.x.4)**Programming software** .This subclause shall describe the software to be used for programming and reprogramming the firmware device. It shall include software to be used for device erasure, loading, verification, and marking, as applicable. Each item of software shall be identified by vendor's name, software name, number, version/release, and any other information necessary to uniquely identify the item of software. A description of each item of software shall be provided, including its purpose, usage, and major capabilities.

3.x.5)**Programming procedures** .This subclause shall describe the procedures to be used for programming and reprogramming the firmware device. It shall include procedures to be used for device erasure, loading, verification, and marking, as applicable. All equipment and software necessary for each procedure shall be identified, together with any security and privacy protection measures to be applied.

3.x.6)**Installation and repair procedures** .This subclause shall contain the installation, replacement, and repair procedures for the firmware device. This subclause shall also include remove-and-replace procedures, device addressing scheme and implementation, description of the host board layout, and any procedures for ensuring continuity of operations in the event of emergencies. Safety precautions, marked by WARNING or CAUTION, shall be included where applicable.

3.x.7)**Vendor information** .This clause shall include or reference any relevant information supplied by the vendor(s) of the firmware device, programming equipment, or programming software.

4) **Notes** .This clause shall contain any general information that aids in understanding this document (e.g., background information, glossary, rationale). This clause shall include an alphabetical listing

of all acronyms, abbreviations, and their meanings as used in this document and a list of terms and definitions needed to understand this document.

A) **Annexes** . Annexes may be used to provide information published separately for convenience in document maintenance (e.g., charts, classified data). As applicable, each annex shall be referenced in the main body of the document where the data would normally have been provided. Annexes may be bound as separate documents for ease in handling. Annexes shall be lettered alphabetically (A, B, etc.).

Annex J

(normative)

User/operator software product descriptions

J.1 Scope

This annex specifies the contents of software products associated with user and operator manuals in this standard. It applies regardless of whether the software products are deliverable. This annex is a normative (that is, binding) part of this standard, subject to tailoring.

J.2 Software products covered

This following subclauses describe the contents of the software products covered by this annex. The products are listed in order they are referenced in this standard and include the following:

a)) Software User Manual (SUM)
b)) Software Input/Output Manual (SIOM)
c)) Software Center Operator Manual (SCOM)
d)) Computer Operation Manual (COM)

J.2.1 Contents of the Software User Manual (SUM)

SOFTWARE USER MANUAL (SUM)

Contents

1) Scope
   1.1) Identification
   1.2) System overview
   1.3) Document overview
2) Referenced documents
3) Software summary
   3.1) Software application
   3.2) Software inventory
   3.3) Software environment
   3.4) Software organization and overview of operation
   3.5) Contingencies and alternate states and modes of operation
   3.6) Security and privacy protection
   3.7) Assistance and problem reporting
4) Access to the software
   4.1) First-time user of the software
      4.1.1)Equipment familiarization
      4.1.2)Access control
      4.1.3)Installation and setup

4.2) Initiating a session
4.3) Stopping and suspending work

5) Processing reference guide
5.1) Capabilities
5.2) Conventions
5.3) Processing procedures
5.3.x)(Aspect of software use)
5.4) Related processing
5.5) Data backup
5.6) Recovery from errors, malfunctions, and emergencies
5.7) Messages
5.8) Quick-reference guide

6) Notes

A) Annexes

1) **Scope** .This clause should be divided into the following subclauses.
1.1) **Identification** .This subclause shall contain a full identification of the system and the software to which this document applies, including, as applicable, identification number(s), title(s), abbreviation(s), version number(s), and release number(s).
1.2) **System overview** .This subclause shall briefly state the purpose of the system and the software to which this document applies. It shall describe the general nature of the system and software; summarize the history of system development, operation, and maintenance; identify the project sponsor, acquirer, user, developer, and maintenance organizations; identify current and planned operating sites; and list other relevant documents.
1.3) **Document overview** .This subclause shall summarize the purpose and contents of this manual and shall describe any security or privacy protection considerations associated with its use.

2) **Referenced documents** .This clause shall list the number, title, revision, date, and source of all documents referenced in this manual.

3) **Software summary** .This clause should be divided into the following subclauses.
3.1) **Software application.** This subclause shall provide a brief description of the intended uses of the software. Capabilities, operating improvements, and benefits expected from its use shall be described.
3.2) **Software inventory** .This subclause shall identify all software files, including databases and data files, that are required to be installed for the software to operate. The identification shall include security and privacy protection considerations for each file and identification of the software necessary to continue or resume operation in case of an emergency.
3.3) **Software environment** .This subclause shall identify the hardware, software, manual operations, and other resources needed for a user to install and run the software. Included, as applicable, shall be identification of:
a) Computer equipment that is required to be present, including amount of memory needed, amount of auxiliary storage needed, and peripheral equipment such as printers and other input/output devices
b) Communications equipment that is required to be present
c) Other software that is required to be present, such as operating systems, databases, data files, utilities, and other supporting systems
d) Forms, procedures, or other manual operations that are required to be present
e) Other facilities, equipment, or resources that are required to be present
3.4) **Software organization and overview of operation** .This subclause shall provide a brief description of the organization and operation of the software from the user's point of view. The description shall include, as applicable:
a) Logical components of the software, from the user's point of view, and an overview of the purpose/operation of each component
b) Performance characteristics that can be expected by the user, such as:
1) Type, volume, rate of input accepted
2) Type, volume, accuracy, rate of output the software can produce

3) Typical response time and factors that affect it
4) Typical processing time and factors that affect it
5) Limitations, such as number of events that can be tracked
6) Error rate that can be expected
7) Reliability that can be expected

c) Relationship of the functions performed by the software with interfacing systems, organizations, or positions
d) Supervisory controls that can be implemented (such as passwords) to manage the software

3.5) **Contingencies and alternate states and modes of operation** .This subclause shall explain differences in what the user will be able to do with the software at times of emergency and in various states and modes of operation, if applicable.

3.6) **Security and privacy protection** .This subclause shall contain an overview of the security and privacy protection considerations associated with the software. A warning shall be included regarding making unauthorized copies of software or documents, if applicable.

3.7) **Assistance and problem reporting** .This subclause shall identify points of contact and procedures to be followed to obtain assistance and report problems encountered in using the software.

4) **Access to the software** .This clause shall contain step-by-step procedures oriented to the first time/occasional user. Enough detail shall be presented so that the user can reliably access the software before learning the details of its functional capabilities. Safety precautions, marked by WARNING or CAUTION, shall be included where applicable.

4.1) **First-time user of the software** .This subclause should be divided into the following.

4.1.1)**Equipment familiarization** .This subclause shall describe the following as appropriate:

a) Procedures for turning on power and making adjustments
b) Dimensions and capabilities of the visual display screen
c) Appearance of the cursor, how to identify an active cursor if more than one cursor can appear, how to position a cursor, and how to use a cursor
d) Keyboard layout and role of different types of keys and pointing devices
e) Procedures for turning power off if special sequencing of operations is needed

4.1.2)**Access control** .This subclause shall present an overview of the access and security features of the software that are visible to the user. The following items shall be included, as applicable:

a) How and from whom to obtain a password
b) How to add, delete, or change passwords under user control
c) Security and privacy protection considerations pertaining to the storage and marking of output reports and other media that the user will generate

4.1.3)**Installation and setup** .This subclause shall describe any procedures that the user is required to perform to be identified or authorized to access or install software on the equipment, to perform the installation, to configure the software, to delete or overwrite former files or data, and to enter parameters for software operation.

4.2) **Initiating a session** .This subclause shall provide step-by-step procedures for beginning work, including any options available. A checklist for problem determination shall be included in case difficulties are encountered.

4.3) **Stopping and suspending work** .This subclause shall describe how the user can cease or interrupt use of the software and how to determine whether normal termination or cessation has occurred.

5) **Processing reference guide** .This clause shall provide the user with procedures for using the software. If procedures are complicated or extensive, additional clauses 6, 7, ... may be added in the same subclause structure as this clause and with titles meaningful to the clauses selected. The organization of the document will depend on the characteristics of the software being documented. For example, one approach is to base the clauses on the organizations in which users work, their assigned positions, their work sites, or the tasks they are required to perform. For other software, it may be more appropriate to have clause 5 be a guide to menus, clause 6 be a guide to the command

language used, and clause 7 be a guide to functions. Detailed procedures are intended to be presented in subclauses of subclause 5.3. Depending on the design of the software, the subclauses might be organized on a function-by-function, menu-by-menu, transaction-by-transaction, or other basis. Safety precautions, marked by WARNING or CAUTION, shall be included where applicable.

5.1) **Capabilities** .This subclause shall briefly describe the interrelationships of the transactions, menus, functions, or other processes in order to provide an overview of the use of the software.

5.2) **Conventions** .This subclause shall describe any conventions used by the software, such as the use of colors in displays, the use of audible alarms, the use of abbreviated vocabulary, and the use of rules for assigning names or codes.

5.3) **Processing procedures** .This subclause shall explain the organization of subsequent subclauses, e.g., by function, by menu, by screen. Any necessary order in which procedures are required to be accomplished shall be described.

5.3.x)**(Aspect of software use)** .The title of this subclause shall identify the function, menu, transaction, or other process being described. This subclause shall describe and give options and examples, as applicable, of menus, graphical icons, data entry forms, user inputs, inputs from other software or hardware that may affect the software's interface with the user, outputs, diagnostic or error messages or alarms, and help facilities that can provide on-line descriptive or tutorial information. The format for presenting this information can be adapted to the particular characteristics of the software, but a consistent style of presentation shall be used, i.e., the descriptions of menus shall be consistent, the descriptions of transactions shall be consistent among themselves.

5.4) **Related processing** .This subclause shall identify and describe any related batch, offline, or background processing performed by the software that is not invoked directly by the user and is not described in subclause 5.3. Any user responsibilities to support this processing shall be specified.

5.5) **Data backup** .This subclause shall describe procedures for creating and retaining backup data that can be used to replace primary copies of data in event of errors, defects, malfunctions, or accidents.

5.6) **Recovery from errors, malfunctions, and emergencies** .This subclause shall present detailed procedures for restart or recovery from errors or malfunctions occurring during processing and for ensuring continuity of operations in the event of emergencies.

5.7) **Messages** .This subclause shall list, or refer to an annex that lists, all error messages, diagnostic messages, and information messages that can occur while accomplishing any of the user's functions. The meaning of each message and the action that should be taken after each such message shall be identified and described.

5.8) **Quick-reference guide** .If appropriate to the software, this subclause shall provide or reference a quick-reference card or page for using the software. This quick-reference guide shall summarize, as applicable, frequently-used function keys, control sequences, formats, commands, or other aspects of software use.

6) **Notes** .This clause shall contain any general information that aids in understanding this document (e.g., background information, glossary, rationale). This clause shall include an alphabetical listing of all acronyms, abbreviations, and their meanings as used in this document and a list of terms and definitions needed to understand this document. If clause 5 has been expanded into clause(s) 6, ..., this clause shall be numbered as the next clause following clause n.

A) **Annexes** . Annexes may be used to provide information published separately for convenience in document maintenance (e.g., charts, classified data). As applicable, each annex shall be referenced in the main body of the document where the data would normally have been provided. Annexes may be bound as separate documents for ease in handling. Annexes shall be lettered alphabetically (A, B, etc.).

J.2.2 Contents of the Software Input/Output Manual (SIOM)

SOFTWARE INPUT/OUTPUT MANUAL (SIOM)

Contents

1) Scope
1.1) Identification
1.2) System overview
1.3) Document overview
2) Referenced documents
3) Software summary
3.1) Software application
3.2) Software inventory
3.3) Software environment
3.4) Software organization and overview of operation
3.5) Contingencies and alternate states and modes of operation
3.6) Security and privacy protection
3.7) Assistance and problem reporting
4) Using the software
4.1) Initiation procedures
4.2) Description of input
4.2.1)Input conditions
4.2.2)Input formats
4.2.3)Composition rules
4.2.4)Input vocabulary
4.2.5)Sample input
4.3) Description of output
4.3.1)General description
4.3.2)Output formats
4.3.3)Sample output
4.3.4)Output vocabulary
4.4) Use of output
4.5) Recovery and error correction procedures
4.6) Communications diagnostics
5) Query procedures
5.1) Database/data file format
5.2) Query capabilities
5.3) Query preparation
5.4) Control instructions
6) User terminal processing procedures
6.1) Available capabilities
6.2) Access procedures
6.3) Display, updates, and retrieval procedures
6.4) Recovery and error correction procedures
6.5) Termination procedures
7) Notes
A) Annexes

1) **Scope** .This clause should be divided into the following subclauses.

1.1) **Identification** .This subclause shall contain a full identification of the system and the software to which this document applies, including, as applicable, identification number(s), title(s), abbreviation(s), version number(s), and release number(s).

1.2) **System overview** .This subclause shall briefly state the purpose of the system and the software to which this document applies. It shall describe the general nature of the system and software; summarize the history of system development, operation, and maintenance; identify the project sponsor, acquirer, user, developer, and maintenance organizations; identify current and planned operating sites; and list other relevant documents.

1.3) **Document overview** .This subclause shall summarize the purpose and contents of this manual and shall describe any security or privacy protection considerations associated with its use.

2) **Referenced documents** .This clause shall list the number, title, revision, date, and source of all documents referenced in this manual.

3) **Software summary** .This clause should be divided into the following subclauses.

3.1) **Software application** .This subclause shall provide a brief description of the intended uses of the software. Capabilities, operating improvements, and benefits expected from its use shall be described.

3.2) **Software inventory** .This subclause shall identify the software files, if any, including databases and data files, that the user is responsible for requesting in order to access the software described in this manual. The identification shall include security and privacy protection considerations for each file and identification of the software necessary to continue or resume operation in case of an emergency.

3.3) **Software environment** .This subclause shall identify the hardware, software, manual operations, and other resources needed to access and use the software. This subclause shall be based on the assumption that the software is installed in a computer center or other centralized or networked environment and shall focus on the resources that a user is required to have to access and use the software in that environment. Included, as applicable, shall be identification of:

a) Computer equipment that is required to be present, such as terminals, printers, or other input/output devices
b) Communications equipment that is required to be present
c) Other software that is required to be present, such as networking software
d) Forms, procedures, or other manual operations that are required to be present
e) Other facilities, equipment, or resources that are required to be present

3.4) **Software organization and overview of operation** .This subclause shall provide a brief description of the organization and operation of the software from the user's point of view. The description shall include, as applicable:

a) Logical components of the software, from the user's point of view, including databases and data files the user can access, Database Management Systems (DBMSs), and communications paths, and an overview of the purpose/operation of each component
b) Performance characteristics that can be expected by the user, such as:
1) Type, volume, rate of input accepted
2) Type, volume, accuracy, rate of output the software can produce
3) Typical response time and factors that affect it
4) Typical processing time and factors that affect it
5) Limitations, e.g, restrictions on what data may be queried and from what location
6) Error rate that can be expected
7) Reliability that can be expected
c) Relationships of the functions performed by the software with interfacing systems and with the organizations or stations that are sources of input or recipients of output
d) Supervisory controls that can be implemented (such as passwords) to manage the software

3.5) **Contingencies and alternate states and modes of operation** .This subclause shall explain the differences in what the user will be able to do with the software at times of emergency and in various states and modes of operation, if applicable.

3.6) **Security and privacy protection** .This subclause shall contain an overview of the security and privacy protection considerations associated with the software. A warning shall be included regarding making unauthorized copies of software or documents, if applicable.

3.7) **Assistance and problem reporting** .This subclause shall identify points of contact and procedures to be followed to obtain assistance and report problems encountered in using the software.

4) **Using the software** .This clause should be divided into the following subclauses to describe how to prepare input to, and interpret output from, the software. If the software has a query capability, this subclause shall reference clause 5 for a description of this capability. If the software can be accessed

via terminal, this subclause shall reference clauses 6 through n to describe terminal processing procedures. Safety precautions, marked by WARNING or CAUTION, shall be included where applicable.

4.1) **Initiation procedures** .This subclause shall contain the procedures that are required to be followed to initiate use of the software. Included may be information such as sample job request forms or sample control statements.

4.2) **Description of input** .This subclause should be divided into the following.

4.2.1)**Input conditions** .This subclause shall describe the conditions to be observed in preparing each type or class of input to the software. The conditions shall include the following, as applicable:

a) Reason for input, such as normal status report, need to update data
b) Frequency of input, such as monthly, on demand
c) Origin of input, such as the organization or station authorized to generate the input
d) Medium of input, such as magnetic tape
e) Related input that is required to be entered at the same time as this input
f) Other applicable information, such as priority; security and privacy protection considerations

4.2.2)**Input formats** .This subclause shall illustrate the layout formats to be used in the preparation of input to the software and shall explain the information that may be entered in the various clauses and lines of each format.

4.2.3)**Composition rules** .This subclause shall describe any rules and conventions that are required to be observed to prepare input. The rules of syntax, usage of punctuation, etc., shall be explained. The rules shall include the following, as applicable:

a) Input transaction length, such as 100 characters maximum
b) Format conventions, such as all input items are required to be left-justified
c) Labeling, such as usage of identifiers to denote major data sets to the software
d) Sequencing, such as order and placement of items in the input
e) Punctuation, such as spacing and use of symbols (virgule, asterisk, character combinations, etc.) to denote start and end of input, of data groups, and of fields
f) Restrictions, such as rules forbidding use of particular characters or parameter sets

4.2.4)**Input vocabulary** .This subclause shall explain the legal character combinations or codes that are required to be used to prepare input. An annex may be provided containing an ordered listing of these codes.

4.2.5)**Sample input** .This subclause shall provide examples that illustrate and explain each type or class of input acceptable by the software. Included shall be information on the following types of input, as applicable:

a) Headers denoting the start of input
b) Text or body of the input
c) Trailers denoting the end of input
d) Portions of the input that may be omitted
e) Portions of the input that may be repeated

4.3) **Description of output** .This subclause should be divided into the following.

4.3.1)**General description** .This subclause shall provide the following information, as applicable, for each type or class of output:

a) Reasons why the output is generated
b) Frequency of the output, such as monthly, on demand
c) Any modifications or variations of the basic output that are available
d) Media, such as printout, display screen, tape
e) Location where the output will appear, such as in the computer area or remotely
f) Any additional characteristics, such as priority, security and privacy protection considerations, associated output that complements the information in this output

4.3.2)**Output formats** .This subclause shall illustrate and explain the layout of each type or class of output from the software. The following aspects shall be explained, as applicable:

a) Security and privacy protection markings
b) Data that may appear in headers
c) Information that may appear in the body or text of the output, including column headings and subsets or clauses in the output format
d) Data that may appear in trailers
e) Additional characteristics, such as the meaning of special symbols

4.3.3) **Sample output** .This subclause shall provide illustrations of each type or class of output from the software. A description of each sample shall be provided, including, as applicable:

a) Meaning and use of each column, entry, etc.
b) Source, such as extracted from database, calculated
c) Characteristics, such as when omitted, range of values, unit of measure

4.3.4) **Output vocabulary** .This subclause shall describe any codes or abbreviations that appear in the output that differ from those used in the input described in subclause 4.2.4.

4.4) **Use of output** .This subclause shall explain the use of the output by the operational area or activity that receives it.

4.5) **Recovery and error correction procedures** .This subclause shall list the error codes generated by the software, give their meanings, and describe the corrective actions to be taken by the user. Also included shall be the procedures to be followed by the user with respect to restart, recovery, and continuity of operations in the event of emergencies.

4.6) **Communications diagnostics** .This subclause shall describe the diagnostic procedures available to the user for validating communications and for identifying and classifying problems.

5) **Query procedures** .This clause shall be prepared for software with a query capability. It should be divided into the following subclauses.

5.1) **Database/data file format** .This subclause shall provide a user's view of the format and content of each database and data file that can be queried. Information such as the following shall be provided for each data element, as applicable:

a) Data element name
b) Synonymous names
c) Definition
d) Format
e) Range and enumeration of values
f) Unit of measurement
g) Data item names, abbreviations, and codes

5.2) **Query capabilities** .This subclause shall identify and describe the preprogrammed and ad hoc query capabilities provided by the software.

5.3) **Query preparation** .This subclause shall provide instructions for preparing queries.

5.4) **Control instructions** .This subclause shall provide instructions for the sequencing of runs and other actions necessary to extract responses to query requests. These instructions shall include control statements that may be required by the computer system or software.

6) **User terminal processing procedures** .This clause should be divided into the following subclauses to provide the user with information on the use of terminals to accomplish processing. If the procedures are complicated or extensive, clauses 7 through n may be added in the same subclause structure as this clause and with titles meaningful to the clauses selected. The organization of the document will depend on the characteristics of the software being documented. For example, clauses might be based on the organizations in which users work, their assigned positions, work sites, or the tasks they are required to perform. For other software, it may be more appropriate to have clause 6 be a guide to menus, clause 7 be a guide to the command language, and clause 8 be a guide to functions. Detailed procedures are intended to be presented in subclauses 6.2 through 6.5. Depending on the design of the software, the subclauses might be organized on a function-by-function, menu-by-menu, transaction-by-transaction, or other basis. Safety precautions, marked by WARNING or CAUTION, shall be included where applicable.

6.1) **Available capabilities** .This subclause shall describe in general terms the capabilities for retrieval, display, and update of data through terminal operations.

6.2) **Access procedures** .This subclause shall present the sequence of steps and any applicable rules pertaining to accessing the software to initiate software operations.

6.3) **Display, updates, and retrieval procedures** .This subclause should be divided into subclauses to provide the step-by-step procedures necessary to produce the displays, updates, and retrievals that are available through the use of a terminal. Each procedure shall include the name of the operation, input formats, and sample responses, as applicable.

6.4) **Recovery and error correction procedures** .This subclause shall identify error messages that may be displayed and shall indicate their meanings and any corrective actions that should be taken. Also included shall be any procedures to be followed by the user with respect to restart, recovery, and continuity of operations in the event of emergencies.

6.5) **Termination procedures** .This subclause shall present the sequence of steps necessary to terminate the processing.

7) **Notes** .This clause shall contain any general information that aids in understanding this document (e.g., background information, glossary, rationale). This clause shall include an alphabetical listing of all acronyms, abbreviations, and their meanings as used in this document and a list of terms and definitions needed to understand this document. If clause 6 has been expanded into clause(s) 7, ..., this clause shall be numbered as the next clause following clause n.

A) **Annexes** . Annexes may be used to provide information published separately for convenience in document maintenance (e.g., charts, classified data). As applicable, each annex shall be referenced in the main body of the document where the data would normally have been provided. Annexes may be bound as separate documents for ease in handling. Annexes shall be lettered alphabetically (A, B, etc.).

J.2.3 Contents of the Software Center Operator Manual (SCOM)

SOFTWARE CENTER OPERATOR MANUAL (SCOM)

Contents

1) Scope
   1.1) Identification
   1.2) System overview
   1.3) Document overview
2) Referenced documents
3) Software summary
   3.1) Software application
   3.2) Software inventory
   3.3) Software environment
   3.4) Software organization and overview of operation
   3.5) Contingencies and alternate states and modes of operation
   3.6) Security and privacy protection
   3.7) Assistance and problem reporting
4) Installation and setup
5) Description of runs
   5.1) Run inventory
   5.2) Phasing
   5.3) Diagnostic procedures
   5.4) Error messages
   5.5) Description of each run
      5.5.x)Run description for (run name or identifier)
      5.5.x.1)Control input
      5.5.x.2)Run management information
      5.5.x.3)Input-Output files

5.5.x.4)Output reports
5.5.x.5)Reproduced output reports
5.5.x.6)Procedures for restart/recovery and continuity of operations

6) Notes

A) Annexes

1) **Scope** .This clause should be divided into the following subclauses.
   1.1) **Identification** .This subclause shall contain a full identification of the system and software to which this document applies, including, as applicable, identification number(s), title(s), abbreviation(s), version number(s), and release number(s).
   1.2) **System overview** .This subclause shall briefly state the purpose of the system and the software to which this document applies. It shall describe the general nature of the system and software; summarize the history of system development, operation, and maintenance; identify the project sponsor, acquirer, user, developer, and maintenance organizations; identify current and planned operating sites; and list other relevant documents.
   1.3) **Document overview** .This subclause shall summarize the purpose and contents of this manual and shall describe any security or privacy protection considerations associated with its use.
2) **Referenced documents** .This clause shall list the number, title, revision, date, and source of all documents referenced in this manual.
3) **Software summary** .This clause should be divided into the following subclauses.
   3.1) **Software application** .This subclause shall provide a brief description of the intended uses of the software. Capabilities, operating improvements, and benefits expected from its use shall be described.
   3.2) **Software inventory** .This subclause shall identify all software files, including databases and data files, that are required to be installed for the software to operate. The identification shall include security and privacy protection considerations for each file and identification of the software necessary to continue or resume operation in case of an emergency.
   3.3) **Software environment** .This subclause shall identify the hardware, software, manual operations, and other resources needed to install and operate the software. Included, as applicable, shall be identification of:
      a) Computer equipment that is required to be present, including amount of memory needed, amount of auxiliary storage needed, and peripheral equipment such as terminals, printers, and other input/output devices
      b) Communications equipment that is required to be present
      c) Other software that is required to be present, such as networking software, operating systems, databases, data files, utilities, permanent files that are referenced, created, or updated by the software; and databases/data files necessary to resume operation in the event of emergencies
      d) Forms, procedures, or other manual operations that are required to be present
      e) Other facilities, equipment, or resources that are required to be present
   3.4) **Software organization and overview of operation** .This subclause shall provide a brief description of the organization and operation of the software from the operator's point of view. The description shall include, as applicable:
      a) Logical components of the software, from the operator's point of view, and an overview of the purpose/operation of each component
      b) Types of input/access that can be made to the software and the software's response to each type
      c) The reports and other output that are produced by the software, including security and privacy protection considerations for each
      d) Typical run times and factors that affect them
      e) Organization of software operation into runs. This description shall use a chart, if applicable, showing how the different operations are interrelated. If sets of runs are grouped by time periods or cycles, each set of integrated operations required on a daily, weekly, etc., basis shall be presented. If runs may be grouped logically by organizational level, the

groups of runs that can be performed by each organizational level such as headquarters or central office processing, field office processing, etc., shall be presented.

f) Any system restrictions, waivers of operational standards, information oriented toward specific support areas (for example, library, small computer and teleprocessing support, interfaces with other systems), or other special aspects of processing

g) General description of the communications functions and processes of the software, including, as applicable, a diagram of the communications network used in the system

3.5) **Contingencies and alternate states and modes of operation** .This subclause shall explain the differences in software operation at times of emergency and in various states and modes of operation, if applicable.

3.6) **Security and privacy protection** .This subclause shall contain an overview of the security and privacy protection considerations associated with the software. A warning shall be included regarding making unauthorized copies of software or documents, if applicable.

3.7) **Assistance and problem reporting** .This subclause shall identify points of contact and procedures to be followed to obtain assistance and report problems encountered in operating the software.

4) **Installation and setup** .This subclause shall describe any procedures that the operator is required to perform to install the software on the equipment, to configure the software, to delete or overwrite former files or data, and to enter parameters for software operation. Safety precautions, marked by WARNING or CAUTION, shall be included where applicable.

5) **Description of runs** .This clause should be divided into the following subclauses to provide a description of the runs to be performed. Safety precautions, marked by WARNING or CAUTION, shall be included where applicable.

5.1) **Run inventory** .This subclause shall provide a list of the runs to be performed, identifying the software and the jobs that make up each run. It shall include a brief summary of the purpose of each run and shall relate the list to the run descriptions included in the remainder of this clause.

5.2) **Phasing** .This subclause shall describe acceptable phasing of the software into a logical series of operations. A run may be phased to permit manual or semiautomatic checking of intermediate results, to provide the user with intermediate results for other purposes, or to permit a logical break if higher priority jobs are submitted. An example of the minimum division for most systems would be edit, file update, and report preparation.

5.3) **Diagnostic procedures** .This subclause shall provide the setup and execution procedures for any software diagnostics. Included shall be procedures for validation and trouble shooting. All parameters (both input and output), codes, and range values for diagnostic software shall be explained.

5.4) **Error messages** .This subclause shall list all error messages output by the software, along with the meaning and corresponding correction procedure for each message.

5.5) **Description of each run** .This subclause should be divided into the following.

5.5.x)**Run description for (run name or identifier)** .This subclause shall identify a run and should be divided into the following to describe the run.

5.5.x.1)**Control input** .This subclause shall provide a listing of the run stream of job control statements needed to initiate the run.

5.5.x.2)**Run management information** .This subclause shall provide the information needed to manage the run including, as applicable:

a) Peripheral and resource requirements
b) Security and privacy protection considerations
c) Method of initiation, such as on request, after another run, or at a predetermined time
d) Estimated run time
e) Required turnaround time
f) Messages and responses
g) Procedures for taking check points
h) Waivers from operational standards

5.5.x.3)**Input-output files** .This subclause shall provide information about the files and databases that serve as input to or that are created or updated by the run. Included for each

shall be information such as name, security and privacy protection, recording medium, retention schedule, and disposition.

5.5.x.4)**Output reports** .This subclause shall provide information about the reports that are produced during the run. Included for each report shall be the following information, as applicable: report identifier, product control number, report control symbol, title, security and privacy protection, media (e.g., hard copy, magnetic tape), volume of report, number of copies, and distribution of copies.

5.5.x.5)**Reproduced output reports** .This subclause shall provide information about computer-generated reports that are subsequently reproduced by other means. Included for each report shall be information such as report identification, security and privacy protection, reproduction technique, paper size, binding method, number of copies, and distribution of copies.

5.5.x.6)**Procedures for restart/recovery and continuity of operations** .This subclause shall provide procedures to be followed by operator personnel concerning restart/recovery in the event of a system failure and for continuity of operations in the event of emergencies.

6) **Note** .This clause shall contain any general information that aids in understanding this document (e.g., background information, glossary, rationale). This clause shall include an alphabetical listing of all acronyms, abbreviations, and their meanings as used in this document and a list of terms and definitions needed to understand this document.

A) **Annexes** . Annexes may be used to provide information published separately for convenience in document maintenance (e.g., charts, classified data). As applicable, each annex shall be referenced in the main body of the document where the data would normally have been provided. Annexes may be bound as separate documents for ease in handling. Annexes shall be lettered alphabetically (A, B, etc.).

J.2.4 Contents of the Computer Operation Manual (COM)

COMPUTER OPERATION MANUAL (COM)

Contents

1) Scope
   1.1) Identification
   1.2) Computer system overview
   1.3) Document overview
2) Referenced documents
3) Computer system operation
   3.1) Computer system preparation and shutdown
      3.1.1)Power on and off
      3.1.2)Initiation
      3.1.3)Shutdown
   3.2) Operating procedures
      3.2.1)Input and output procedures
      3.2.2)Monitoring procedures
      3.2.3)Off-line procedures
      3.2.4)Other procedures
   3.3) Problem-handling procedures
4) Diagnostic features
   4.1) Diagnostic features summary
   4.2) Diagnostic procedures
   4.3) Diagnostic tools
5) Notes

A) Annexes

1) **Scope** .This clause should be divided into the following subclauses.
   1.1) **Identification** .This subclause shall contain the manufacturer's name, model number, and any other identifying information for the computer system to which this COM applies.
   1.2) **Computer system overview** .This subclause shall briefly state the purpose of the computer system to which this COM applies.
   1.3) **Document overview** .This subclause shall summarize the purpose and contents of this manual and shall describe any security or privacy protection considerations associated with its use.
2) **Referenced documents** .This clause shall list the number, title, revision, date, and source of all documents referenced in this manual.
3) **Computer system operation** .This clause should be divided into the following subclauses. Safety precautions, marked by WARNING or CAUTION, shall be included where applicable.
   3.1) **Computer system preparation and shutdown** .This subclause should be divided into the following.
      3.1.1)**Power on and off** .This subclause shall contain the procedures necessary to power-on and power-off the computer system.
      3.1.2)**Initiation** .This subclause shall contain the procedures necessary to initiate operation of the computer system, including, as applicable, equipment setup, pre-operation, bootstrapping, and commands typically used during computer system initiation.
      3.1.3)**Shutdown** .This subclause shall contain the procedures necessary to terminate computer system operation.
   3.2) **Operating procedures** .This subclause should be divided into the following. If more than one mode of operation is available, instructions for each mode shall be provided.
      3.2.1)**Input and output procedures** .This subclause shall describe the input and output media (e.g., magnetic disk, tape) relevant to the computer system, state the procedures to read and write on these media, briefly describe the operating system control language, and list procedures for interactive messages and replies (e.g, terminals to use, passwords, keys).
      3.2.2)**Monitoring procedures** .This subclause shall contain the procedures to be followed for monitoring the computer system in operation. It shall describe available indicators, interpretation of those indicators, and routine and special monitoring procedures to be followed.
      3.2.3)**Off-line procedures** .This subclause shall contain the procedures necessary to operate all relevant off-line equipment of the computer system.
      3.2.4)**Other procedures** .This subclause shall contain any additional procedures to be followed by the operator (e.g., computer system alarms, computer system security or privacy protection considerations, switch over to a redundant computer system, or other measures to ensure continuity of operations in the event of emergencies).
   3.3) **Problem-handling procedures** .This subclause shall identify problems that may occur in any step of operation described in the preceding subclauses in clause 3. It shall state the error messages or other indications accompanying those problems and shall describe the automatic and manual procedures to be followed for each occurrence, including, as applicable, evaluation techniques, conditions requiring computer system shutdown, procedures for on-line intervention or abort, steps to be taken to restart computer system operation after an abort or interruption of operation, and procedures for recording information concerning a malfunction.
4) **Diagnostic features** .This clause should be divided into the following subclauses to describe diagnostics that may be performed to identify and troubleshoot malfunctions in the computer system.
   4.1) **Diagnostic features summary** .This subclause shall summarize the diagnostic features of the computer system, including error message syntax and hierarchy for fault isolation. This subclause shall describe the purpose of each diagnostic feature.
   4.2) **Diagnostic procedures** .This subclause should be divided as needed to describe the diagnostic procedures to be followed for the computer system, including:
      a) Identification of hardware, software, or firmware necessary for executing each procedure
      b) Step-by-step instructions for executing each procedure
      c) Diagnostic messages and the corresponding required action

4.3) **Diagnostic tools** .This subclause should be divided as needed to describe the diagnostic tools available for the computer system. These tools may be hardware, software, or firmware. This subclause shall identify each tool by name and number and shall describe the tool and its application.

5) **Notes** .This clause shall contain any general information that aids in understanding this document (e.g., background information, glossary, rationale). This clause shall include an alphabetical listing of all acronyms, abbreviations, and their meanings as used in this document and a list of terms and definitions needed to understand this document.

A) **Annexes** . Annexes may be used to provide information published separately for convenience in document maintenance (e.g., charts, classified data). As applicable, each annex shall be referenced in the main body of the document where the data would normally have been provided. Annexes may be bound as separate documents for ease in handling. Annexes shall be lettered alphabetically (A, B, etc.).

Annex K

(informative)

Software product description format and structure

K.1 Scope

This annex provides guidance on the format and structure of deliverable software products. It is informative only, provided to aid in using this standard. Content requirements for software products associated with this standard are found in annexes E through J.

K.2 Software products covered

Figure 10 identifies the software products covered by this standard and provides guidance on the use of each product.

K.3 Format and structure for all software products

The following guidelines apply to all of the software products in annexes E through J.

K.3.1 Structure

Annexes E through J describe software products in terms of clauses and subclauses for use in developing traditional documents. When other forms of presenting information are allowed and where the intent is that a traditional document need not be produced, such as information in CASE tools or "in contractor format", this structure does not apply. In all cases, the content requirements do apply, as applicable to the project. When two or more software products are to be combined into a single deliverable, the acquirer should decide which one document should be the "parent" and which should be an annex(es) allowing the annexed document(s) to be attached without renumbering paragraphs or pages.

K.3.2 Format

The term "document" is to be interpreted to mean a collection of information regardless of the medium in which it is stored. The format for delivery of software products is project dependent, as described in annex H. Examples of format choices are: 1) whether the information is to be delivered on paper or electronic media; 2) whether electronic deliverables are required to be compatible with a specified standard, word processor, or other maintenance software; and 3) whether the information may reside in a CASE or other automated tool rather than in the form of a traditional document.

Software Product	Annex	Overview
Computer Operation Manual (COM)	J.2.4	Provides information needed to operate a given computer and its peripheral equipment. Focuses on the computer itself, not on particular software that will run on the computer. Intended for newly developed computers, special-purpose computers, or other computers for which commercial or other operation manuals are not readily available.
Computer Programming Manual (CPM)	I.2.3	Provides information needed by a programmer to understand how to program a given computer. Focuses on the computer itself, not on particular software that will run on the computer. Intended for newly developed computers, special-purpose computers, or other computers for which commercial or other programming manuals are not readily available.
Database Design Description (DBDD)	G.2.3	Describes the design of a database, that is, a collection of related data stored in one or more computerized files in a manner that can be accessed by users or computer programs via a database management system (DBMS). Can also describe the software units used to access or manipulate the data. Used as the basis for implementing the database and related software units. Provides the acquirer visibility into the design and provides information needed for software maintenance.
Firmware Support Manual (FSM)	I.2.4	Provides the information needed to program and reprogram the firmware devices of a system. Applies to read only memories (ROMs), Programmable ROMs (PROMs), Erasable PROMs (EPROMs), and other firmware devices. Describes the firmware devices and the equipment, software, and procedures needed to erase firmware devices, load software into the firmware devices, verify the load process, and mark the loaded firmware devices.
Interface Design Description (IDD)	G.2.2	Describes the interface characteristics of one or more systems, subsystems, hardware items, software items, manual operations, or other system components. May describe any number of interfaces. Can be used to supplement the System/Subsystem Design Description (SSDD), Software Design Description (SDD), and Database Design Description (DBDD). With its companion Interface Requirements Specification (IRS), serves to communicate and control interface design decisions.
Interface Requirements Specification (IRS)	F.2.3	Specifies the requirements imposed on one or more systems, subsystems, hardware items, software items, manual operations, or other system components to achieve one or more interfaces among these entities. Can cover any number of interfaces. Can be used to supplement the System/Subsystem Specification (SSS) and Software Requirements Specification (SRS) as the basis for design and qualification testing of systems and software items.
Operational Concept Description (OCD)	F.2.1	Describes a proposed system in terms of the user needs it will fulfill, its relationship to existing systems or procedures, and the ways it will be used. Used to obtain consensus among the acquirer, developer, maintenance, and user organizations on the operational concept of a proposed system. Depending on its use, an OCD may focus on communicating the user's needs to the developer or the developer's ideas to the user and other interested parties.

Figure10 — Overview of software products

Software Product	Annex	Overview
Software Center Operator Manual (SCOM)	J.2.3	Provides personnel in a computer center or other centralized or networked software installation information on how to install and operate a software system. Developed for software systems that will be installed in a computer center or other centralized or networked software installation, with users accessing the system via terminals or personal computers or submitting and receiving input and output in batch or interactive mode. Often used with the Software Input/Output Manual (SIOM). This pair of manuals is an alternative to the Software User Manual (SUM).
Software Design Description (SDD)	G.2.4	Describes the design of a software item. Describes the software item-wide design decisions, the software item architectural design, and the detailed design needed to implement the software. The SDD may be supplemented by Interface Design Descriptions (IDDs) and Database Design Descriptions (DBDDs). With its associated IDDs and DBDDs, is used as the basis for implementing the software. Provides the acquirer visibility into the design and provides information needed for software maintenance.
Software Development Plan (SDP)	E.2.1	Describes a developer's plans for conducting a software development effort. Covers new development, modification, reuse, reengineering, maintenance, and all other activities resulting in software products. Provides the acquirer insight into, and a tool for monitoring, the processes to be followed for software development, the methods to be used, the approach to be followed for each activity, and project schedules, organization, and resources. Portions of the plan may be bound separately if this approach enhances their usability. Examples include plans for software configuration management and software quality assurance.
Software Input/Output Manual (SIOM)	J.2.2	Tells a user how to access, submit input to, and interpret output from, a batch or interactive software system that is run by personnel in a computer center or other centralized or networked software installation. Developed for software systems that will be installed in a computer center or other centralized or networked software installation, with users accessing the system via terminals or personal computers or submitting and receiving input and output in batch mode. Often used with the Software Center Operator Manual (SCOM). This pair of manuals is an alternative to the Software User Manual (SUM).
Software Installation Plan (SIP)	E.2.3	A plan for installing software at user sites, including preparations, user training, and conversion from existing systems. Prepared when the developer will be involved in the installation of software at user sites and when the installation process will be sufficiently complex to require a documented plan. For software embedded in a hardware-software system, an installation plan for the hardware-software system may make a separate SIP unnecessary.
Software Product Specification (SPS)	I.2.1	Contains or references the executable software, source files, and software maintenance information, including "as built" design information and compilation, build, and modification procedures, for a software item. Can be used to order the executable software and/or source files for a software item and is the primary software maintenance document for the software item.
Software Requirements Specification (SRS)	F.2.4	Specifies the requirements for a software item and the methods to be used to ensure that each requirement has been met. Requirements pertaining to the software item's external interfaces may be presented in the SRS or in one or more Interface Requirements Specifications (IRSs) referenced from the SRS. The SRS, possibly supplemented by IRSs, is used as the basis for design and qualification testing of a software item.

Figure10 — Overview of software products (continued)

Software Product	Annex	Overview
System/Subsystem Design Description (SSDD)	G.2.1	Describes the system- or subsystem-wide design and the architectural design of a system or subsystem. May be supplemented by Interface Design Descriptions (IDDs) and Database Design Descriptions (DBDDs). With its associated IDDs and DBDDs, is used as the basis for further system development. May be prepared as a System Design Description or Subsystem Design Description (each using the acronym SSDD).
System/Subsystem Specification (SSS)	F.2.2	Specifies the requirements for a system or subsystem and the methods to be used to ensure that each requirement has been met. Requirements pertaining to the system or subsystem external interfaces may be presented in the SSS or in one or more Interface Requirements Specifications (IRSs) referenced from the SSS. The SSS, possibly supplemented by IRSs, is used as the basis for design and qualification testing of a system or subsystem. May be prepared as a System Specification or Subsystem Specification (each using the acronym SSS).
Software Test Description (STD)	H.2.1	Describes the test preparations, test cases, and test procedures to be used to perform qualification testing of a software item or a software system or subsystem. Enables the acquirer to assess the adequacy of the qualification testing to be performed.
Software Test Plan (STP)	E.2.2	Describes plans for qualification testing of software items and software systems. Describes the software test environment to be used for the testing, identifies the tests to be performed, and provides schedules for test activities. There is usually a single STP for a project. Enables the acquirer to assess the adequacy of planning for software item and, if applicable, software system qualification testing.
Software Test Report (STR)	H.2.2	Provides a record of the qualification testing performed on a software item, a software system or subsystem, or other software-related item. Enables the acquirer to assess the testing and its results.
Software Transition Plan (STrP)	E.2.4	Identifies the hardware, software, and other resources needed for life cycle support of deliverable software and describes the developer's plans for transitioning deliverable items to the maintenance organization. Developed if the software support strategy calls for transition of responsibility from the developer to a separate maintenance organization.
Software User Manual (SUM)	J.2.1	Tells a hands-on software user how to install and use a software item, a group of related software items, or a software system or subsystem. May also cover a particular aspect of software operation, such as instructions for a particular position or task. Developed for software that is run by the user and has a user interface requiring on-line user input or interpretation of displayed output. If the software is embedded in a hardware-software system, user manuals or operating procedures for that system may make separate SUMs unnecessary. An alternative to the Software Center Operator Manual (SCOM) and Software Input/Output Manual (SIOM).
Software Version Description (SVD)	I.2.2	Identifies and describes a software version consisting of one or more software items. Used to release, track, and control software versions. The term "version" may be applied to the initial release of the software, to a subsequent release of that software, or to one of multiple forms of the software released at approximately the same time (for example, to different sites).

Figure10 — Overview of software products (continued)

K.3.3 Title page or identifier

If a software product is in the form of a traditional document, it is to include a title page containing, as applicable: document number; volume number; version/revision indicator; security markings or other restrictions on the handling of the document; date; document title; name, abbreviation, and any other identifier for the system, subsystem, or item to which the document applies; contract number; the software product's identification number in the contract; organization for which the document has been prepared; name and address of the preparing organization; and distribution restrictions. If the software product is in an alternative form, such as a database, this information is to be included on external and internal labels or by equivalent identification methods.

K.3.4 Table of contents and index

If a software product is in the form of a traditional document, it is to contain a table of contents providing the number, title, and page number of each titled subclause, figure, table, and annex. Manuals are to also contain an index providing an alphabetic listing of key terms and concepts covered and the pages or subclauses in which they are covered. If the software product is in an alternative form, such as a database, there is to be an internal or external table of contents containing pointers to, or instructions for accessing, information corresponding to each subclause, figure, table, and annex, and, for manuals, an external or internal index containing pointers to, or instructions for accessing, information relevant to key terms or concepts.

K.3.5 Page numbering/labeling

If a software product is in the form of a traditional document, each page is to contain a unique page number and display the document number, including version, volume, and date, as applicable. If the software product is in an alternative form, such as a database, then files, screens, or other entities are to be assigned names or numbers in such a way that desired data can be indexed and accessed.

K.3.6 Response to tailoring instructions

If a software product is in the form of a traditional document and a subclause has been tailored out of the corresponding software product description in an annex, the resulting document is to contain the corresponding subclause number and title, followed by "This subclause has been tailored out." If the software product is in an alternative form, such as a database, this representation need occur only in the table of contents or equivalent.

K.3.7 Multiple clauses and their subordinates

Any clause or subclause may be written as multiple clauses or subclauses to enhance readability.

K.3.8 Alternative presentation styles

Diagrams, tables, matrices, and other presentation styles are acceptable substitutes for text when required information can be made more readable using these styles.

K.3.9 Substitution of existing documents

Commercial or other existing documents may be substituted for all or part of a software product if they contain the required data.

K.3.10 Standard data descriptions

If a data description required by this annex has been published in a standard data element dictionary specified in the contract, reference to an entry in that dictionary is preferred over including the description itself.

K.3.11 Applicability of required contents

All content requirements in annexes E through J are "as applicable." If the contents of a given subclause do not apply to a particular project, the developer may satisfy that subclause (or a portion thereof) with "Not applicable." If there is a possibility of disagreement with the acquirer regarding which content requirements are applicable, it is advised that the developer use the Software Development Plan and joint technical and management reviews as avenues to propose and reach agreement on the applicability of required content.

Annex L

(normative)

Software product evaluations

L.1 Scope

This annex identifies the software products that are to undergo software product evaluations, identifies the criteria to be used for each evaluation, and contains a default set of definitions for the evaluation criteria. This annex is normative (that is, binding), subject to the following conditions: 1) these requirements may be tailored, 2) the developer may use alternate criteria or definitions if approved by the acquirer, and 3) if the development of a given software product has been tailored out of the standard, the requirement to evaluate that product does not apply.

L.2 Required evaluations

Figure 11 identifies the software products that are to undergo software product evaluations and states the criteria to be applied to each one. Each software product and criterion is labelled for purposes of identification and tailoring. For convenience, they may be treated as subordinate clauses of this subclause (referring to the first criterion, for example, as L.2.1.a). The software products are expressed in lower case letters to emphasize that they are generic products, not necessarily in the form of hard-copy documents. Evaluations of system-level products are to be interpreted as participation in these evaluations. Some of the criteria are subjective. Because of this, there is no requirement to prove that the criteria have been met; the requirement is to perform the evaluations using these criteria and to identify possible problems for discussion and resolution.

NOTE—The evaluation criteria for each software product has been presented in tabular form in figure 11 using the applicable criteria definitions in L.3.1-L.3.14. Note that the lower case letters in the figure are for criterion identification and tailoring purposes only. By substituting the appropriate evaluation criteria for the verb phrases in figure 11 a full set of evaluation criteria may be determined. For example, the criteria to be used for evaluation of a software test plan (item 2) are as follows: a) contains all applicable information in E.2.2 (STP) (see L.3-4); b) meets SOW, if applicable (see L.3.10); c) meets delivery requirements, if applicable (see L.3.9); d) understandable (see L.3.14);e) internally consistent (see L.3.8);f) follows Software Development Plan (see L.3.7); g) covers all software-related qualification activities in the SOW (see L.3.5); h) covers all requirements for the items under test (see L.3.5); i) consistent with other project plans (see L.3.3); and j) presents a sound approach to the testing (see L.3.11).

L.3 Criteria definitions

The following subclauses provide definitions for the criteria in figure 11 that may not be self-explanatory. The criteria are listed in alphabetical order, matching as closely as possible the wording used in figure 11.

L.3.1 Accurately describes (an item)

This criterion, applied to user/operator/programmer instructions and to the “as built” design and version descriptions, means that the instructions or descriptions are correct depictions of the software or other item described.

Software Product	Evaluation Criteria							
	Contains all applic. info in:	Meets SOW, if applic.	Meets deliv reqts, if applic.	Under-stand-able	Intern. consis-tent	Follows SW dev plan	Additional Criteria
1. Software development plan (5.1.1)	a. E.2.1 (SDP)	b.	c.	d.	e.	f. (Up-dates)	g. Covers all activities/deliverables required by the contract h. Consistent with other project plans i. Presents a sound approach to the development
2. Software test plan (5.1.2, 5.1.3)	a. E.2.2 (STP)	b.	c.	d.	e.	f.	g. Covers all software-related qualification activities in the SOW h. Covers all requirements for the items under test i. Consistent with other project plans j. Presents a sound approach to the testing
3. Software installation plan (5.1.4)	a. E.2.3 (SIP)	b.	c.	d.	e.	f.	g. Covers all user site installation activities in the SOW h. Consistent with other project plans i. Presents a sound approach to the installation
4. Software transition plan (5.1.5)	a. E.2.4 (STrP)	b.	c.	d.	e.	f.	g. Covers all transition-related activities in the SOW h. Consistent with other project plans i. Presents a sound approach to the transition
5. Operational concept (5.3.2)	a. F.2.1 (OCD)	b.	c.	d.	e.	f.	g. Feasible
6. System requirements (5.3.3)	a. F.2.2, F.2.3 (SSS, IRS)	b.	c.	d.	e.	f.	g. Covers the operational concept h. Feasible i. Testable
7. System-wide design decisions (5.4.1)	a. G.2.1, G.2.2, G.2.3 (SSDD, IDD, DBDD)	b.	c.	d.	e.	f.	g. Consistent with system requirements h. Feasible
8. System architectural design (5.4.2)	a. G.2.1, G.2.2 (SSDD, IDD)	b.	c.	d.	e.	f.	g. Covers the system requirements h. Consistent with the system-wide design decisions i. Feasible

Figure11 — Software products and associated evaluation criteria

Software Product	Evaluation Criteria						
	Contains all applic. info in:	Meets SOW, if applic.	Meets deliv reqts, if applic.	Under-stand-able	Intern. consis-tent	Follows SW dev plan	Additional Criteria
9. Software item requirements (5.5)	a. F.2.4, F.2.3 (SRS, IRS)	b.	c.	d.	e.	f.	g. Covers system requirements allocated to the software item h. Feasible i. Testable
10. Software item-wide design decisions (5.6.1)	a. G.2.4, G.2.2, G.2.3 (SDD, IDD, DBDD)	b.	c.	d.	e.	f.	g. Consistent with software item requirements h. Feasible
11. Software item architectural design (5.6.2)	a. G.2.4, G.2.2 (SDD, IDD)	b.	c.	d.	e.	f.	g. Covers software item requirements h. Consistent with software item-wide design decisions i. Feasible
12. Software item detailed design (5.6.3)	a. G.2.4, G.2.2, G.2.3 (SDD, IDD, DBDD)	b.	c.	d.	e.	f.	g. Covers software item requirements allocated to each unit h. Consistent with software item-wide design decisions
13. Implemented software (5.7.1)	N/A	b.	c.	d.	e.	f.	g. Covers the software item detailed design
14. Software item qualification test descriptions (5.9.3)	a. H.2.1 (STD)	b.	c.	d.	e.	f.	g. Covers all software item requirements
15. Software item qualification test results (5.9.7)	a. H.2.2 (STR)	b.	c.	d.	e.	f.	g. Covers all planned software item qualification test cases h. Shows evidence that the software item meets its requirements

Figure11 — Software products and associated evaluation criteria (continued)

Software Product	Evaluation Criteria						
	Contains all applic. info in:	Meets SOW, if applic.	Meets deliv reqts, if applic.	Under-stand-able	Intern. consis-tent	Follows SW dev plan	Additional Criteria
16. System qualification test descriptions (5.11.3)	a. H.2.1 (STD)	b.	c.	d.	e.	f.	g. Covers all system requirements
17. System qualification test results (5.11.7)	a. H.2.2 (STR)	b.	c.	d.	e.	f.	g. Covers all planned system qualification test cases h. Shows evidence the system meets its requirements
18. Executable software (5.12.1, 5.13.1)	N/A	b.	c.	d.	e.	f.	g. Meets delivery requirements h. All software necessary for execution is present i. Version exactly matches version that passed testing j. Deliverable media accurately labelled
19. Software version descriptions (5.12.2, 5.13.3)	a. I.2.2 (SVD)	b.	c.	d.	e.	f.	g. Accurately identifies the version of each software component (file, unit, software item, etc.) delivered h. Accurately identifies the changes incorporated
20. Software user manuals (5.12.3.1)	a. J.2.1 (SUM)	b.	c.	d.	e.	f.	g. Accurately describes software installation and use to the intended audience of this manual
21. Software input/ output manuals (5.12.3.2)	a. J.2.2 (SIOM)	b.	c.	d.	e.	f.	g. Accurately describes software input/output to the intended audience of this manual
22. Software center operator manuals (5.12.3.3)	a. J.2.3 (SCOM)	b.	c.	d.	e.	f.	g. Accurately describes software installation and operation to the intended audience of this manual
23. Computer operation manuals (5.12.3.4)	a. J.2.4 (COM)	b.	c.	d.	e.	f.	g. Accurately describes the operational characteristics of the computer
24. Source files (5.13.2)	a. I.2.1 (SPS)	b.	c.	d.	e.	f.	g. Meets delivery requirements h. All required software is present i. Version exactly matches version that passed testing j. Deliverable media accurately labelled

Figure11 — Software products and associated evaluation criteria (continued)

Software Product	Evaluation Criteria							
	Contains all applic. info in:	Meets SOW, if applic.	Meets deliv reqts, if applic.	Under-stand-able	Intern. consis-tent	Follows SW dev plan	Additional Criteria
25. "As built" software item design and related information (5.13.4)	a. I.2.1 (SPS)	b.	c.	d.	e.	f.	g. Accurately describes the "as built" design of the software item h. Accurately describes compilation/build procedures i. Accurately describes modification procedures j. Source files cover all units in the software item design k. Measured resource utilization meets software item requirements
26. "As built" system design (5.13.5)	a. G.2.1 (SSDD)	b.	c.	d.	e.	f.	g. Accurately describes the "as built" system design
27. Computer programming manuals (5.13.6.1)	a. I.2.3 (CPM)	b.	c.	d.	e.	f.	g. Accurately describes the programming features of the computer
28. Firmware support manuals (5.13.6.2)	a. I.2.4 (FSM)	b.	c.	d.	e.	f.	g. Accurately describes firmware programming features
29. Sampling of software development files (5.7.2, 5.7.3, 5.8.1, 5.8.4, 5.9.4, 5.10.1, 5.10.4, 5.11.4)	N/A	b.	N/A	d.	e.	f.	g. Contents are current with the ongoing effort h. Adequate unit test cases/procedures/data/results i. Adequate unit integration test cases/procedures/ data/results j. Adequate software item qualification dry run results k. Adequate software/hardware item integration test cases/ procedures/data/results l. Adequate system qualification dry run results

Figure11 — Software products and associated evaluation criteria (continued)

L.3.2 Adequate test cases, procedures, data, results

Test cases are adequate if they cover all applicable requirements or design decisions and specify the input to be used, the expected results, and the criteria to be used for evaluating those results. Test procedures are adequate if they specify the steps to be followed in carrying out each test case. Test data are adequate if they enable the execution of the planned test cases and test procedures. Test or dry run results are adequate if they describe the results of all test cases and show that all criteria have been met, possibly after revision and retesting.

L.3.3 Consistent with indicated product(s)

This criterion means that: (1) no statement or representation in one software product contradicts a statement or representation in the other software products, (2) a given term, acronym, or abbreviation means the same thing in all of the software products, and (3) a given item or concept is referred to by the same name or description in all of the software products.

L.3.4 Contains all applicable information in (a specified annex)

This criterion uses annexes E through J to specify the required content of software products, regardless of whether a deliverable document has been ordered. Allowances are to be made for the applicability of each topic in the annex. The formatting specified in the annex (required subclause structure and numbering) are not relevant to this evaluation.

L.3.5 Covers (a given set of items)

A software product “covers” a given set of items if every item in the set has been dealt with in the software product. For example, a plan covers the SOW if every provision in the SOW is dealt with in the plan; a design covers a set of requirements if every requirement has been dealt with in the design; a test plan covers a set of requirements if every requirement is the subject of one or more tests. “Covers” corresponds to the downward traceability (for example, from requirements to design) in the requirements, design, and test planning/descriptions in xannexes E through J.

L.3.6 Feasible

This criterion means that, based on the knowledge and experience of the evaluator, a given concept, set of requirements, design, test, etc. violates no known principles or lessons learned that would render it impossible to carry out.

L.3.7 Follows Software Development Plan

This criterion means that the software product shows evidence of having been developed in accordance with the approach described in the Software Development Plan. Examples include following design and coding standards described in the plan. For the Software Development Plan itself, this criterion applies to updates to the initial plan.

L.3.8 Internally consistent

This criterion means that: (1) no two statements or representations in a software product contradict one another, (2) a given term, acronym, or abbreviation means the same thing throughout the software product, and (3) a given item or concept is referred to by the same name or description throughout the software product.

L.3.9 Meets delivery requirements, if applicable

This criterion applies if the software product being evaluated is deliverable and has been formatted for delivery at the time of evaluation. It focuses on the format, markings, and other provisions specified in the contract, rather than on content, covered by other criteria.

L.3.10 Meets SOW, if applicable

This criterion means that the software product fulfills any Statement of Work provisions regarding it. For example, the Statement of Work may place constraints on the operational concept or the design.

L.3.11 Presents a sound approach

This criterion means that, based on the knowledge and experience of the evaluator, a given plan represents a reasonable way to carry out the required activities.

L.3.12 Shows evidence that (an item under test) meets its requirements

This criterion means that recorded test results show that the item under test either passed all tests the first time or was revised and retested until the tests were passed.

L.3.13 Testable

A requirement or set of requirements is considered to be testable if an objective and feasible test can be designed to determine whether each requirement has been met.

L.3.14 Understandable

This criterion means “understandable by the intended audience.” For example, software products intended for programmer-to-programmer communication need not be understandable by non-programmers. A product that correctly identifies its audience (based on information in figure 10 in annex K) and is considered understandable to that audience meets this criterion.

Annex M

(normative)

Category and priority classifications for problem reporting

M.1 Scope

This annex contains requirements for a category and priority classification scheme to be applied to each problem submitted to the corrective action system. This annex is normative (that is, binding), subject to the following conditions: 1) these requirements may be tailored, and 2) the developer may use alternate category and priority schemes if approved by the acquirer.

M.2 Classification by category

The developer shall:

a)) Assign each problem in software products to one or more of the categories in figure 12.
b)) Assign each problem in activities to one or more of the activities in figure 1 (shown at the start of clause 5).

M.3 Classification by priority

The developer shall assign each problem in software products or activities to one of the priorities in figure 13.

Category	Applies to problems in:
a. Plans	One of the plans developed for the project
b. Concept	The operational concept
c. Requirements	The system or software requirements
d. Design	The design of the system or software
e. Code	The software code
f. Database/data file	A database or data file
g. Test information	Test plans, test descriptions, or test reports
h. Manuals	The user, operator, or maintenance manuals
i. Other	Other software products

Figure12 — Categories to be used for classifying problems in software products

Priority	Applies if a problem could:
1	a) Prevent the accomplishment of an essential capability b) Jeopardize safety, security, or other requirement designated "critical"
2	a) Adversely affect the accomplishment of an essential capability and no work-around solution is known b) Adversely affect technical, cost, or schedule risks to the project or to life cycle support of the system, and no work-around solution is known
3	a) Adversely affect the accomplishment of an essential capability but a work-around solution is known b) Adversely affect technical, cost, or schedule risks to the project or to life cycle support of the system, but a work-around solution is known
4	a) Result in user/operator inconvenience or annoyance but does not affect a required operational or mission essential capability b) Result in inconvenience or annoyance for development or maintenance personnel, but does not prevent the accomplishment of those responsibilities
5	Any other effect

Figure13 — Priorities to be used for classifying problems

Annex N

(informative)

Candidate joint management reviews

N.1 Scope

This annex describes a candidate set of joint management reviews that might be held during a software development project. It is informative only, provided to aid in using this standard.

N.2 Assumptions

This annex makes the following assumptions:

a)) The acquirer has reviewed the subject products in advance, and one or more joint technical reviews have been held to resolve issues, leaving the joint management review as a forum to resolve open issues and reach agreement as to the acceptability of each product.
b)) Any of the reviews may be conducted incrementally, dealing at each review with a subset of the listed items or a subset of the system or software items being reviewed.

N.3 Candidate reviews

Given below is a set of candidate joint management reviews that might be held during a software development project. There is no intent to require these reviews or to preclude alternatives or combinations of these reviews. The objectives supplement those given in 5.1 8.2. Software products are expressed in lower case letters to emphasize that they are generic products, not necessarily in the form of hard-copy documents.

N.3.1 Software plan reviews

These reviews are held to resolve open issues regarding one or more of the following:

a)) The software development plan
b)) The software test plan
c)) The software installation plan
d)) The software transition plan

N.3.2 Operational concept reviews

These reviews are held to resolve open issues regarding the operational concept for a software system.

N.3.3 System/subsystem requirements reviews

These reviews are held to resolve open issues regarding the specified requirements for a software system or subsystem.

N.3.4 System/subsystem design reviews

These reviews are held to resolve open issues regarding one or more of the following:

a)) The system- or subsystem-wide design decisions
b)) The architectural design of a software system or subsystem

N.3.5 Software requirements reviews

These reviews are held to resolve open issues regarding the specified requirements for a software item.

N.3.6 Software design reviews

These reviews are held to resolve open issues regarding one or more of the following:

a)) The software item-wide design decisions
b)) The architectural design of a software item
c)) The detailed design of a software item or portion thereof (such as a database)

N.3.7 Test readiness reviews

These reviews are held to resolve open issues regarding one or more of the following:

a)) The status of the software test environment
b)) The test cases and test procedures to be used for software item qualification testing or system qualification testing
c)) The status of the software to be tested

N.3.8 Test results reviews

These reviews are held to resolve open issues regarding the results of software item qualification testing or system qualification testing.

N.3.9 Software usability reviews

These reviews are held to resolve open issues regarding one or more of the following:

a)) The readiness of the software for installation at user sites
b)) The user and operator manuals
c)) The software version descriptions
d)) The status of installation preparations and activities

N.3.10 Software maintenance reviews

These reviews are held to resolve open issues regarding one or more of the following:

a)) The readiness of the software for transition to the maintenance organization
b)) The software product specifications
c)) The software maintenance manuals
d)) The software version descriptions
e)) The status of transition preparations and activities, including transition of the software development environment, if applicable

N.3.11 Critical requirement reviews

These reviews are held to resolve open issues regarding the handling of critical requirements, such as those for safety, security, and privacy protection.

Annex O

(informative)

Candidate management indicators

O.1 Scope

This annex identifies a set of management indicators that might be used on a software development project. It is informative only, provided to aid in using this standard.

O.2 Candidate indicators

Given below is a set of candidate management indicators that might be used on a software development project. There is no intent to impose these indicators or to preclude others.

a)) Requirements volatility: total number of requirements and requirement changes over time.
b)) Software size: planned and actual number of units, lines of code, or other size measurement over time.
c)) Software staffing: planned and actual staffing levels over time.
d)) Software complexity: complexity of each software unit.
e)) Software progress: planned and actual number of software units designed, implemented, unit tested, and integrated over time.
f)) Problem/change report status: total number, number closed, number opened in the current reporting period, age, priority.
g)) Build release content: planned and actual number of software units released in each build.
h)) Computer hardware resource utilization: planned and actual use of computer hardware resources (such as processor capacity, memory capacity, input/output device capacity, auxiliary storage device capacity, and communications/network equipment capacity) over time.
i)) Milestone performance: planned and actual dates of key project milestones.
j)) Scrap/rework: amount of resources expended to replace or revise software products after they are placed under project-level or higher configuration control.
k)) Effect of reuse: a breakout of each of the indicators above for reused versus new software products.

Annex P

(informative)

Questionnaire on use of this standard

This publication of J-STD-016-1995 is as a standard for Trial Use during the period of September 1995 through September 1996. During this period reactions and comments regarding this standard are solicited. Below is a questionnaire that can help the joint IEEE/ElA working group assess the usefulness and applicability of the standard. Please feel free to copy this questionnaire for others to use. Send responses by 30 June 1996 to:

Perry DeWeese

Lockheed-Martin Aeronautical Systems

D/73-F9 MZ0685 86 South Cobb Drive

Marietta, GA 30063

FAX 404/494-1661

email: pdweese@lasc.lockheed.com

(Circle as many as apply)

Question	Response		
What are the characteristics of your project?	Small	Medium	Large
	Safety-critical	Security / Privacy-critical	Communications system
	Weapons system	Information system	State / county / city
	DoD / Federal Agency	Multinational	In-house
Did you plan to apply the standard on international projects?	Yes	No	Already apply
If you used the standard to develop non-government commercial products, what type of software do you develop?	Financial Database Medical Development tools	Client-server Artificial Intel Operating sys Word processor	Games Other (list):
If you have used the standard on client-server project applications, did the standard meet your needs?	Yes	No	Somewhat
Was the standard helpful in supporting business process reengineering activities?	Yes	No	Somewhat
Was the standard useful in facilitating the acquirer-supplier agreement/negotiation process?	Yes	No	N/A
Does the standard conflict with established company organizational-level software standards/procedures?	Yes	No	Somewhat
How does the standard affect your software time-to-market?	Improve	Delay	None/don't know
Have you found the standard to be supportive of innovative procedures in your company?	Yes	No	Somewhat
Was the standard useful for non-traditional life-cycle models?	Incremental	Evolutionary	Other
	Yes / No	Yes / No	Yes / No
Is the concept of joint reviews useful?	Yes	No	Don't know
How are you using the software product descriptions?	Checklist of information	Information in tools or database	Traditional document
Has the standard helped improve the quality of your software products?	Yes	No	Somewhat

Question	Response		
Were you able to draw a meaningful distinction between requirements and design?	Yes	No	Don't know
Were you able to draw a meaningful distinction between software architecture design and detailed design?	Yes	No	Don't know
Should the standard provide requirements on the interface between developer and the acquirer's CM control of requirements?	Yes	No	Don't care
Should the standard require that specific products be baselined at predetermined points in the development?	Yes	No	Don't care
Should the standard provide requirements on the interface between the developer and the acquirer's configuration audits?	Yes	No	Don't care
The standard has incorporated activities sometimes treated as non-software activities. Does this support your development process?	Software QA	Sys Rqmt Def	Sys Test
	Yes / No	Yes / No	Yes / No
The standard does not include activities sometimes used in software development. Should this standard include requirements on:	Domain analysis	Business Process Improvement	Data Standardization
	Yes / No	Yes / No	Yes / No
Which Military standards for software development and documentation do you currently use?	DOD-STD-2167A/2167	DOD-STD-7935A/7935	DOD-STD-1703
Which commercial standards for software development and documentation do you currently use?	IEEE Standards	EIA Standards	In-house standards

Please provide any comments that you feel will help improve this document. Attach additional sheets if necessary.

Contact information (optional):

Name: _____

Address: _____

_____

_____

Phone: _____

e-mail: _____

Bijlage W MIL-STD-1521B (USAF) 4 juni 1985, met Notice 1 19 december 1985; Military Standard Technical reviews and audits for systems, equipments, and computer software

Rijkswaterstaat
Ministerie van Infrastructuur en Waterstaat

Bijlage W MIL-STD-1521B (USAF) 4 juni 1985, met Notice 1 19 december 1985

Bijlage bij Vraagspecificatie Proces

D&C Vervanging Verlichting Schipholtunnel
Zaaknummer: 31212908

Downloaded from http://www.everyspec.com

MIL-STD-1521 B (USAF
4 JUNE 1985
SUPERSEDING
MIL-STD-1521A (USAF)
1 JUNE 1976

MILITARY STANDARD

TECHNICAL REVIEWS AND AUDITS FOR SYSTEMS, EQUIPMENTS, AND COMPUTER SOFTWARE

AMSC NO. F3631
AREA CMAN

DISTRIBUTION STATEMENT A. Approved for public release; distribution is unlimited.

Downloaded from http://www.everyspec.com

DEPARTMENT OF DEFENSE

WASHINGTON, D.C. 20301

Technical Reviews and Audits for Systems, Equipments, and Computer Software

1. This Military Standard is approved for use by all Departments and Agencies of the Department of Defense.

2. Beneficial comments (recommendations, additions, deletions) and any pertinent data which may be of use in improving this document should be addressed to: Commander, Hq ESD/ALET, Hanscom AFB, MA 01731 by using the self-addressed Standardization Document Improvement Proposal (DD Form 1426) appearing at the end of this document or by letter.

Downloaded from http://www.everyspec.com

FOREWORD

This standard has been designed to take advantage of current technological advancement and management procedures in conducting reviews and audits.

Downloaded from http://www.everyspec.com

CONTENTS

Paragraph		Page
1.	SCOPE	1
1.1	Purpose	1
1.2	Classification	1
1.3	Application	1
2.	REFERENCED DOCUMENTS	3
3.	DEFINITIONS	5
3.1	System Requirements Review (SRR)	5
3.2	System Design Review (SDR)	5
3.3	Software Specification Review (SSR)	5
3.4	Preliminary Design Review (PDR)	5
3.5	Critical Design Review (CDR)	6
3.6	Test Readiness Review (TRR)	6
3.7	Functional Configuration Audit (FCA)	6
3.8	Physical Configuration Audit (PCA)	6
3.9	Formal Qualification Review (FQR)	6
3.10	Production Readiness Review (PRR)	7
4.	GENERAL REQUIREMENTS	9
4.1	Contractor Participation and Responsibilities	9
4.1.1	Subcontractors and Suppliers	9
4.1.2	Location	9
4.1.3	Contractor Requirements	9
4.2	Contracting Agency Participation	10
4.3	Sample Forms	11
5.	DETAILED REQUIREMENTS	13
6.	NOTES	15
6.1	Intended use	15
6.2	Data requirements list and cross reference	15
6.3	Changes from previous issue	15

Downloaded from http://www.everyspec.com

FIGURES

Section		Page
Figure 1	Engineering and Test Flow.....	16
Figure 2	Sample Action Item Form.....	17
Figure 3	Sample Certification Attachment (FCA).....	85
Figure 4	Sample Certification Attachment (PCA).....	96

APPENDIXES

Appendix		Page
A.	System Requirements Review (SRR).....	19
B.	System Design Review (SDR).....	23
C.	Software Specification Review (SSR).....	31
D.	Preliminary Design Review (PDR).....	33
E.	Critical Design Review (CDR).....	53
F.	Test Readiness Review (TRR).....	69
G.	Functional Configuration Audit (FCA).....	71
H.	Physical Configuration Audit (PCA).....	75
I.	Formal Qualification Review (FQR).....	83
J.	Application Guide for Tailoring MIL-STD-1521..	117
K.	Production Readiness Review (PRR).....	123

Downloaded from http://www.everyspec.com

SECTION 1

SCOPE

1.1 Purpose. This standard prescribes the requirements for the conduct of Technical Reviews and Audits on Systems, Equipments, and Computer Software.

1.2 Classification. The following technical reviews and audits shall be selected by the program manager at the appropriate phase of program development. Each review/audit is generally described in Section 3, Definitions, and more specifically defined in a separate appendix.

System Requirements Review (SRR)
System Design Review (SDR)
Software Specification Review (SSR)
Preliminary Design Review (PDR)
Critical Design Review (CDR)
Test Readiness Review (TRR)
Functional Configuration Audit (FCA)
Physical Configuration Audit (PCA)
Formal Qualification Review (FQR)
Production Readiness Review (PRR)

NOTE: A typical engineering and test flow relative to program activities is illustrated in Figure 1.

1.3 Application. Technical Reviews and Audits defined herein shall be conducted in accordance with this standard to the extent specified in the contract clauses, Statement of Work (SOW), and the Contract Data Requirements List. Guidance in applying this standard is provided in Appendix J. The contracting agency shall tailor this standard to require only what is needed for each individual acquisition.

Downloaded from http://www.everyspec.com

SECTION 2

REFERENCED DOCUMENTS

2.1 Reference documents are not included in this document. The Statement of Work shall be referenced for applicable documents.

(Copies of specifications, standards, drawings, and publications required by contractors in connection with specific procurement functions should be obtained from the contracting agency or as directed by the contracting officer).

Downloaded from http://www.everyspec.com

SECTION 3

DEFINITIONS

TECHNICAL REVIEWS AND AUDITS

3.1 System Requirements Review (SRR). The objective of this review is to ascertain the adequacy of the contractor's efforts in defining system requirements. It will be conducted when a significant portion of the system functional requirements has been established.

3.2 System Design Review (SDR). This review shall be conducted to evaluate the optimization, correlation, completeness, and risks associated with the allocated technical requirements. Also included is a summary review of the system engineering process which produced the allocated technical requirements and of the engineering planning for the next phase of effort. Basic manufacturing considerations will be reviewed and planning for production engineering in subsequent phases will be addressed. This review will be conducted when the system definition effort has proceeded to the point where system characteristics are defined and the configuration items are identified.

3.3 Software Specification Review (SSR). A review of the finalized Computer Software Configuration Item (CSCI) requirements and operational concept. The SSR is conducted when CSCI requirements have been sufficiently defined to evaluate the contractor's responsiveness to and interpretation of the system, segment, or prime item level requirements. A successful SSR is predicated upon the contracting agency's determination that the Software Requirements Specification, Interface Requirements Specification(s), and Operational Concept Document form a satisfactory basis for proceeding into preliminary software design.

3.4 Preliminary Design Review (PDR). This review shall be conducted for each configuration item or aggregate of configuration items to (1) evaluate the progress, technical adequacy, and risk resolution (on a technical, cost, and schedule basis) of the selected design approach, (2) determine its compatibility with performance and engineering speciality requirements of the Hardware Configuration Item (HWCI) development specification, (3) evaluate the degree of definition and assess the technical risk associated with the selected manufacturing methods/processes, and (4) establish the existence and compatibility of the physical and functional interfaces among the configuration item and other items of equipment, facilities, computer software, and personnel. For CSCIs, this review will focus on: (1) the evaluation of the progress, consistency, and technical adequacy of the selected top-level design and test approach, (2) compatability between software requirements and preliminary design, and (3) on the preliminary version of the

Downloaded from http://www.everyspec.com

operation and support documents.

3.5 Critical Design Review (CDR). This review shall be conducted for each configuration item when detail design is essentially complete. The purpose of this review will be to (1) determine that the detail design of the configuration item under review satisfies the performance and engineering specialty requirements of the HWCI development specifications, (2) establish the detail design compatibility among the configuration item and other items of equipment, facilities, computer software and personnel, (3) assess configuration item risk areas (on a technical, cost, and schedule basis), (4) assess the results of the producibility analyses conducted on system hardware, and (5) review the preliminary hardware product specifications. For CSCIs, this review will focus on the determination of the acceptability of the detailed design, performance, and test characteristics of the design solution, and on the adequacy of the operation and support documents.

3.6 Test Readiness Review (TRR). A review conducted for each CSCI to determine whether the software test procedures are complete and to assure that the contractor is prepared for formal CSCI testing. Software test procedures are evaluated for compliance with software test plans and descriptions, and for adequacy in accomplishing test requirements. At TRR, the contracting agency also reviews the results of informal software testing and any updates to the operation and support documents. A successful TRR is predicated on the contracting agency's determination that the software test procedures and informal test results form a satisfactory basis for proceeding into formal CSCI testing.

3.7 Functional Configuration Audit (FCA). A formal audit to validate that the development of a configuration item has been completed satisfactorily and that the configuration item has achieved the performance and functional characteristics specified in the functional or allocated configuration identification. In addition, the completed operation and support documents shall be reviewed.

3.8 Physical Configuration Audit (PCA). A technical examination of a designated configuration item to verify that the configuration item "As Built" conforms to the technical documentation which defines the configuration item.

3.9 Formal Qualification Review (FQR). The test, inspection, or analytical process by which a group of configuration items comprising the system are verified to have met specific contracting agency contractual performance requirements (specifications or equivalent). This review does not apply to hardware or software requirements verified at FCA for the individual configuration item.

Downloaded from http://www.everyspec.com

3.10 Production Readiness Review (PRR). This review is intended to determine the status of completion of the specific actions which must be satisfactorily accomplished prior to executing a production go-ahead decision. The review is accomplished in an incremental fashion during the Full-Scale Development phase, usually two initial reviews and one final review to assess the risk in exercising the production go-ahead decision. In its earlier stages the PRR concerns itself with gross level manufacturing concerns such as the need for identifying high risk/low yield manufacturing processes or materials or the requirement for manufacturing development effort to satisfy design requirements. The reviews become more refined as the design matures, dealing with such concerns as production planning, facilities allocation, incorporation of producibility-oriented changes, identification and fabrication of tools/test equipment, long lead item acquisition etc. Timing of the incremental PRRs is a function of program posture and is not specifically locked in to other reviews.

OTHER DEFINITIONS

3.11 For further guidance on cost terminology see the latest edition of DODI 5000.33, Uniform Budget/Cost Terms and Definitions.

3.12 New titles are being phased in for the levels of maintenance. They are (with their former terms): On Equipment (Organizational), Off Equipment - On Site (Intermediate), Off Equipment - Off Site (Depot). See the latest edition of AFR 66-14, Equipment Maintenance Policies, Objectives, and Responsibilities.

3.13 For definitions of the various levels of repair, see the latest edition of MIL-STD-280A, Definition of Item Levels, Item Exchangeability, Models, and Related Terms.

3.14 Configuration item. Hardware or software, or an aggregation of both, which is designated by the contracting agency for configuration management.

Downloaded from http://www.everyspec.com

SECTION 4

GENERAL REQUIREMENTS

4.1 Contractor Participation and Responsibilities. The contractor shall be responsible for conducting the Technical Reviews and Audits in accordance with the following requirements except as amended by the contract.

4.1.1 Subcontractors and Suppliers. The contractor shall be responsible for insuring that subcontractors, vendors, and suppliers participate in formal Reviews/Audits, as appropriate.

4.1.2 Location. Unless otherwise specified in the Statement of Work, the Reviews/Audits shall be conducted at the contractor's facility or at a designated subcontractor facility, if approved by the contracting agency. Accordingly, the contractor shall be required to provide the necessary resources and material to perform the Review/Audit effectively. This includes the following items to the extent appropriate for the type and scope of Review/Audit required by the contract:

a. Meeting agenda/plans

b. Conference room(s)

c. Applicable system engineering data, specifications, drawings, manuals, schedules, and design and test data

d. Specialty study results

e. Trade study results

f. Risk analysis results

g. Mockups, breadboards, in-process hardware, and finished hardware

h. Test methods and data

i. Meeting minutes

4.1.3 Contractor Requirements. The contractor shall be responsible for establishing the time, place and agenda for each Review/Audit in consonance with the master milestone schedule, subject to coordination with the contracting agency. This should be accomplished sufficiently in advance of each Review/Audit to allow adequate preparation for the meeting by both the contractor and the contracting agency (see 6.2). In addition, the contractor shall:

4.1.3.1 Insure that each Review/Audit schedule is compatible with the availability of the necessary information and contract

Downloaded from http://www.everyspec.com

articles, e.g., system engineering data, trade study results, producibility analysis results, risk analysis results, specifications, manuals, drawings, reports, hardware, software, or mockups.

4.1.3.2 Prepare for each Review/Audit in sufficient detail consistent with the scope and magnitude of the Review/Audit.

4.1.3.3 Designate a Co-Chairperson for each Review/Audit. Participating contractor and subcontractor personnel or those chosen to make presentations shall be prepared to discuss in technical detail any of the presented material within the scope of the review.

4.1.3.4 Provide a stenographer or other acceptable method to record inputs to official meeting minutes. Minutes shall be recorded only as dictated by either Co-Chairperson and shall consist of significant questions and answers, action items, deviations, conclusions, recommended courses of action resulting from presentations or discussions. Conclusions from discussions conducted during side meetings shall be summarized in the main meeting at an appointed time, and appropriate comments shall be read into the official minutes. Recommendations not accepted should also be recorded together with the reason for non-acceptance. The minutes of each daily session shall be available for review by both the contractor and contracting agency personnel at the conclusion of each day's session (see 6.2).

4.1.3.5 Clearly record all action items in the minutes and identify whether contracting agency and/or contractor action is required for its resolution. (See Figure 2 for Sample Action Item Form).

4.1.3.6 Publish and distribute official minutes.

4.2 Contracting Agency Participation.

4.2.1 Serves as Co-Chairperson.

4.2.2 Provides the name, organization, and security clearance of each participating individual to the contractor prior to each Review/Audit.

4.2.3 Reviews the daily minutes and ensures that they reflect all significant contracting agency inputs.

4.2.4 Provides formal acknowledgement to the contractor of the accomplishment of each Review/Audit after receipt of Review/Audit minutes (see 6.1). The contracting agency establishes the adequacy of the contractor's review performance by notification of:

a. Approval -- to indicate that the review was satisfactori

Downloaded from http://www.everyspec.com

completed.

b. Contingent approval -- to indicate that the review is not considered accomplished until the satisfactory completion of resultant action items.

c. Disapproval -- to indicate that the review was seriously inadequate.

4.3 Sample Forms. A sample action item form and sample certification attachment are provided for guidance purposes (see Figures 2, 3 and 4).

Downloaded from http://www.everyspec.com

SECTION 5

DETAILED REQUIREMENTS

5.1 The appropriate Reviews or Audits will be conducted as specified in the following appendices (as selected and/or modified in the contract):

5.1.1 System Requirements Review. See Appendix A.

5.1.2 System Design Review. See Appendix B.

5.1.3 Software Specification Review. See Appendix C.

5.1.4 Preliminary Design Review. See Appendix D.

5.1.5 Critical Design Review. See Appendix E.

5.1.6 Test Readiness Review. See Appendix F.

5.1.7 Functional Configuration Audit. See Appendix G.

5.1.8 Physical Configuration Audit. See Appendix H.

5.1.9 Formal Qualification Review. See Appendix I.

5.1.10 Application Guide For Tailoring MIL-STD-1521. See Appendix J.

5.1.11 Production Readiness Review. See Appendix K.

Downloaded from http://www.everyspec.com

SECTION 6

NOTES

6.1 Intended use. This standard prescribes the requirements for conducting Technical Reviews and Audits on Systems, Equipments, and Computer Software. Official acknowledgement by the contracting agency of the accomplishment of a Review/Audit is not to be interpreted as approval of statements made in the minutes or of matters discussed at the Review/Audit and does not relieve the contractor from requirements which are a part of the contract.

6.2 Data requirements list and cross reference. When this standard is used in an acquisition which incorporates a DD Form 1423, Contract Data Requirements List (CDRL), the data requirements identified below shall be developed as specified by an approved Data Item Description (DD Form 1664) and delivered in accordance with the approved CDRL incorporated into the contract. When the provisions of the DOD FAR clause on data requirements (currently DOD FAR Supplement 52.227-7031) are invoked and the DD Form 1423 is not used, the data specified below shall be delivered by the contractor in accordance with the contract or purchase order requirements. Deliverable data required by this standard is cited in the following paragraphs.

Paragraph No.	Data Requirement Title	Applicable DID No.
4.1.3	Conference Agenda	DI-A-7088
4.1.3.4	Conference Minutes	DI-A-7089

(Data item descriptions related to this standard, and identified in section 6 will be approved and listed as such in DOD 5000.19-L., Vol. II, AMSDL. Copies of data item descriptions required by the contractors in connection with specific acquisition functions should be obtained from the Naval Publications and Forms Center or as directed by the contracting officer.)

6.3 Changes from previous issue. Asterisks or vertical lines are not used in this revision to identify changes with respect to the previous issue due to the extensiveness of the changes.

Downloaded from http://www.everyspec.com

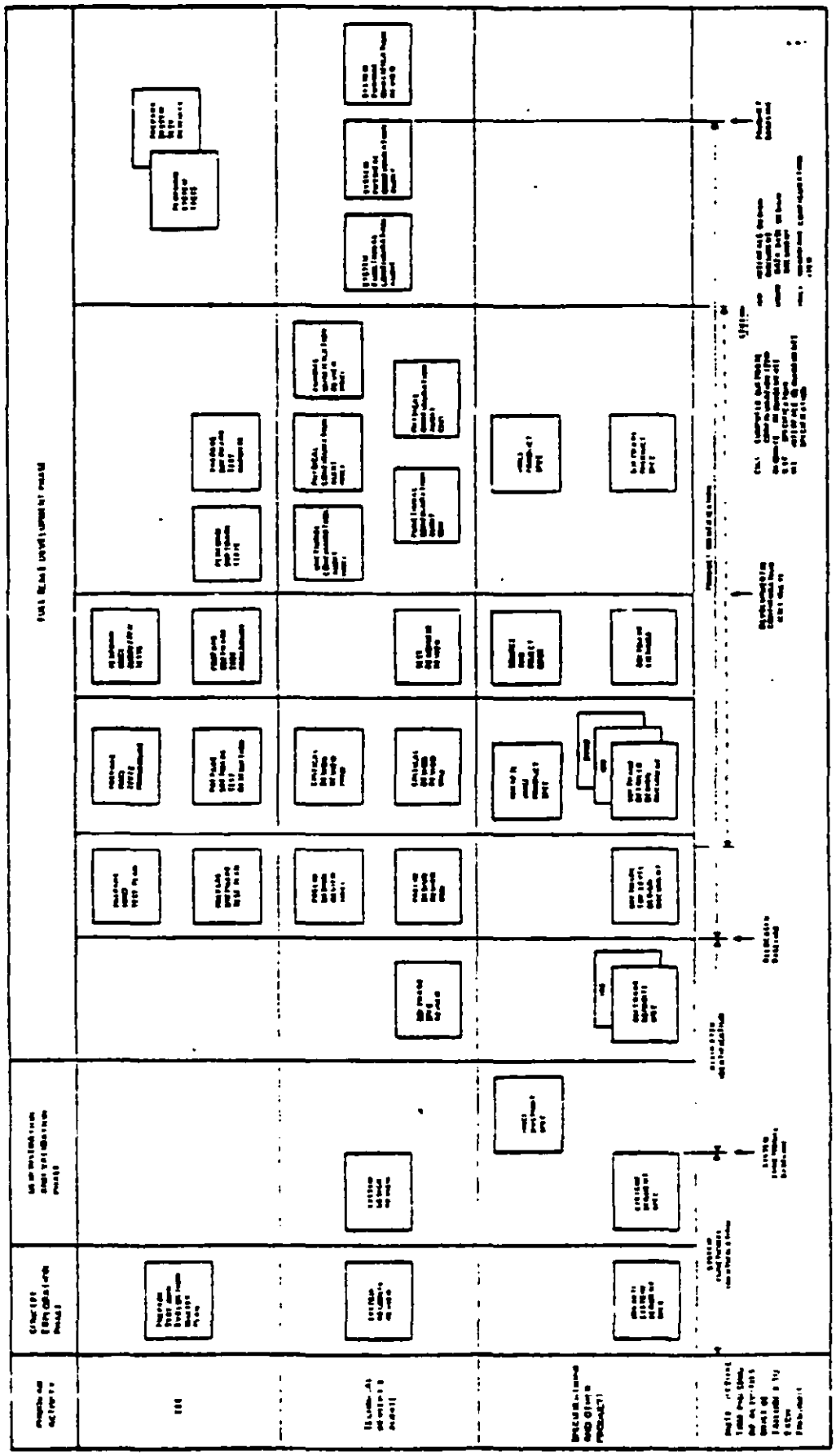


FIGURE 1. Engineering and Test Flow.

Downloaded from http://www.everyspec.com

ACTION ITEM

CONTROL NUMBER _____

DATE OF MEETING	SUBJECT:	LOCATION
ACTION REQUIRED/COMPLIANCE		DUE DATE _____
ASSIGNED TO: _____		ORIGINATOR
_____		AGENCY
FOLLOW UP STATUS: _____		
ASSIGNEE:		
DATE COMPLETED:		DOCUMENT NO.

COORDINATORS			TECHNICAL APPROVAL
PHONE	AGENCY	SIGNATURE	DATE
PHONE	AGENCY	SIGNATURE	DATE
PHONE	AGENCY	SIGNATURE	DATE

CONTRACTING AGENCY	DATE	CONTRACTOR	DATE	CONTRACTS	DATE

Figure 2 Sample Action Item Form

Downloaded from http://www.everyspec.com

10. System Requirements Review (SRR).

10.1 General. The SRRs are normally conducted during the system Concept Exploration or Demonstration and Validation phase. Such reviews may be conducted at any time but normally will be conducted after the accomplishment of functional analysis and preliminary requirements allocation (to operational/maintenance/training Hardware Configuration Items (HWCIs), Computer Software Configuration Items (CSCIs), facility configuration items, manufacturing considerations, personnel and human factors) to determine initial direction and progress of the contractor's System Engineering Management effort and his convergence upon an optimum and complete configuration.

10.2 Purpose. The total System Engineering Management activity and its output shall be reviewed for responsiveness to the Statement of Work and system/segment requirements. Contracting agency direction to the contractor will be provided, as necessary, for continuing the technical program and system optimization.

10.3 Items to be Reviewed. Representative items to be reviewed include the results of the following, as appropriate:

a. Mission and Requirements Analysis

b. Functional Flow Analysis

c. Preliminary Requirements Allocation

d. System/Cost Effectiveness Analysis

e. Trade Studies (e.g., addressing system functions in hardware/firmware/software)

f. Synthesis

g. Logistics Support Analysis

h. Specialty Discipline Studies (i.e., hardware and software reliability analysis, maintainability analysis, armament integration, electromagnetic compatibility, survivability/vulnerability (including nuclear), inspection methods/techniques analysis, energy management, environmental considerations).

i. System Interface Studies

j. Generation of Specifications

k. Program Risk Analysis

l. Integrated Test Planning

Downloaded from http://www.everyspec.com

m. Producibility Analysis Plans

n. Technical Performance Measurement Planning

o. Engineering Integration

p. Data Management Plans

q. Configuration Management Plans

r. System Safety

s. Human Factors Analysis

t. Value Engineering Studies

u. Life Cycle Cost Analysis

v. Preliminary Manufacturing Plans

w. Manpower Requirements/Personnel Analysis

x. Milestone Schedules

10.3.1 The contractor shall describe his progress and problems in:

10.3.1.1 Risk identification and risk ranking (the interrelationship among system effectiveness analysis, technical performance measurement, intended manufacturing methods, and costs shall be discussed, as appropriate).

10.3.1.2 Risk avoidance/reduction and control (the interrelationships with trade-off studies, test planning, hardware proofing, and technical performance measurement shall be discussed, as appropriate).

10.3.1.3 Significant trade-offs among stated system/segment specification requirements/constraints and resulting engineering design requirements/constraints, manufacturing methods/process constraints, and logistic/cost of ownership requirements/constraints and unit production cost/design-to-cost objectives.

10.3.1.4 Identifying computer resources of the system and partitioning the system into HWCIs and CSCIs. Include any trade-off studies conducted to evaluate alternative approaches and methods for meeting operational needs and to determine the effects of constraints on the system. Also include any evaluations of logistics, technology, cost, schedule, resource limitations, intelligence estimates, etc., made to determine their impact on the system. In addition, address the following specific tradeoffs related to computer resources:

Downloaded from http://www.everyspec.com

a. Candidate programming languages and computer architectures evaluated in light of DoD requirements for approved higher order languages and standard instruction set architectures.

b. Alternative approaches evaluated for implementing security requirements. If an approach has been selected, discuss how it is the most economical balance of elements which meet the total system requirements.

c. Alternative approaches identified for achieving the operational and support concepts, and, for joint service programs, opportunities for interservice support.

10.3.1.5 Producibility and manufacturing considerations which could impact the program decision such as critical components, materials and processes, tooling and test equipment development, production testing methods, long lead items, and facilities/personnel/skills requirements.

10.3.1.6 Significant hazard consideration should be made here to develop requirements and constraints to eliminate or control these system associated hazards.

10.3.2 Information which the contractor identifies as being useful to his analysis and available through the contracting agency shall be requested prior to this review (e.g., prior studies, operational/support factors, cost factors, safety data, test plan(s), etc.). A separate SRR may be conducted for each of the operational support subsystems depending upon the nature and complexity of the program.

10.4 Post Review Action. After completing the SRR, the contractor shall publish and distribute copies of Review minutes. The contracting agency officially acknowledges completion of the SRR as indicated in paragraph 4.2.4.

Downloaded from http://www.everyspec.com

20. System Design Review (SDR).

20.1 General. The SDR shall be conducted to evaluate the optimization, traceability, correlation, completeness, and the risk of the allocated requirements, including the corresponding test requirements in fulfilling the system/segment requirements (the functional baseline). The review encompasses the total system requirements, i.e., operations/maintenance/test/training hardware, computer software, facilities, personnel, preliminary logistic support considerations. Also included shall be a summary review of the System Engineering Management Activities (e.g., mission and requirements analysis, functional analysis, requirements allocation, manufacturing methods/process selection, program risk analysis, system/cost effectiveness analysis, logistics support analysis, trade studies, intra- and inter-system interface studies, integrated test planning, specialty discipline studies, and Configuration Management) which produced the above system definition products. A technical understanding shall be reached on the validity and the degree of completeness of the following information:

a. System/Segment Specification

b. The engineering design/cost of the system (see Section 3, Definitions).

c. Preliminary Operational Concept Document

d. Preliminary Software Requirements Specification

e. Preliminary Interface Requirements Specification(s)

f. As appropriate:

(1) Prime Item Development Specification

(2) Critical Item Development Specification

20.2 Purpose. An SDR shall be conducted as the final review prior to the submittal of the Demonstration and Validation Phase products or as the initial Full Scale Development Review for systems not requiring a formal Demonstration and Validation Phase but sufficiently complex to warrant the formal assessment of the allocated requirements (and the basis of these requirements) before proceeding with the preliminary design of HWCIs or the detailed requirements analysis for CSCIs. The SDR is primarily concerned with the overall review of the operational/support requirements (i.e., the mission requirements), updated/completed System/Segment Specification requirements, allocated performance requirements, programming and manufacturing methods/processes/planning, and the accomplishment of the System Engineering Management activities to insure that the definition

Downloaded from http://www.everyspec.com

effort products are necessary and sufficient. The purposes of the SDR are to:

20.2.1 Insure that the updated/completed System/Segment Specification is adequate and cost effective in satisfying validated mission requirements.

20.2.2 Insure that the allocated requirements represent a complete and optimal synthesis of the system requirements.

20.2.3 Insure that the technical program risks are identified, ranked, avoided, and reduced through:

a. Adequate trade-offs (particularly for sensitive mission requirements versus engineering realism and manufacturing feasibility to satisfy the anticipated production quantities of corresponding performance requirements);

b. Subsystem/component hardware proofing;

c. A responsive test program; and

d. Implementation of comprehensive engineering disciplines (e.g., worst case analysis, failure mode and effects analysis, maintainability analysis, producibility analysis and standardization.)

20.2.4 Identify how the final combination of operations, manufacturing, maintenance, logistics and test and activation requirements have affected overall program concepts; quantities and types of equipment, unit product cost (see Section 3, Definitions, paragraph 3.11), computer software, personnel, and facilities.

20.2.5 Insure that a technical understanding of requirements has been reached and technical direction is provided to the contractor.

20.3 Items to be Revieved. The SDR shall include a review of the following items, as appropriate:

20.3.1 System Engineering Management Activities, e.g.:

a. Mission and Requirements Analysis

b. Functional Analysis

c. Requirements Allocation

d. System/Cost Effectiveness

e. Synthesis

Downloaded from http://www.everyspec.com

f. Survivability/Vulnerability (including nuclear)

g. Reliability/Maintainability/Availability (R/M/A)

h. Electromagnetic Compatibility

i. Logistics Support Analysis (to address, as appropriate, integrated logistics support including logistics support concept, maintenance, supply, software support facilities, etc.)

j. System Safety (emphasis shall be placed on system hazard analysis and identification of safety test requirements)

k. Security

l. Human Factors

m. Transportability (including Packaging and Handling)

n. System Mass Properties

o. Standardization

p. Electronic Warfare

q. Value Engineering

r. System Growth Capability

s. Program Risk Analysis

t. Technical Performance Measurement Planning

u. Producibility Analysis and Manufacturing

v. Life Cycle Cost/Design to Cost Goals

w. Quality Assurance Program

x. Environmental Conditions (Temperature, Vibration, Shock, Humidity, etc.)

y. Training and Training Support

z. Milestone Schedules

aa. Software Development Procedures

20.3.2 Results of significant trade studies, for example:

a. Sensitivity of selected mission requirements versus

Downloaded from http://www.everyspec.com

realistic performance parameters and cost estimates.

b. Operations design versus maintenance design

c. System centralization versus decentralization

d. Automated versus manual operation

e. Reliability/Maintainability/Availability

f. Commercially available items versus new developments

g. National Stock Number (NSN) items versus new development

h. Testability trade studies (Allocation of fault detection/isolation capabilities between elements of built-in test, on board/on-site fault detection/isolation subsystems, separate support equipment, and manual procedures)

i. Size and weight

j. Desired propagation characteristics versus reduction in interference to other systems (optimum selection of frequencies)

k. Performance/logistics trade studies

l. Life cycle cost reduction for different computer programming languages

m. Functional allocation between hardware, software, firmware and personnel/procedures

n. Life Cycle Cost/system performance trade studies to include sensitivity of performance parameters to cost.

o. Sensitivity of performance parameters versus cost

p. Cost versus performance

q. Design versus manufacturing consideration

r. Make versus buy

s. Software development schedule

20.3.3 Updated design requirements for operations/maintenance functions and items.

20.3.4 Updated requirements for manufacturing methods and processes.

Downloaded from http://www.everyspec.com

20.3.5 Updated operations/maintenance requirements for facilities.

20.3.6 Updated requirements for operations/maintenance personnel and training.

20.3.7 Specific actions to be performed include evaluations of:

a. System design feasibility and system/cost effectiveness

b. Capability of the selected configuration to meet requirements of the System/Segment Specification

c. Allocations of system requirements to subsystems/configuration items

d. Use of commercially available and standard parts

e. Allocated inter- and intra- system interface requirements

f. Size, weight, and configuration of HWCIs to permit economical and effective transportation, packaging, and handling consistent with applicable specifications and standards

g. Specific design concepts which may require development toward advancing the state-of-the-art

h. Specific subsystems/components which may require "hardware proofing" and high-risk long-lead time items

i. The ability of inventory items to meet overall system requirements, and their compatibility with configuration item interfaces

j. The planned system design in view of providing multi-mode functions, as applicable

k. Considerations given to:

(1) Interference caused by the external environment to the system and the system to the external environment.

(2) Allocated performance characteristics of all system transmitters and receivers to identify potential intra-system electromagnetic (EM) incompatibilities.

(3) Non-design, spurious and harmonic system performance characteristics and their effect on electromagnetic environments of operational deployments.

l. Value Engineering studies, preliminary Value Engineering Change Proposals (VECPs) and VECPs (as applicable).

Downloaded from http://www.everyspec.com

20.3.8 Review the Preliminary Operational Concept Document, and sections 1.0, 2.0, 3.0, 5.0, 6.0, and 10.0 of the System/Segment Specification, all available HWCI Development Specifications, preliminary Software Requirements, and Interface Requirements Specifications for format, content, technical adequacy, completeness and traceability/correlation to the validated mission/support requirements. All entries marked "not applicable (N/A)" or "to be determined (TBD)" are identified and explained by the contractor.

20.3.9 Review section 4.0 of the System/Segment Specification, all available hardware Development Specifications, and preliminary Software Requirements and Interface Requirements Specifications for format, content, technical adequacy, and completeness. All available test documentation, including HWCI/subsystem and system test plans, shall be reviewed to insure that the proposed test program satisfies the test requirements of section 4.0 of all applicable specifications. All entries labeled "not applicable (N/A)" or "to be determined (TBD)" in section 4.0 of any applicable specification are identified and explained by the contractor.

20.3.10 Review the system, HWCI, and CSCI design for interaction with the natural environment. If any effect or interaction is not completely understood and further study is required, or it is known but not completely compensated for in the design, the proposed method of resolution shall also be reviewed. All proposed environmental tests shall be reviewed for compatibility with the specified natural environmental conditions.

20.3.11 Maintenance functions developed by the contractor to determine that support concepts are valid, technically feasible, and understood. In particular, attention is given to:

a. R/M/A considerations in the updated System/Segment Specification

b. Maintenance design characteristics of the system

c. Corrective and preventive maintenance requirements

d. Special equipment, tools, or material required

e. Requirements or planning for automated maintenance analysis

f. Item Maintenance Analysis compatibility with required maintenance program when weapon is deployed

g. Specific configuration item support requirements

h. Forms, procedures, and techniques for maintenance analysis

Downloaded from http://www.everyspec.com

i. Maintenance related trade-off studies and findings (includes commercially available equipment, software fault diagnostic techniques)

j. Logistic cost impacts

k. Support procedures and tools for computer software which facilitate software modification, improvements, corrections and updates

l. Hardness critical items/processes

20.3.12 System compliance with nuclear, non-nuclear and laser hardening requirements. High risk areas or design concepts requiring possible advances of the state-of-the-art as a result of survivability critieria shall be identified, and prepared approach(es) to the problem reviewed. Prepared test programs shall be reviewed for sufficiency and compatibility with the specified threat environment and existing simulation test facilities.

20.3.13 The optimization, traceability, completeness, and risks associated with the allocated technical requirements, and the adequacy of allocated system requirements as a basis for proceeding with the development of hardware and software configuration items. Include any available preliminary Software Requirements and Interface Requirements Specifications.

20.3.14 Manufacturing (HWCIs only).

20.3.14.1 Production feasibility and risk analyses addressed at the SRR shall be updated and expanded. This effort should review the progress made in reducing production risk and evaluate the risk remaining for consideration in the Full Scale Development Phase. Estimates of cost and schedule impacts shall be updated.

20.3.14.2 Review of the Production Capability Assessment shall include:

20.3.14.2.1 A review of production capability shall be accomplished which will constitute an assessment of the facilities, materials, methods, processes, equipment and skills necessary to perform the full scale development and production efforts. Identification of requirements to upgrade or develop manufacturing capabilities shall be made. Requirements for Manufacturing Technology (MANTECH) programs will also be identified as an element of this production assessment.

20.3.14.3 Present the management controls and the design/manufacturing engineering approach to assure that the equipment is producible.

Downloaded from http://www.everyspec.com

20.3.14.4 Present a review of trade-off studies for design requirements against the requirement for producibility, facilities, tooling, production test equipment, inspection, and capital equipment for intended production rates and volume.

20.3.14.5 The analysis, assessments and trade-off studies should recommend any additional special studies or development efforts as needed.

20.4 Post Review Action. After completing the SDR, the contractor shall publish and distribute copies of Review Minutes. The contracting agency officially acknowledges completion of the SDR as indicated in paragraph 4.2.4.

Downloaded from http://www.everyspec.com

30. Software Specification Review (SSR).

30.1 General. The SSR shall be a formal review of a CSCI's requirements as specified in the Software Requirements Specification and the Interface Requirements Specification(s). Normally, it shall be held after System Design Review but prior to the start of CSCI preliminary design. A collective SSR for a group of configuration items, treating each configuration item individually, may be held when such an approach is advantageous to the contracting agency. Its purpose is to establish the allocated baseline for preliminary CSCI design by demonstrating to the contracting agency the adequacy of the Software Requirements Specification (SRS), Interface Requirements Specification(s) (IRS), and Operational Concept Document (OCD).

30.2 Items to be reviewed. The contractor shall present the following items for review by the contracting agency:

a. Functional overview of the CSCI, including inputs, processing, and outputs of each function.

b. Overall CSCI performance requirements, including those for execution time, storage requirements, and similar constraints.

c. Control flow and data flow between each of the software functions that comprise the CSCI.

d. All interface requirements between the CSCI and all other configuration items both internal and external to the system.

e. Qualification requirements that identify applicable levels and methods of testing for the software requirements that comprise the CSCI.

f. Any special delivery requirements for the CSCI.

g. Quality factor requirements; i.e., Correctness, Reliability, Efficiency, Integrity, Usability, Maintainability, Testability, Flexibility, Portability, Reusability, and Interoperability.

h. Mission requirements of the system and its associated operational and support environments.

i. Functions and characteristics of the computer system within the overall system.

j. Milestone schedules.

k. Updates since the last review to all previously delivered

Downloaded from http://www.everyspec.com

software related CDRL items.

1. Any actions or procedures deviating from approved plans.

30.3 Post Review Action. After completing the SSR, the contractor shall publish and distribute copies of Review Minutes. The contracting agency officially acknowledges completion of the SSR as indicated in paragraph 4.2.4.

30.3.1 The accomplishment of the SSR shall be recorded on the configuration item Development Record by the contractor (see MIL-STD-483, Appendix VII).

Downloaded from http://www.everyspec.com

40. Preliminary Design Review (PDR)

40.1 General. The PDR shall be a formal technical review of the basic design approach for a configuration item or for a functionally related group of configuration items. It shall be held after the Hardware Development Specification(s), the Software Top Level Design Document (STLDD), the Software Test Plan (STP), the HWCI Test Plan, and preliminary versions of the Computer System Operator's Manual (CSOM), Software User's Manual (SUM), Computer System Diagnostic Manual (CSDM), and Computer Resources Integrated Support Document (CRISD) are available, but prior to the start of detailed design. For each configuration item the actions described below may be accomplished as a single event, or they may be spread over several events, depending on the nature and the extent of the development of the configuration item, and on provisions specified in the contract Statement of Work. A collective PDR for a group of configuration items, treating each configuration item individually, may be held when such an approach is advantageous to the contracting agency; such a collective PDR may also be spread over several events, as for a single configuration item. The overall technical program risks associated with each configuration item shall also be reviewed on a technical, cost, and schedule basis. For software, a technical understanding shall be reached on the validity and the degree of completeness of the STLDD, STP, and the preliminary versions of the CSOM, SUM, CSDM, and CRISD.

40.2 Items to be Reviewed. The contractor shall present the following for review by the contracting agency:

40.2.1 HWCIs:

a. Preliminary design synthesis of the hardware Development Specification for the item being reviewed.

b. Trade-studies and design studies results (see paragraph 20.3.2 of SDR for a representative listing).

c. Functional flow, requirements allocation data, and schematic diagrams.

d. Equipment layout drawings and preliminary drawings, including any proprietary or restricted design/process/components and information.

e. Environment control and thermal design aspects

f. Electromagnetic compatibility of the preliminary design

g. Power distribution and grounding design aspects

h. Preliminary mechanical and packaging design of consoles,

Downloaded from http://www.everyspec.com

racks, drawers, printed circuit boards, connectors, etc.

i. Safety engineering considerations

j. Security engineering considerations

k. Survivability/Vulnerability (including nuclear) considerations

l. Preliminary lists of materials, parts, and processes

m. Pertinent relability/maintainability/availability data

n. Preliminary weight data

o. Development test data

p. Interface requirements contained in configuration item Development Specifications and interface control data (e.g., interface control drawings) derived from these requirements

q. Configuration item development schedule

r. Mock-ups, models, breadboards, or prototype hardware when appropriate

s. Producibility and Manufacturing Considerations (e.g., materials, tooling, test equipment, processes, facilities, skills, and inspection techniques). Identify single source, sole source, diminishing source.

t. Value Engineering Considerations, Preliminary VECPs and VECPs (if applicable).

u. Transportability, packaging, and handling considerations

v. Human Engineering and Biomedical considerations (including life support and Crew Station Requirements).

w. Standardization considerations

x. Description and characteristics of commercially available equipment, including any optional capabilities such as special features, interface units, special instructions, controls, formats, etc., (include limitations of commercially available equipment such as failure to meet human engineering, safety, and maintainability requirements of the specification and identify deficiencies).

y. Existing documentation (technical orders, commercial manuals, etc.,) for commercially available equipment and copies of contractor specifications used to procur

Downloaded from http://www.everyspec.com

equipment shall be made available for review by the contracting agency.

z. Firmware to be provided with the system: microprogram logic diagrams and reprogramming/instruction translation algorithm descriptions, fabrication, packaging (integration technology (e.g., LSI, MSI), device types (e.g., CMOS, PMOS)), and special equipment and support software needed for developing, testing, and supporting the firmware.

aa. Life Cycle Cost Analysis

ab. Armament compatibility

ac. Corrosion prevention/control considerations

ad. Findings/Status of Quality Assurance Program

40.2.2 CSCIs:

a. Functional flow. The computer software functional flow embodying all of the requirements allocated from the Software Requirements Specification and Interface Requirements Specification(s) to the individual Top-Level Computer Software Components (TLCSCs) of the CSCI.

b. Storage allocation data. This information shall be presented for each CSCI as a whole, describing the manner in which available storage is allocated to individual TLCSCs. Timing, sequencing requirements, and relevant equipment constraints used in determining the allocation are to be included.

c. Control functions description. A description of the executive control and start/recovery features for the CSCI shall be available, including method of initiating system operation and features enabling recovery from system malfunction.

d. CSCI structure. The contractor shall describe the top-level structure of the CSCI, the reasons for choosing the components described, the development methodology which will be used within the constraints of the available computer resources, and any support programs which will be required in order to develop/maintain the CSCI structure and allocation of data storage.

e. Security. An identification of unique security requirements and a description of the techniques to be used for implementing and maintaining security within the CSCI shall be provided.

Downloaded from http://www.everyspec.com

f. Reentrancy. An identification of any reentrancy requirements and a description of the techniques for implementing reentrant routines shall be available.

g. Computer software development facilities. The availability, adequacy, and planned utilization of the computer software development facilities shall be addressed.

h. Computer software development facility versus the operational system. The contractor shall provide information relative to unique design features which may exist in a TLCSC in order to allow use within the computer software development facility, but which will not exist in the TLCSC installed in the operational system. The contractor shall provide information on the design of support programs not explicitly required for the operational system but which will be generated to assist in the development of the CSCI(s). The contractor shall also provide details of the Software Development Library controls.

i. Development tools. The contractor shall describe any special simulation, data reduction, or utility tools that are not deliverable under the terms of the contract, but which are planned for use during software development.

j. Test tools. The contractor shall describe any special test systems, test data, data reduction tools, test computer software, or calibration and diagnostic software that are not deliverable under terms of the contract, but which are planned for use during product development.

k. Description and characteristics of commercially available computer resources, including any optional capabilities such as special features, interface units, special instructions, controls, formats, etc. Include limitations of commercially available equipment such as failure to meet human engineering, safety and maintainability requirements of the specification and identify deficiencies.

l. Existing documentation (technical orders, commercial manuals, etc.) for commercially available computer resources and copies of contractor specifications used to procure computer resources shall be made available for review by the contracting agency.

m. Support resources. The contractor shall describe those resources necessary to support the software and firmware during operational deployment of the system, such as operational and support hardware and software, personnel, special skills, human factors, configuration management, test, and facilities/space.

Downloaded from http://www.everyspec.com

n. Operation and support documents. The preliminary versions of the CSOM, SUM, CSDM, and CRISD shall be reviewed for technical content and compatability with the top-level design documentation.

o. Updates since the last review to all previously delivered software related CDRL items.

p. Review considerations applicable to 40.2.1 as appropriate.

40.2.3 Support Equipment (SE):

a. Review considerations applicable to paragraph 40.2.1 and 40.2.2 as appropriate.

b. Verify testability analysis results. For example, on repairable integrated circuit boards are test points available so that failures can be isolated to the lowest level of repair (See Section 3 Definitions, for "Levels of repair").

c. Verify that the Government furnished SE is planned to be used to the maximum extent possible.

d. Review progress of long-lead time SE items, identified through interim release and SE Requirements Document (SERD) procedures.

e. Review progress toward determining total SE requirements for installation, checkout, and test support requirements.

f. Review the reliability/maintainability/availability of support equipment items.

g. Identify logistic support requirements for support equipment items and rationale for their selection.

h. Review calibration requirements.

i. Describe technical manuals and data availability for support equipment.

j. Verify compatibility of proposed support equipment with the system maintenance concept.

k. If a Logistic Support Analysis (LSA) is not done, then review the results of SE trade-off studies for each alternative support concept. For existing SE and printed circuit board testers, review Maintainability data resulting from the field use of these equipments. Review the cost difference between systems using single or multipurpose SE vs. proposed new SE. Examine technical feasibility in

Downloaded from http://www.everyspec.com

using existing, developmental, and proposed new SE. For mobile systems, review the mobility requirements of support equipment.

l. Review the relationship of the computer resources in the system/subsystem with those in Automatic Test Equipment (ATE). Relate this to the development of Built In Test Equipment (BITE) and try to reduce the need for complex supporting SE.

40.3 Evaluation of Electrical, Mechanical, and Logical Designs

40.3.1 HWCIs. The material of paragraph 40.2.1 above shall be evaluated to:

a. Determine that the preliminary detail design provides the capability of satisfying the performance characteristics paragraph of the HWCI Development specifications.

b. Establish compatibility of the HWCI operating characteristics in each mode with overall system design requirements if the HWCI is involved in multi-mode functions.

c. Establish the existence and nature of physical and functional interfaces between the HWCI and other items of equipment, computer software, and facilities.

40.3.2 CSCIs. The material of paragraph 40.2.2 above shall be evaluated to:

a. Determine whether all interfaces between the CSCI and all other configuration items both internal and external to the system meet the requirements of the Software Requirements Specification and Interface Requirements Specification(s).

b. Determine whether the top-level design embodies all the requirements of the Software Requirements and Interface Requirements Specifications.

c. Determine whether the approved design methodology has been used for the top-level design.

d. Determine whether the appropriate Human Factors Engineering (HFE) principals have been incorporated in the design.

e. Determine whether timing and sizing constraints have been met throughout the top-level design.

f. Determine whether logic affecting system and nuclear safety has been incorporated in the design.

Downloaded from http://www.everyspec.com

40.4 Electromagnetic Compatibility. Review HWCI design for compliance with electromagnetic compatibility/electromagnetic interference (EMC/EMI) requirements. Use Electromagnetic Compatibility Plan as the basis for this review. Check application of MIL-STDs and MIL-Specs cited by the system/equipment specification(s) to the HWCI/Subsystem design. Review preliminary EMI test plans to assess adequacy to confirm that EMC requirements have been met.

40.5 Design Reliability.

40.5.1 Identify the quantitative reliability requirements specified in the hardware Development and Software Requirements Specification(s), including design allocations, and the complexity of the CSCIs.

40.5.2 Review failure rate sources, derating policies, and prediction methods. Review the reliability mathematical models and block diagrams as appropriate.

40.5.3 Describe planned actions when predictions are less than specified requirements.

40.5.4 Identify and review parts or components which have a critical life or require special consideration, and general plan for handling. Agencies so affected shall present planned actions to deal with these components or parts.

40.5.5 Identify applications of redundant HWCI elements. Evaluate the basis for their use and provisions for "on-line" switching of the redundant element.

40.5.6 Review critical signal paths to determine that a fail-safe/fail-soft design has been provided.

40.5.7 Review margins of safety for HWCIs between functional requirements and design provisions for elements, such as: power supplies, transmitter modules, motors, and hydraulic pumps. Similarly, review structural elements; i.e., antenna pedestals, dishes, and radomes to determine that adequate margins of safety shall be provided between operational stresses and design strengths.

40.5.8 Review Reliability Design Guidelines for HWCIs to insure that design reliability concepts shall be available and used by equipment designers. Reliability Design Guidelines shall include, as a minimum, part application guidelines (electrical derating, thermal derating, part parameter tolerances), part selection order of preference, prohibited parts/materials, reliability apportionments/predictions, and management procedures to ensure compliance with the guidelines.

Downloaded from http://www.everyspec.com

40.5.9 Review for HWCIs preliminary reliability demonstration plan: failure counting ground rules, accept-reject criteria, number of test articles, test location and environment, planned starting date, and test duration.

40.5.10 Review elements of reliability program plan to determine that each task has been initiated toward achieving specified requirements.

40.5.11 Review subcontractor/supplier reliability controls.

40.6 Design Maintainability

40.6.1 Identify the quantitative maintainability requirements specified in the hardware Development and Software Requirements Specifications; if applicable, compare preliminary predictions with specified requirements.

40.6.2 Review HWCI preventive maintenance schedules in terms of frequencies, durations, and compatibility with system schedules.

40.6.3 Review repair rate sources and prediction methods.

40.6.4 Review planned actions when predictions indicate that specified requirements will not be attained.

40.6.5 Review planned designs for accessibility, testability, and ease of maintenance characteristics (including provisions for automatic or operator-controlled recovery from failure/malfunctions) to determine consistency with specified requirements.

40.6.6 Determine if planned HWCI design indicates that parts, assemblies, and components will be so placed that there is sufficient space to use test probes, soldering irons, and other tools without difficulty and that they are placed so that structural members of units do not prevent access to them or their ease of removal.

40.6.7 Review provisions for diagnosing cause(s) of failure; means for localizing source to lowest replaceable element; adequacy and locations of planned test points; and planned system diagnostics that provide a means for isolating faults to and within the configuration item . This review shall encompass on-line diagnostics, off-line diagnostics, and proposed technical orders and/or commercial manuals.

40.6.8 Review for HWCIs the Design for Maintainability Checklist to insure that listed design principles shall lead to a mature maintainability design. Determine that contractor design engineers are using the checklist.

Downloaded from http://www.everyspec.com

40.6.9 Evaluate for HWCIs the preliminary maintainability demonstration plan, including number of maintenance tasks that shall be accomplished; accept-reject criteria; general plans for introducing faults into the HWCI and personnel involved in the demonstration.

40.6.10 Review elements of maintainability program plan to determine that each task has been initiated towards achieving specified requirements.

40.6.11 Insure that consideration has been given to optimizing the system/item from a maintainability and maintenance viewpoint and that it is supportable within the maintenance concept as developed. Also, for HWCIs insure that a Repair Level Analysis (RLA) has been considered.

40.7 Human Factors

40.7.1 The contractor shall present evidence that substantiates the functional allocation decisions. The Review shall cover all operational and maintenance functions of the configuration item. In particular, ensure that the approach to be followed emphasizes the functional integrity of the man with the machine to accomplish a system operation.

40.7.2 Review design data, design descriptions and drawings on system operations, equipments, and facilities to insure that human performance requirements of the hardware Development and Software Requirements Specifications are met. Examples of the types of design information to be reviewed are:

a. Operating modes for each display station, and for each mode, the functions performed, the displays and control used, etc.

b. The exact format and content of each display, including data locations, spaces, abbreviations, the number of digits, all special symbols (Pictographic), alert mechanisms (e.g., flashing rates), etc.

c. The control and data entry devices and formats including keyboards, special function keys, cursor control, etc.

d. The format of all operator inputs, together with provisions for error detection and correction.

e. All status, error, and data printouts - including formats, headings, data units, abbreviations, spacings, columns, etc.

These should be presented in sufficient detail to allow contracting agency personnel to judge adequacy from a human usability standpoint, and design personnel to know what is required, and test personnel to prepare tests.

Downloaded from http://www.everyspec.com

40.7.3 Make recommendations to update the System/Segment, or Software Requirements Specification and Interface Requirements Specification(s) in cases where requirements for human performance need to be more detailed.

40.7.4 Review man/machine functions to insure that man's capabilities are utilized and that his limitations are not exceeded.

40.8 System Safety

40.8.1 Review results of configuration item safety analyses, and quantitative hazard analyses (if applicable).

40.8.2 Review results of system and intra-system safety interfaces and trade-off studies affecting the configuration item.

40.8.3 Review safety requirements levied on subcontractors.

40.8.4 Review known special areas of safety, peculiar to the nature of the system (e.g., fuel handling, fire protection, high levels of radiated energy, high voltage protection, safety interlocks, etc.).

40.8.5 Review results of preliminary safety tests (if appropriate).

40.8.6 Generally review adequacy and completeness of configuration item from design safety viewpoint.

40.8.7 Review compliance of commercially available configuration items or configuration item components with system safety requirements and identify modifications to such equipment, if required.

40.9 Natural Environment

40.9.1 Review contractor's planned design approach toward meeting climatic conditions (operating and non-operating ranges for temperature, humidity, etc.) that are specified in the HWCI Development Specification.

40.9.2 Insure that the contractor clearly understands the effect of, and the interactions between, the natural aerospace environment and HWCI design. In cases where the effect and interactions are not known or are ambiguous, insure that studies are in progress or planned to make these determinations.

40.9.3 Current and forecast natural aerospace environment parameters may be needed for certain configuration items; e.g., display of airbase conditions in a command and control system, calculation of impact point for a missile, etc. Insure

Downloaded from http://www.everyspec.com

compatibility between the configuration item design and appropriate meteorological communications by comparing characteristics of the source (teletype, facsimile, or data link) with that of the configuration item. Insure that arrangements or plans to obtain needed information have been made and that adequate display of natural environmental information shall be provided.

40.10 Equipment and Part Standardization

40.10.1 Equipment and Components:

a. Review current and planned contractor actions to determine that equipment or components for which standards or specifications exist shall be used whenever practical. (Standard item with NSN should have first preference).

b. Review specific trade-offs or modifications that may be required of existing designs if existing items are, or will be, incorporated in the HWCI.

c. Existing designs will be reviewed for use or non-use based on the potential impact on the overall program in the following areas:

(1) Performance

(2) Cost

(3) Time

(4) Weight

(5) Size

(6) Reliability

(7) Maintainability

(8) Supportability

(9) Producibility

d. Review HWCI design to identify areas where a practical design change would materially increase the number of standard items that could be incorporated.

e. Insure that Critical Item Specifications shall be prepared for hardware items identified as engineering or logistics critical.

Downloaded from http://www.everyspec.com

40.10.2 Parts Standardization and Interchangeability:

a. Review procedures to determine if maximum practical use will be made of parts built to approved standards or specifications. The potential impact on the overall program is to be evaluated when a part built to approved standards and specifications cannot be used for any of the following reasons:

(1) Performance

(2) Weight

(3) Size

(4) Reliability/Mantainability/Availability

(5) Supportability

(6) Survivability (including nuclear)

b. Identify potential design changes that will permit a greater use of standard or preferred parts and evaluate the trade-offs.

c. Insure understanding of parts control program operations for selection and approval of parts in new design or major modifications.

d. Review status of the Program Parts Selection List.

e. Review status of all non-standard parts identified.

f. Review pending parts control actions that may cause program slippages, such as non-availability of tested parts.

40.10.3 Assignment of Official Nomenclature:

a. Insure understanding of procedure for obtaining assignment of nomenclature and approval of nameplates.

b. Determine that a nomenclature conference has been held and agreement has been reached with the contracting agency on the level of nomenclature; i.e., system, set, central, group, component, sub-assembly, unit, etc.

40.11 Value Engineering

40.11.1 Review the Contractor's in-house incentive Value Engineering Program, which may include but not be limited to the following:

Downloaded from http://www.everyspec.com

a. Contractor's Value Engineering organization, policies and procedures.

b. Contractor's Value Engineering Training Program.

c. Potential Value Engineering projects, studies and VECPs.

d. Schedule of planned Value Engineering tasks/events.

e. Policies and procedures for subcontractor Value Engineering Programs.

40.12 Transportability

40.12.1 Review HWCI to determine if design meets contracts requirements governing size and weight to permit economical handling, loading, securing, transporting, and disassembly for shipment within existing capabilities of military and commercial carriers. Identify potential outsized and overweight items. Identify system/items defined as being hazardous. Ensure packaging afforded hazardous items complies with hazardous materials regulations.

40.12.2 Identify HWCIs requiring special temperature and humidity control or those possessing sensitive and shock susceptibility characteristics. Determine special transportation requirements and availability for use with these HWCIs.

40.12.3 Review Transportability Analysis to determine that transportation conditions have been evaluated and that these conditions are reflected in the design of protective, shipping, and handling devices. In addition to size and weight characteristics, determine that analysis includes provisions for temperature and humidity controls, minimization of sensitivity, susceptibility to shock, and transit damage.

40.13 Test

40.13.1 Review all changes to the System/Segment, HWCI Development, Software Requirements, and Interface Requirements Specifications subsequent to the established Allocated Baseline to determine whether Section 4.0 of all these specifications adequately reflects these changes.

40.13.2 Review information to be provided by the contractor regarding test concepts for Development Test and Evaluation (DT&E) testing (both informal and formal). Information shall include:

a. The organization and responsibilities of the group that will be responsible for test.

Downloaded from http://www.everyspec.com

b. The management of his in-house development test effort provides for:

(1) Test Methods (plans/procedures)

(2) Test Reports

(3) Resolution of problems and errors

(4) Retest procedure

(5) Change control and configuration management

(6) Identification of any special test tools that are not deliverable under the contract.

c. The methodology to be used to meet quality assurance requirements/qualification requirements, including the test repeatability characteristics and approach to regression testing.

d. The progress/status of the test effort since the previous reporting milestone.

40.13.3 Review status of all negative or provisional entries such as "not applicable (N/A)" or "to be determined (TBD)" in Section 4.0 of the System/Segment, hardware Development, Software Requirements or Interface Requirements Specifications. Review all positive entries for technical adequacy. Insure that associated test documentation includes these changes.

40.13.4 Review interface test requirements specified in Section 4.0 of the hardware Development, Software Requirements, and Interface Requirements Specifications for compatibility, currency, technical adequacy, elimination of redundant test. Insure that all associated test documents reflect these interface requirements.

40.13.5 Insure that all test planning documentation has been updated to include new test support requirements and provisions for long-lead time support requirements.

40.13.6 Review contractor test data from prior testing to determine if such data negates the need for additional testing.

40.13.7 Examine all available breadboards, mock-ups, or devices which will be used in implementing the test program or which affect the test program, for program impact.

40.13.8 Review plans for software Unit testing to ensure that they:

Downloaded from http://www.everyspec.com

a. Address Unit level sizing, timing, and accuracy requirements.

b. Present general and specific requirements that will be demonstrated by Unit testing.

c. Describe the required test-unique support software, hardware, and facilities and the interrelationship of these items.

d. Describe how, when, and from where the test-unique support items will be obtained.

e. Provide test schedules consistent with higher level plans.

40.13.9 Review plans for CSC integration testing to ensure that they:

a. Define the type of testing required for each level of the software structure above the unit level.

b. Present general and specific requirements that will be demonstrated by CSC integration testing.

c. Describe the required test-unique support software, hardware, and facilities and the interrelationship of these items.

d. Describe how, when, and from where the test-unique support items will be obtained.

e. Describe CSC integration test management, to include:

(1) Organization and responsibilities of the test team

(2) Control procedures to be applied during test

(3) Test reporting

(4) Review of CSC integration test results

(5) Generation of data to be used in CSC integration testing.

f. Provide test schedules consistent with higher level plans.

40.13.10 Review plans for formal CSCI testing to ensure that they:

a. Define the objective of each CSCI test, and relate the test to the software requirements being tested.

Downloaded from http://www.everyspec.com

b. Relate formal CSCI tests to other test phases.

c. Describe support software, hardware, and facilities required for CSCI testing; and how, when, and from where they will be obtained.

d. Describe CSCI test roles and responsibilities.

e. Describe requirements for Government-provided software, hardware, facilities, data, and documentation.

f. Provide CSCI test schedules consistent with higher-level plans.

g. Identify software requirements that will be verified by each formal CSCI test.

40.14 Maintenance and Maintenance Data (HWCIs)

40.14.1 Describe System Maintenance concept for impact on design and SE. Review adequacy of maintenance plans. Coverage shall be provided for On Equipment (Organizational), Off Equipment - On Site (Intermediate), Off Equipment - Off Site (Depot) level maintenance of Government Furnished Equipment (GFE), and Contractor Furnished Equipment (CFE). (See Section 3, Definitions, para 3.12 for levels of maintenance.)

40.14.2 Determine degree of understanding of the background, purpose, requirements, and usage of Maintenance (failure) Data Collection and Historical/Status Records. (Ref Data Item titled, "Reliability and Maintainability Data Reporting and Feedback Failure Summary Reports").

40.14.3 Describe method of providing Maintenance, Failure, Reliability, Maintainability Data to contracting agency.

40.14.4 Describe how requirements are submitted to the contracting agency for Equipment Classification (EQ/CL) Codes (formerly Work Order Number Prefix/Suffix Codes) when this requirement exists.

40.14.5 Review plans for (and status of) Work Unit Coding of the equipment. Work Unit codes shall be available for documenting Maintenance Data commencing with configuration item/Subsystem Testing. (Ref. Data Item titled "Technical Orders" and the military specification on work unit coding).

40.15 Spares and Government Furnished Property (GFP).

40.15.1 Review logistics and provisioning planning to insure full understanding of scope of requirements in these areas and that a reasonable time-phased plan has been developed for accomplishment. Of specific concern are the areas of: provisioning requirements,

Downloaded from http://www.everyspec.com

GFP usage, and spare parts, and support during installation, checkout, and test.

40.15.2 Review provisioning actions and identify existing or potential provisioning problems - logistic critical and long-lead time items are identified and evaluated against use of the interim release requirements.

40.15.3 Review plans for maximum screening and usage of GFP, and extent plans have been implemented.

40.15.4 Review progress toward determining and acquiring total installation, checkout, and test support requirements.

40.16 Packaging/SDPE (Special Design Protective Equipment)

40.16.1 Analyze all available specifications (System/Segment, HWCI Development, Software Requirements, Interface Requirements, and Critical Items) for packaging (Section 5) requirements for each product fabrication and material specification.

40.16.2 Evaluate user/operational support requirements and maintenance concepts for effect and influence on package design.

40.16.3 Establish that time phased plan for package design development is in consonance with the development of the equipment design.

40.16.4 Review planned and/or preliminary equipment designs for ease of packaging and simplicity of package design, and identify areas where a practical design change would materially decrease cost, weight, or volume of packaging required.

40.16.5 Review requirements for SDPE necessary to effectively support configuration item during transportation, handling and storage processes. Insure SDPE is categorized as a configuration item utilizing specifications conforming to the types and forms as prescribed in the contract. Review SDPE development/product specifications for adequacy of performance/interface requirements.

40.16.6 Determine initial package design baselines, concepts, parameters, constraints, etc., to the extent possible at this phase of the configuration item development process.

40.16.7 Insure previously developed and approved package design data for like or similar configuration items is being utilized.

40.16.8 Establish plans for trade studies to determine the most economical and desirable packaging design approach needed to satisfy the functional performance and logistic requirements.

Downloaded from http://www.everyspec.com

40.16.9 Verify the adequacy of the prototype package design.

40.16.10 Review Section 5 of Specification to insure full understanding by contractor for contractor requirements. Identify package specification used for hazardous materials.

40.17 Technical Manuals

40.17.1 Review status of the "Technical Manual Publications Plan" to insure that all aspects of the plan have been considered to the extent that all concerned agencies are apprised of the technical manual coverage to be obtained under this procurement. The suitability of available commercial manuals and/or modifications thereto shall also be determined.

40.17.2 Review the availability of technical manuals for validation/verification during the latter phases of DT&E testing.

40.17.3 If a Guidance Conference was not accomplished or if open items resulted from it, then review as applicable provisions for accomplishing TO in-process reviews, validation, verification, prepublication, and postpublication reviews.

40.18 System Allocation Document

40.18.1 Review the Draft System Allocation Document for completeness and technical adequacy to extent completed.

40.18.2 The format shall provide the following minimum information:

a. Drawing Number
b. Issue
c. Number of Sheets
d. Location
e. Configuration Item Number
f. Title
g. Part Number
h. Serial Number
i. Specification Number
j. Equipment Nomenclature
k. Configuration Item Quantity
l. Assembly Drawing

40.19 Design Producibility and Manufacturing

40.19.1 The contractor shall demonstrate and present evidence that manufacturing engineering will be integrated into the design process.

Downloaded from http://www.everyspec.com

a. The contractor shall provide evidence of performing producibility analyses on development hardware trading off design requirements against manufacturing risk, cost, production, volume, and existing capability/availability.

Evidence of such analyses may be in the contractor's own format but must conclusively demonstrate that in-depth analyses were performed by qualified organizations/individuals and the results of those analyses will be incorporated in the design.

b. Preliminary manufacturing engineering and production planning demonstrations shall address: material and component selection, preliminary production sequencing, methods and flow concepts, new processes, manufacturing risk, equipment and facility utilization for intended rates and volume, production in-process and acceptance test and inspection concepts. (Efforts to maximize productivity in the above areas should be demonstrated.)

c. Management systems to be utilized will insure that producibility and manufacturing considerations are integrated throughout the FSD effort.

40.19.2 The producibility and manufacturing concerns identified in the SRR and the SDR shall be updated and expanded to:

a. Provide evidence that concerns identified in the Manufacturing Feasibility Assessment and the Production Capability Estimate have been addressed and that resolutions are planned or have been performed.

b. Make recommendations including manufacturing technology efforts and provide a schedule of necessary actions to the program office to resolve open manufacturing concerns and reduce manufacturing risk.

40.20 Post Review Action

40.20.1 After completing the PDR, the contractor shall publish and distribute copies of Review minutes. The contracting agency officially acknowledges completion of a PDR as indicated in paragraph 4.2.4.

40.20.2 The accomplishment of the PDR shall be recorded on the configuration item Development Record by the contractor.

Downloaded from http://www.everyspec.com

50. Critical Design Review

50.1 General. The CDR shall be conducted on each configuration item prior to fabrication/production/coding release to insure that the detail design solutions, as reflected in the Draft Hardware Product Specification, Software Detailed Design Document (SDDD), Data Base Design Document(s) (DBDD(s)), Interface Design Document(s) (IDD(s)), and engineering drawings satisfy requirements established by the hardware Development Specification and Software Top Level Design Document (STLDD). CDR shall be held after the Computer Software Operator's Manual (CSOM), Software User's Manual (SUM), Computer System Diagnostic Manual (CSDM), Software Programmer's Manual (SPM), and Firmware Support Manual (FSM) have been updated or newly released. For complex/large configuration items the CDR may be conducted on an incremental basis, i.e., progressive reviews are conducted versus a single CDR. The overall technical program risks associated with each configuration item shall also be reviewed on a technical (design and manufacturing), cost and schedule basis. For software, a technical understanding shall be reached on the validity and the degree of completeness of the SDDD, IDD(s), DBDD(s), STD, CRISD, SPM, and FSM, and preliminary versions of the CSOM, SUM, and CSDM.

50.1.1 Equipment/Facilities configuration items. The detail design as disclosed by the hardware Product Specification, dravings, schematics, mockups, etc., shall be reviewed against the HWCI Development Specification performance requirements. For other than facilities, the result of a successful CDR shall be the establishment of the design baseline for detailed fabrication/production planning i.e., the contractor is permitted to use the detail design as presented at CDR and reflected in the hardware Product Specification for planning for production and, if specifically authorized, for initial fabrication/production efforts.

50.1.2 Computer Software configuration items (CSCIs). The CDR for a CSCI shall be a formal technical review of the CSCI detail design, including data base and interfaces. The CDR is normally accomplished for the purpose of establishing integrity of computer software design at the level of a Unit's logical design prior to coding and testing. CDR may be accomplished at a single review meeting or in increments during the development process corresponding to periods at which components or groups of components reach the completion of logical design. The primary product of the CDR is a formal identification of specific software documentation which will be released for coding and testing. By mutual agreement between the contractor and the contracting agency, CDRs may be scheduled concurrently for two or more CSCIs.

50.1.2.1 Since computer software development is an iterative process, the completion of a CDR for a CSCI is not necessarily sufficient for maintaining adequate visibility into the remaining

Downloaded from http://www.everyspec.com

development effort through testing.

50.1.2.2 Additional In-Progress Reviews may be scheduled post-CDR which address:

a. Response to outstanding action items

b. Modifications to design necessitated by approved ECPs or design/program errors

c. Updating sizing and timing data

d. Updated design information, as applicable

e. Results obtained during in-house testing, including problems encountered and solutions implemented or proposed.

50.2 Items to be Reviewed. The contractor shall present the following for review by the contracting agency:

50.2.1 HWCIs

a. Adequacy of the detail design reflected in the draft hardware Product Specification in satisfying the requirements of the HWCI Development Specification for the item being reviewed.

b. Detail engineering drawings for the HWCI including schematic diagrams.

c. Adequacy of the detailed design in the following areas:

(1) Electrical design

(2) Mechanical design

(3) Environmental control and thermal aspects

(4) Electromagnetic compatibility

(5) Power generation and grounding

(6) Electrical and mechanical interface compatibility

(7) Mass properties

(8) Reliability/Maintainability/Availability

(9) System Safety Engineering

(10) Security Engineering

Downloaded from http://www.everyspec.com

(11) Survivability/Vulnerability (including nuclear)

(12) Producibility and Manufacturing

(13) Transportability, Packaging and handling

(14) Human Engineering and Biomedical Requirements (including Life Support and Crew Station Requirements)

(15) Standardization

(16) Design versus Logistics Trade-offs

d. Interface control drawings

e. Mock-ups, breadboards, and/or prototype hardware

f. Design analysis and test data

g. System Allocation Document for HWCI inclusion at each scheduled location.

h. Initial Manufacturing Readiness (for example, manufacturing engineering, tooling demonstrations, development and proofing of new materials, processes, methods, tooling, test equipment, procedures, reduction of manufacturing risks to acceptable levels).

i. Preliminary VECPs and/or formal VECPs

j. Life cycle costs

k. Detail design information on all firmware to be provided with the system.

l. Verify corrosion prevention/control considerations to insure materials have been chosen that will be compatible with operating environment.

m. Findings/Status of Quality Assurance Program

50.2.2 CSCIs.

a. Software Detailed Design, Data Base Design, and Interface Design Document(s). In cases where the CDR is conducted in increments, complete documents to support that increment shall be available.

b. Supporting documentation describing results of analyses, testing, etc., as mutually agreed by the contracting agency and the contractor.

Downloaded from http://www.everyspec.com

c. System Allocation Document for CSCI inclusion at each scheduled location.

d. Computer Resources Integrated Support Document.

e. Software Programmer's Manual

f. Firmware Support Manual

g. Progress on activities required by CSCI PDR (para 40.2.2).

h. Updated operation and support documents (CSOM, SUM, CSDM).

i. Schedules for remaining milestones.

j. Updates since the last review to all previously delivered software related CDRL items.

50.2.3 Support Equipment (SE):

a. Review requirements (paragraphs 50.2.1 and 50.2.2) for SE.

b. Verify maximum considerations GFE SE

c. Identify existing or potential SE provisioning problems

d. Determine qualitative and quantitative adequacy of provisioning drawings and data

e. Review reliability of SE

f. Review logistic support requirements for SE items

g. Review calibration requirements

h. Review documentation for SE.

50.3 Detailed Evaluation of Electrical, Mechanical, and Logical Designs.

50.3.1 HWCIs. Detailed block diagrams, schematics, and logic diagrams shall be compared with interface control drawings to determine system compatibility. Analytical and available test data shall be reviewed to insure the hardware Development Specification has been satisfied.

50.3.1.1 The contractor shall provide information on firmware which is included in commercially available equipment or to be included in equipment developed under the contract. Firmware in this context includes the microprocessor and associated sequence of micro-instructions necessary to perform the allocated tasks. As a minimum, the information presented during CDR shall provide

Downloaded from http://www.everyspec.com

descriptions and status for the following:

a. Detailed logic flow diagrams

b. Processing algorithms

c. Circuit diagrams

d. Clock and timing data (e.g., timing charts for micro-instructions)

e. Memory (e.g., type (RAM, PROM), word length, size (total and spare capacity))

f. Micro-instruction list and format

g. Device functional instruction set obtained by implementation of firmware.

h. Input/output data width (i.e., number of bits for data and control.)

i. Self-test (diagnostics) within firmware.

j. Support software for firmware development:

(1) Resident assembler

(2) Loader

(3) Debugging routines

(4) Executive (monitor)

(5) Non-resident diagnostics

(6) Cross assembler and higher level language on host computer

(7) Instruction simulator

50.3.2 CSCIs. The contractor shall present the detailed design (including rationale) of the CSCI to include:

a. The assignment of CSCI requirements to specific Lower-Level Computer Software Components (LLCSCs) and Units, the criteria and design rules used to accomplish this assignment, and the traceability of Unit and LLCSC designs to satisfy CSCI requirements, with emphasis on the necessity and sufficiency of the Units for implementing TLCSC design requirements.

Downloaded from http://www.everyspec.com

b. The overall information flow between software Units, the method(s) by which each Unit gains control, and the sequencing of Units relative to each other.

c. The design details of the CSCI, TLCSCs, LLCSCs, and Units including data definitions, timing and sizing, data and storage requirements and allocations.

d. The detailed design characteristics of all interfaces, including their data source, destination, interface name and interrelationships; and, if applicable, the design for direct memory access. The contractor shall also give an overview of the key design issues of the interface software design, and indicate whether data flow formats are fixed or subject to extensive dynamic changes.

e. The detailed characteristics of the data base. Data base structure and detailed design, including all files, records, fields, and items. Access rules, how file sharing will be controlled, procedures for data base recovery/regeneration from a system failure, rules for data base manipulation, rules for maintaining file integrity, rules for usage reporting, and rules governing the types and depth of access shall be defined. Data management rules and algorithms for implementing them shall be described. Details of the language required by the user to access the data base shall also be described.

50.4 Electromagnetic Compatibility:

a. Review contractor EMC design of all HWCIs. Determine compliance with requirements of the Electromagnetic Compatibility Plan and HWCI specifications.

b. Review system EMC including effects on the electromagnetic environment (inter-system EMC) and intra-system EMC. Determine acceptability of EMC design and progress toward meeting contractual EMC requirements.

c. Review EMC test plans. Determine adequacy to confirm EMC design characteristics of the system/HWCI/subsystem.

50.5 Design Reliability:

50.5.1 Review the most recent predictions of hardware and software reliability and compare against requirements specified in hardware Development Specification and Software Requirements Specification. For hardware, predictions are substantiated by review of parts application stress data.

50.5.2 Review applications of parts or configuration items with minimum life, or those which require special consideration to

Downloaded from http://www.everyspec.com

insure their effect on system performance is minimized.

50.5.3 Review completed Reliability Design Review Checklist to insure principles have been satisfactorily reflected in the configuration item design.

50.5.4 Review applications of redundant configuration item elements or components to establish that expectations have materialized since the PDR.

50.5.5 Review detailed HWCI reliability demonstration plan for compatibility with specified test requirements. The number of test articles, schedules, locations, test conditions, and personnel involved are reviewed to insure a mutual understanding of the plan and to provide overall planning information to activities concerned.

50.5.6 Review the failure data reporting procedures and methods for determination of failure trends.

50.5.7 Review the thermal analysis of components, printed circuit cards, modules, etc. Determine if these data are used in performing the detailed reliability stress predictions.

50.5.8 Review on-line diagnostic programs, off-line diagnostic programs, support equipment, and preliminary technical orders (and/or commercial manuals) for compliance with the system maintenance concept and specification requirements.

50.5.9 Review software reliability prediction model and its updates based upon test data and refined predictions of component usage rates and complexity factors.

50.6 Design Maintainability

50.6.1 Review the most recent predictions of quantitative maintainability and compare these against requirements specified in the HWCI Development Specification and Software Requirements Specification.

50.6.2 Review preventive maintenance frequencies and durations for compatibility with overall system requirements and planning criteria.

50.6.3 Identify unique maintenance procedures required for the configuration item during operational use and evaluate their total effects on system maintenance concepts. Assure that system is optimized from a maintenance and maintainability viewpoint and conforms with the planned maintenance concept. This shall include a review of provisions for automatic, semi-automatic, and manual recovery from hardware/software failures and malfunctions.

Downloaded from http://www.everyspec.com

50.6.4 Identify design-for-maintainability criteria provided by the checklist in the design detail to insure that criteria have, in fact been incorporated.

50.6.5 Determine if parts, assemblies, and other items are so placed that there is sufficient space to use test probes, soldering irons, and other tools without difficulty and that they are placed so that structural members of units do not prevent access to them or their ease of removal.

50.6.6 Review detailed maintainability demonstration plan for compatibility with specified test requirements. Supplemental information is provided and reviewed to insure a mutual understanding of the plan and to provide overall planning information to activities concerned.

50.7 Human Factors

50.7.1 Review detail design presented on drawings, schematics, mockups, or actual hardware to determine that it meets human performance requirements of the HWCI Development Specification and Software Requirements Specification, Interface Requirements Specification(s), and accepted human engineering practices.

50.7.2 Demonstrate by checklist or other formal means the adequacy of design for human performance.

50.7.3 Review each facet of design for man/machine compatibility. Review time/cost/effectiveness considerations and forced trade-offs of human engineering design.

50.7.4 Evaluate the following human engineering/biomedical design factors:

a. Operator controls

b. Operator displays

c. Maintenance features

d. Anthropometry

e. Safety features and emergency equipment

f. Work space layout

g. Internal environmental conditions (noise, lighting, ventilation, etc.)

h. Training equipment

i. Personnel accommodations

Downloaded from http://www.everyspec.com

50.8 System Safety

50.8.1 Review configuration item detail design for compliance to safety design requirements.

50.8.2 Review acceptance test requirements to insure adequate safety requirements are reflected therein.

50.8.3 Evaluate adequacy of detailed design for safety and protective equipment/devices.

50.8.4 Review configuration item operational maintenance safety analyses and procedures.

50.9 Natural Environment

50.9.1 Review detail design to determine that it meets natural environment requirements of the hardware Development Specification.

50.9.2 Insure that studies have been accomplished concerning effects of the natural environment on, or interactions with, the HWCI. Studies which have been in progress shall be complete at this time.

50.9.3 Determine whether arrangements have been made to obtain current and/or forecast natural environment information, when needed for certain HWCIs. Assure compatibility of HWCI and source of information by comparing electrical characteristics and formats for the source and the HWCI.

50.10 Equipment and Parts Standardization.

50.10.1 Equipment and Components. Determine that every reasonable action has been taken to fulfill the standardization requirements for use of standard items (standard item with NSN should be first preference) and to obtain approval for use of non-standard or non-preferred items. Accordingly, the following criteria shall be evaluated:

a. Data sources that were reviewed.

b. Factors that were considered in the decision to reject known similar, existing designs.

c. Factors that were considered in decisions to accept any existing designs which were incorporated, and the trade-offs, if any, that had to be made.

50.10.2 Parts

a. Determine whether there are any outstanding non-standard or

Downloaded from http://www.everyspec.com

non-preferred parts approval requests and action necessary for approval or disapproval. (Status of parts control program operations).

b. Identify non-standard-non-preferred parts approval problems and status of actions toward resolving the problems.

c. Review potential fabrication/production line delays due to non-availability of standard or preferred parts. In such cases, determine whether it is planned to request use of parts which may be replaced by standard items during subsequent support repair cycles. Assure that appropriate documentation makes note of these items and that standard replacement items shall be provisioned for support and used for repair.

d. Require certification that maximum practical interchangeability of parts exists among components, assemblies, and HWCIs. Reservations concerning interchangeability are identified, particularly for hardness critical items.

e. Sample preliminary drawings and cross check to insure that parts indicated on the drawings are compatible with the Program Parts Selection List.

50.10.3 Assignment of Official Nomenclature.

a. Determine whether official nomenclature and approval of nameplates have been obtained to extent practical.

b. Determine whether DD Form 61, Request for Nomenclature, has been processed to the agreed level of indenture.

c. Insure that approved nomenclature has been reflected in the Development and Product Specifications.

d. Identify problems associated with nomenclature requests (DD-61s) together with status of actions towards resolving the problems.

e. Insure that a software inventory numbering system has been agreed to and implemented to the CSCI level.

50.11 Value Engineering (VE)

50.11.1 Review status of all VECPs presented per the terms of the contract.

50.11.2 Review any new areas of potential Value Engineering considered profitable to challenge.

Downloaded from http://www.everyspec.com

50.11.3 If required by contract (funded VE program), review the actual Value Engineering accomplishments against the planned VE program.

50.12 Transportability

50.12.1 Review transportability evaluations accomplished for those items identified as outsized, overweight, sensitive, and/or requiring special temperature and humidity controls.

50.12.2 Review actions taken as a result of the above evaluation to insure adequate facilities and military or commercial transporting equipment are available to support system requirements during Production and Deployment Phases.

50.12.3 Review design of special materials handling equipment, when required, and action taken to acquire equipment.

50.12.4 Insure DOD Certificates of Essentiality for movement of equipment have been obtained for equipment exceeding limitations of criteria established in contract requirements.

50.12.5 Insure transportability approval has been annotated on design documents and shall remain as long as no design changes are made that modify significant transportability parameters.

50.12.6 Identify equipment to be test loaded for air transportability of material in Military Aircraft.

50.13 Test

50.13.1 Review updating changes to all specifications subsequent to the PDR, to determine whether Section 4.0 of the specifications adequately reflects these changes.

50.13.2 Review all available test documentation for currency, technical adequacy, and compatibility with Section 4.0 of all Specification requirements.

50.13.3 For any development model, prototype, etc., on which testing may have been performed, examine test results for design compliance with hardware Development, Software Requirements, and Interface Requirements Specification requirements.

50.13.4 Review quality assurance provisions/qualification requirements in HWCI Product, Software Requirements, or Interface Requirements Specifications for completeness and technical adequacy. Section 4.0 of these specifications shall include the minimum requirements that the item, materiel, or process must meet to be acceptable.

50.13.5 Review all test documentation required to support test

Downloaded from http://www.everyspec.com

requirements of Section 4.0 of HWCI Product Specifications for compatibility, technical adequacy, and completeness.

50.13.6 Inspect any breadboards, mockups, or prototype hardware available for test program implications.

50.13.7 Review Software Test Descriptions to ensure they are consistent with the Software Test Plan and they thoroughly identify necessary parameters and prerequisites to enable execution of each planned software test and monitoring of test results. As a minimum, test descriptions shall identify the following for each test:

a. Required preset hardware and software conditions and the necessary input data, including the source for all data.

b. Criteria for evaluating test results.

c. Prerequisite conditions to be established or set prior to test execution.

d. Expected or predicted test results.

50.14 Maintenance and Maintenance Data

50.14.1 Review adequacy of maintenance plans.

50.14.2 Review status of unresolved maintenance and maintenance data problems since the PDR.

50.14.3 Review status of compliance with Data Item titled "Reliability, Maintainability Data Reporting and Feedback Failure Summary Reports."

50.15 Spare Parts and Government Furnished Property (GFP).

50.15.1 Review provisioning planning through normal logistics channels and Administrative Contracting Officer (ACO) representative (Industrial Specialist) to insure its compatibility (content and time phasing) with contractual requirements (data and SOW items). The end objective is to provision by a method which shall insure system supportability at operational date of the first site. Also accomplish the following:

a. Insure contractor understanding of contractual requirements, including time phasing, instructions from logistics support agencies, interim release authority and procedure, and responsibility to deliver spare/repair parts by need date.

b. Determine that scheduled provisioning actions, such as, guidance meetings, interim release and screening, are being accomplished adequately and on time.

Downloaded from http://www.everyspec.com

c. Identify existing or potential provisioning problems.

50.15.2 Determine quantitative and qualitative adequacy of provisioning drawings and data. Verify that Logistics Critical items are listed for consideration and that adequate procedures exist for reflecting design change information in provisioning documentation and Technical Orders.

50.15.3 Insure support requirements have been determined for installation, checkout, and test for approval by contracting agency. Insure screening has been accomplished and results are included into support requirements lists.

50.15.4 Determine that adequate storage space requirements have been programmed for on-site handling of Installation and Checkout (I&C), test support material, and a scheme has been developed for "down streaming" and joint use of insurance (high cost) or catastrophic failure support items.

50.15.5 Assure that Acquisition Method Coding (AMC) is considered.

50.16 Packaging/SDPE

50.16.1 Review proposed package design to insure that adequate protection to the HWCI, and the media on which the CSCI is recorded, is provided against natural and induced environments/hazards to which the equipment will be subjected throughout its life cycle, and to insure compliance with contractual requirements. Such analysis shall include, but not be limited to, the following:

a. Methods of preservation

b. Physical/mechanical/shock protection including cushioning media, shock mounting and isolation features, load factors, support pads, cushioning devices, blocking and bracing, etc.

c. Mounting facilities and securing/hold-down provisions

d. Interior and exterior container designs.

e. Handling provisions and compatibility with aircraft materials handling system (463L)

f. Container marking.

g. Consideration and identification of dangerous/hazardous commodities

50.16.2 Review design of SDPE HWCI to determine if a category I container is required. The analysis of the proposed container or handling, shipping equivalent shall encompass as a minimum:

Downloaded from http://www.everyspec.com

a. Location and type of internal mounting or attaching provisions

b. Vibration - shock isolation features, based on the pre-determined fragility rating (or other constraint of the item to be shipped.)

c. Service items (indicators, relief valves, etc.)

d. Environmental control features

e. External handling, stacking and tie-down provisions with stress ratings

f. Dimensional and weight data (gross and net)

g. Bill-of-material

h. Marking provisions including the center-of-gravity location

i. For wheeled SDPE (self-powered or tractor/trailer) the overall length, width, and height with mounted item, turning radius, mobility, number of axles, unit contact load, number of tires, etc.

j. Position and travel of adjustable wheels, titling, or other adjustments to facilitate loading.

50.16.3 Review the results of trade studies, engineering analyses, etc., to substantiate selected package/SDPE design approach, choice of materials, handling provisions, environmental features, etc.

50.16.4 Insure that package/SDPE design provides reasonable balance between cost and desired performance.

50.16.5 Review all preproduction test results of the prototype package design to insure that the HWCI is afforded the proper degree of protection.

50.16.6 Review Section 5, Packaging, of the HWCI Product Specification for correct format, accuracy and technical adequacy.

50.16.7 Review contractor procedures to assure that the requirements of Section 5, Preparation for Delivery of the approved HWCI Product Specification, will be incorporated into the package design data for provisioned spares.

50.17 System Allocation Document

50.17.1 Review maintenance of the System Allocation Document since PDR.

Downloaded from http://www.everyspec.com

50.17.2 Insure plans are initiated for configuration item re-allocations that may be necessary due to actions occurring prior to, or during, CDR.

50.18 Design Producibility and Manufacturing

50.18.1 Review the status of all producibility (and productivity) efforts for cost and schedule considerations.

50.18.2 Review the status of efforts to resolve manufacturing concerns identified in previous technical reviews and their cost and schedule impact to the production program.

50.18.3 Review the status of Manufacturing Technology programs and other previously recommended actions to reduce cost, manufacturing risk and industrial base concerns.

50.18.4 Identify open manufacturing concerns that require additional direction/effort to minimize risk to the production program.

50.18.5 Review the status of manufacturing engineering efforts, tooling and test equipment demonstrations, proofing of new materials, processes, methods, and special tooling/test equipment.

50.18.6 Review the intended manufacturing management system and organization for the production program in order to show how their efforts will effect a smooth transition into production.

50.19 Post Review Action

50.19.1 After completing the CDR, the contractor shall publish and distribute copies of Review minutes. The contracting agency officially acknowledges completion of a CDR as indicated in paragraph 4.2.4.

50.19.2 The accomplishment of the CDR shall be recorded on the configuration item Development Record by the contractor.

Downloaded from http://www.everyspec.com

60. Test Readiness Review (TRR).

60.1 General. The TRR shall be a formal review of the contractor's readiness to begin formal CSCI testing. It is conducted after software test procedures are available and CSC integration testing is complete. The purpose of TRR is for the contracting agency to determine whether the contractor is in fact ready to begin CSCI testing. A technical understanding shall be reached on the informal test results, and on the validity and the degree of completeness of the Computer System Operator's Manual (CSOM), Software User's Manual (SUM), and Computer System Diagnostic Manual (CSDM).

60.2 Items to be reviewed. The contractor shall present the following for review:

60.2.1 Requirements changes. Any changes to the Software Requirements Specification or Interface Requirements Specification(s) that have been approved since SSR, and which impact CSCI testing.

60.2.2 Design changes. Any changes to the Software Top-Level Design Document, Software Detailed Design Document, Data Base Design Document(s), or Interface Design Document(s) that have been made since PDR and CDR, and which impact CSCI testing.

60.2.3 Software test plans and descriptions. Any changes to approved Software Test Plans and Software Test Descriptions.

60.2.4 Software test procedures. Test procedures to be used in conducting CSCI testing, including retest procedures for test anomalies and corrections.

60.2.5 CSC integration test cases, procedures, and results. CSC integration test cases and procedures used in conducting informal CSC integration tests and the test results.

60.2.6 Software test resources. Status of the development facility hardware, Government Furnished Software (GFS), test personnel, and supporting test software and materials, including software test tool qualification and review of the traceability between requirements and their associated tests.

60.2.7 Test limitations. Identification of all software test limitations.

60.2.8 Software problems. Summary of software problem status including all known discrepancies of the CSCI and test support software.

60.2.9 Schedules. Schedules for remaining milestones.

Downloaded from http://www.everyspec.com

60.2.10 Documentation Updates. Updates to all evolving and previously delivered CDRL items (e.g., CSOM, SUM, CSDM).

60.3 Post Review Action.

60.3.1 After completing the TRR, the contractor shall publish and distribute copies of Review Minutes. The contracting agency officially acknowledges completion of a TRR as indicated in paragraph 4.2.4.

60.3.2 The accomplishment of the TRR shall be recorded on the configuration item Development Record by the contractor.

Downloaded from http://www.everyspec.com

70. Functional Configuration Audit.

70.1 General. The objective of the Functional Configuration Audit (FCA) shall be to verify that the configuration item's actual performance complies with its Hardware Development or Software Requirements and Interface Requirements Specifications. Test data shall be reviewed to verify that the hardware or computer software performs as required by its functional/allocated configuration identification. For configuration items developed at Government expense, an FCA shall be a prerequisite to acceptance of the configuration item. For software, a technical understanding shall be reached on the validity and the degree of completeness of the Software Test Reports, and as appropriate, Computer System Operator's Manual (CSOM), Software User's Manual (SUM), and Computer System Diagnostic Manual (CSDM).

70.1.1 The FCA for a complex configuration item may be conducted on a progressive basis, when so specified by the contracting agency, throughout the configuration item's development and culminates at the completion of the qualification testing of the configuration item with a review of all discrepancies at the final FCA. The FCA shall be conducted on that configuration of the configuration item which is representative (prototype or preproduction) of the configuration to be released for production of the operational inventory quantities. When a prototype or preproduction article is not produced, the FCA shall be conducted on a first production article. For cases where configuration item qualification can only be determined through integrated system testing, FCA's for such configuration items will not be considered complete until completion of such integrated testing.

70.1.2 Recommendations of configuration item acceptance or non-acceptance to the local contract management agency are based upon and governed by procedures and requirements outlined in subsequent paragraphs.

70.2 Contract Requirements

70.2.1 The schedules for the FCA shall be recorded on the configuration item development record by the contractor. A configuration item cannot be audited without the contracting agency authentication of the functional and allocated baseline. In addition, the contractor shall submit the final draft Product Specification for the configuration item to be audited to the contracting agency for review prior to FCA.

70.3 Contractor Responsibility

70.3.1 Prior to the FCA date (for configuration items to be audited), the contractor shall provide the following information to the contracting agency (this information shall be provided in addition to the general requirements of Section 4.):

Downloaded from http://www.everyspec.com

a. Contractor representation (the test manager should be in attendance).

b. Identification of items to be audited:

(1) Nomenclature

(2) Specification identification number

(3) Configuration Item number

(4) Current listing of all deviations/waivers against the configuration item, either requested of, or approved by the contracting agency.

(5) Status of Test Programs to test configured items with automatic test equipment (when applicable).

70.4 Procedures and Requirements

70.4.1 The contractor's test procedures and results shall be reviewed for compliance with specification requirements.

70.4.2 The following testing information shall be available for the FCA team.

a. Test plans, specifications, descriptions, procedures, and reports for the configuration item.

b. A complete list of successfully accomplished functional tests during which pre-acceptance data was recorded.

c. A complete list of successful functional tests if detailed test data are not recorded.

d. A complete list of functional tests required by the specification but not yet performed. (To be performed as a system or subsystem test).

e. Preproduction and production test results

70.4.3 Testing accomplished with the approved test procedures and validated data (witnessed) shall be sufficient to insure configuration item performance as set forth in the specification Section 3 and meet the quality assurance provisions/qualification requirements contained in the specification Section 4.

70.4.4 For those performance parameters which cannot completely be verified during testing, adequate analysis or simulations shall have been accomplished. The results of the analysis or simulations will be sufficient to insure configuration item performance as outlined in the specification.

Downloaded from http://www.everyspec.com

70.4.5 Test reports, procedures, and data used by the FCA team shall be made a matter of record in the FCA minutes.

70.4.6 A list of the contractor's internal documentation (drawings) of the configuration item shall be revieved to insure that the contractor has documented the physical configuration of the configuration item for which the test data are verified.

70.4.7 Drawings of HWCI parts which are to be provisioned should be selectively sampled to assure that test data essential to manufacturing are included on, or furnished with, the drawings.

70.4.8 Configuration items which fail to pass quality assurance test provisions/qualification requirements are to be analyzed as to the cause of failure to pass. Appropriate corrections shall be made before a configuration item is subjected to a requalification.

70.4.9 A checklist shall be developed which identifies documentation and hardware and computer software to be available and tasks to be accomplished at the FCA for the configuration item. See Pre-FCA checksheet.

70.4.10 Retests or additional tests shall be performed to assure compliance with paragraph 70.4.3.

70.4.11 Acknowledge accomplishment of partial completion of the FCA for those configuration items whose qualification is contingent upon completion of integrated systems testing.

70.4.12 For CSCIs the following additional requirements shall apply:

a. The contractor shall provide the FCA team with a briefing for each CSCI being audited and shall delineate the test results and findings for each CSCI. As a minimum, the discussion shall include CSCI requirements that were not met, including a proposed solution to each item, an account of the ECPs incorporated and tested as well as proposed, and a general presentation of the entire CSCI test effort delineating problem areas as well as accomplishments.

b. An audit of the formal test plans/descriptions/procedures shall be made and compared against the official test data. The results shall be checked for completeness and accuracy. Deficiencies shall be documented and made a part of the FCA minutes. Completion dates for all discrepancies shall be clearly established and documented.

c. An audit of the Software Test Reports shall be performed to validate that the reports are accurate and completely describe the CSCI tests.

Downloaded from http://www.everyspec.com

d. All ECPs that have been approved shall be revieved to ensure that they have been technically incorporated and verified.

e. All updates to previously delivered documents shall be revieved to ensure accuracy and consistency throughout the documentation set.

f. Preliminary and Critical Design Review minutes shall be examined to ensure that all findings have been incorporated and completed.

g. The interface requirements and the testing of these requirements shall be reviewed for CSCIs.

h. Review data base characteristics, storage allocation data and timing, and sequencing characteristics for compliance with specified requirements.

70.5 Post Audit Actions

70.5.1 After completion of the FCA, the contractor shall publish and distribute copies of FCA minutes. The contracting agency officially acknowledges completion of the FCA as indicated in paragraph 4.2.4.

70.5.2 The accomplishment of the FCA shall be recorded on the configuration item Development Record by the contractor.

Downloaded from http://www.everyspec.com

80. Physical Configuration Audit (PCA)

80.1 General. The Physical Configuration Audit (PCA) shall be the formal examination of the as-built version of a configuration item against its design documentation in order to establish the product baseline. After successful completion of the audit, all subsequent changes are processed by engineering change action. The PCA also determines that the acceptance testing requirements prescribed by the documentation is adequate for acceptance of production units of a configuration item by quality assurance activities. The PCA includes a detailed audit of engineering drawings, specifications, technical data and tests utilized in production of HWCIs and a detailed audit of design documentation, listings, and manuals for CSCIs. The review shall include an audit of the released engineering documentation and quality control records to make sure the as-built or as-coded configuration is reflected by this documentation. For software, the Software Product Specification and Version Description Document shall be a part of the PCA review.

80.1.1 The PCA shall be conducted on the first article of configuration items and those that are a reprocurement of a configuration item already in the inventory shall be identified and selected jointly by the contracting agency and the contractor. A PCA shall be conducted on the first configuration item to be delivered by a new contractor even though PCA was previously accomplished on the first article delivered by a different contractor.

80.1.2 Formal approval by the contracting agency of the configuration item Product specification, and the satisfactory completion of a PCA results in establishment of the product baseline.

80.1.3 Recommendations of configuration item acceptance or nonacceptance to the responsible contract adminstration office (CAO) are based upon and governed by procedures and requirements outlined in subsequent paragraphs.

80.1.4 A final review shall be made of all operation and support documents (i.e., Computer System Operator's Manual (CSOM), Software User's Manual (SUM), Computer System Diagnostic Manual (CSDM), Software Programmer's Manual (SPM), Firmware Support Manual (FSM)) to check format, completeness, and conformance with applicable data item descriptions.

80.2 Contract Requirements

80.2.1 The schedules for the PCA shall be recorded on the configuration item Development Record by the contractor. A current set of listings shall be provided for each CSCI being audited. The contractor shall submit the final draft of the

Downloaded from http://www.everyspec.com

product specification for the configuration item to be audited to the contracting agency for review prior to PCA.

80.3 Contractor Responsibility

80.3.1 The contractor shall provide the following information to the contracting agency (this information shall be provided in accordance with the general instructions of Section 4 and the contractual requirements):

a. Contractor representation (the test manager should be in attendance).

b. Identification of items to be accepted by:

(1) Nomenclature

(2) Specification Identification Number

(3) Configuration item Identifiers

(4) Serial Numbers

(5) Drawing and Part Numbers

(6) Identification Numbers

(7) Code Identification Numbers

(8) Software inventory numbering system

c. A list delineating all deviations/waivers against the configuration item either requested or contracting agency approved.

80.3.2 The PCA cannot be performed unless data pertinent to the configuration item being audited is provided to the PCA team at time of the audit. The contractor shall compile and make this information available for ready reference. Required information shall include:

a. Configuration item product specification.

b. A list delineating both approved and outstanding changes against the configuration item.

c. Complete shortage list.

d. Acceptance test procedures and associated test data.

e. Engineering drawing index including revision letters.

Downloaded from http://www.everyspec.com

f. Operating, maintenance, and illustrated parts breakdown manuals.

g. Proposed DD Form 250, "Material Inspection and Receiving Report".

h. Approved nomenclature and nameplates.

i. Software Programmer's Manuals (SPMs), Software User's Manuals (SUMs) Computer System Operator's Manual (CSOM), Computer System Diagnostic Manual (CSDM), and Firmware Support Manual (FSM).

j. Software Version Description Document.

k. FCA minutes for each configuration item.

l. Findings/Status of Quality Assurance Programs.

80.3.3 The contractor shall assemble and make available to the PCA team at time of audit all data describing the item configuration. Item configuration data shall include:

a. Current approved issue of hardware development specification, Software Requirements Specification, and Interface Requirements Specification(s) to include approved specification change notices and approved deviations/waivers.

b. Identification of all changes actually made during test.

c. Identification of all required changes not completed.

d. All approved drawings and documents by the top drawing number as identified in the configuration item product specification. All drawings shall be of the category and form specified in the contract.

e. Manufacturing instruction sheets for HWCIs identified by the contracting agency.

80.3.4 The contractor shall identify any difference between the physical configurations of the selected production unit and the Development Unit(s) used for the FCA and shall certify or demonstrate to the Government that these differences do not degrade the functional characteristics of the selected units.

80.4 PCA Procedures and Requirements

80.4.1 Drawing and Manufacturing Instruction Sheet Review Instructions:

Downloaded from http://www.everyspec.com

a. A representative number of drawings and associated manufacturing instruction sheets for each item of hardware, identified by the contracting agency Co-Chairperson, shall be revieved to determine their accuracy and insure that they include the authorized changes reflected in the engineering drawings and the hardware. Unless otherwise directed by the contracting agency Co-Chairperson, inspection of drawings and associated manufacturing instruction sheets may be accomplished on a valid sampling basis. The purpose of this review is to insure the manufacturing instruction sheets accurately reflect all design details contained in the drawings. Since the hardware is built in accordance with the manufacturing instruction sheets, any discrepancies between the instruction sheets and the design details and changes in the drawings will also be reflected in the hardware.

b. The following minimum information shall be recorded for each drawing reviewed:

(1) Drawing number/title (include revision letter)

(2) Date of drawing approval

(3) List of manufacturing instruction sheets (numbers with change letter/titles and date of approval) associated with this drawing.

(4) Discrepancies/comments

(5) Select a sample of part numbers reflected on the drawing. Check to insure compatibility with the Program Parts Selection List, and examine the HWCI to insure that the proper parts are actually installed.

c. As a minimum, the following inspections shall be accomplished for each drawing and associated manufacturing instruction sheets:

(1) Drawing number identified on manufacturing instruction sheet should match latest released drawing.

(2) List of materials on manufacturing instruction sheets should match materials identified on the drawing.

(3) All special instructions called on the drawing should be on the manufacturing instruction sheets.

(4) All dimensions, tolerances, finishes, etc., called out on the drawing should be identified on the manufacturing instruction sheets.

Downloaded from http://www.everyspec.com

(5) All special processes called out on the drawing should be identified on the manufacturing instruction sheets.

(6) Nomenclature descriptions, part numbers and serial number markings called out on the drawing should be identified on the manufacturing instruction sheets.

(7) Review drawings and associated manufacturing instruction sheets to ascertain that all approved changes have been incorporated into the configuration item.

(8) Check release record to insure all drawings revieved are identified.

(9) Record the number of any drawings containing more than five outstanding changes attached to the drawing.

(10) Check the drawings of a major assembly/black box of the hardware configuration item for continuity from top draving down to piece-part drawing.

80.4.2 Review of all records of baseline configuration for the HWCI by direct comparison with contractor's engineering release system and change control procedures to establish that the configuration being produced does accurately reflect released engineering data. This includes interim releases of spares provisioned prior to PCA to ensure delivery of currently configured spares.

80.4.3 Audit of contractor's engineering release and change control system to ascertain that they are adequate to properly control the processing and formal release of engineering changes. The minimum needs and capabilities set forth below are required of his engineering release records system. The contractor's formats, systems, and procedures are to be used. Information in addition to the basic requirements is to be considered part of the contractor's internal system.*

80.4.3.1 As a minimum, the following information shall be contained on one release record supplied by the contractor, subcontractor, or vendor for each drawing number, if applicable:

a. Serial numbers, top drawing number, specification number;

b. Drawing number, title, code number, number of sheets, date

---

* Contract Administration Office (CAO) Quality Assurance Representative (QAR) records can be revieved for purpose of determining the contractor's present and most recent past performance.

Downloaded from http://www.everyspec.com

of release, change letter, date of change letter release, engineering change order (ECO) number.

80.4.3.2 The contractor's release function and documentation will be capable of determining:

a. The composition of any part at any level in terms of subordinate part numbers (disregard standard parts);

b. The next higher assembly using the part number, except for assembly into standard parts;

c. The composition of the configuration item or part number with respect to other configuration items or part numbers;

d. The configuration item and associated serial number on which subordinate parts are used. (This does not apply to contractors below prime level who are not producing configuration items);

e. The accountability of changes which have been partially or completely released against the configuration item;

f. The configuration item and serial number effectively of any change.

g. The standard specification number or standard part numbers used within any nonstandard part number;

h. The contractor specification document and specification control numbers associated with any subcontractor, vendor, or supplier part number.

80.4.3.3 The engineering release system and associated documentation shall be capable of:

a. Identifying changes and retaining records of superseded configurations formally accepted by the contracting agency;

b. Identifying all engineering changes released for production incorporation. These changes shall be completely released and incorporated prior to formal acceptance of the configuration item;

c. Determining the configuration released for each configuration item at the time of formal acceptance.

80.4.3.4 Engineering data shall be released or processed through a central authority to ensure coordinated action and preclude unilateral release of data.

80.4.3.5 Engineering change control numbers shall be unique.

Downloaded from http://www.everyspec.com

80.4.4 Difference between the configuration of the configuration item qualified and the configuration item being audited shall be a matter of record in the minutes of the PCA.

80.4.5 For HWCI acceptance tests data and procedures shall comply with its product specification. The PCA team shall determine any acceptance tests to be reaccomplished, and reserves the prerogative to have representatives of the contracting agency witness all or any portion of the required audits, inspections, or tests.

80.4.6 HWCIs which fail to pass acceptance test requirements shall be repaired if necessary and be retested by the contractor in the manner specified by the PCA team leader in accordance with the product specification.

80.4.7 The contractor shall present data confirming the inspection and test of subcontractor equipment end items at point of manufacture. Such data shall have been witnessed by Government representative.

80.4.8 The PCA team reviews the prepared back-up data (all initial documentation which accompanies the configuration item) for correct types and quantities to ensure adequate coverage at the time of shipment to the user.

80.4.9 Configuration items which have demonstrated compliance with the product specification are approved for acceptance as follows:

a. The PCA team shall certify by signature that the configuration item has been built in accordance with the drawings and specifications.

80.4.10 As a minimum, the following actions shall be performed by the PCA team on each CSCI being audited:

a. Review all documents which will comprise the Software Product Specification for format and completeness

b. Review FCA minutes for recorded discrepancies and actions taken

c. Review the design descriptions for proper entries, symbols, labels, tags, references, and data descriptions.

d. Compare Top-Level Computer Software Component (TLCSC) design descriptions with Lower-Level Computer Software Components (LLCSC) descriptions for consistency

e. Compare all lower-level design descriptions with all software listings for accuracy and completeness

Downloaded from http://www.everyspec.com

f. Check Software User's Manual(s), Software Programmer's Manual, Computer System Operator's Manual, Firmware Support Manual, and Computer System Diagnostic Manual for format completeness and conformance with applicable data item descriptions. (Formal verification/acceptance of these manuals should be withheld until system testing to ensure that the procedural contents are correct)

g. Examine actual CSCI delivery media (card decks, tapes, etc.,) to insure conformance with Section 5 of the Software Requirements Specification.

h. Review the annotated listings for compliance with approved coding standards (e.g. Appendix C of DOD-STD-2167).

80.5 Post Audit Actions

80.5.1 Contracting agency acceptance or rejection of the configuration item and the configuration item product specification presented for PCA must be furnished to the contractor in writing by the responsible contract management agency or other designated agency after completion of PCA.

80.5.2 After completion of the PCA, the contractor shall publish and distribute copies of PCA minutes. The contracting agency officially acknowledges completion of the PCA as indicated in paragraph 4.2.4.

80.5.3 The accomplishment of the PCA shall be recorded on the configuration item Development Record by the contractor.

Downloaded from http://www.everyspec.com

90. Formal Qualification Review.

90.1 General. The objective of the FQR shall be to verify that the actual performance of the configuration items of the system as determined through test comply with the hardware Development Specification, Software Requirements and Interface Requirements Specifications, and to identify the test report(s)/data which document results of qualification tests of the configuration items. The point of Government certification will be determined by the contracting agency and will depend upon the nature of the program, risk aspects of the particular hardware and software, and contractor progress in successfully verifying the requirements of the configuration items. When feasible, the FQR shall be combined with the FCA at the end of configuration item/subsystem testing, prior to PCA. If sufficient test results are not available at the FCA to insure the configuration items will perform in their system environment, the FQR shall be conducted (post PCA) during System testing whenever the necessary tests have been successfully completed to enable certification of configuration items. For non-combined FCA/FQRs, traceability, correlation, and completeness of the FQR shall be maintained with the FCA and duplication of effort avoided.

90.2 Requirements.

90.2.1 In cases where the FQR and the FCA can be accomplished in a single combined Audit/Review, contractor and Government "certification" of the configuration items shall be accomplished after completion of the FCA and such certification shall be considered as accomplishment of the FQR.

90.2.2 When the agency responsible for qualification of the configuration items at the contracting agency judges that the system is not ready for FQR at the time of FCA, the FQR will be delayed until it is determined that sufficient information on the system's qualification is available. The FQR may be delayed up to the end of System testing if deemed necessary.

90.2.3 When a separate FQR is necessary, the contractor shall notify the contracting agency of the sufficiency of the configuration items test results to substantiate a FQR and coordinate the agenda with the Deputy Director for Test and Deployment. The FQR team will be assembled in the same manner as that required for the FCA team. No duplication of FCA effort shall occur at the FQR; however, the following additional efforts must be accomplished:

90.2.3.1 A review of the FCA minutes must be performed and the FQR shall be considered as an extension of FCA. New/additional qualification data shall be audited and reviewed to insure qualification of the configuration items against the System/Segment, Software Requirements, and Interface Requirements

Downloaded from http://www.everyspec.com

Specifica-

90.2.3.2 Any testing accomplished against configuration item qualification during System testing shall be considered.

90.2.3.3 The contractor shall, after notification of certification by the contracting agency enter the date of system certification of qualification and the identity of the test reports/documentation which sets forth the results of the associated test(s) in the configuration item Development Record.

90.2.4 All other factors such as: agenda, team organization, review procedures, data to be revieved, etc., shall be accomplished as delineated in the FCA and General Requirements and Procedures sections of this standard to the extent necessary to accomplish the FQR.

90.3 Post Review Action

90.3.1 After the conduct of the FQR, the contractor shall publish and distribute copies of FQR minutes. The contracting agency will officially acknowledge the conduct of the Review as indicated in paragraph 4.2.4.

Downloaded from http://www.everyspec.com

SAMPLE CERTIFICATION ATTACHMENT

PRE-FCA CHECK SHEET

NOMENCLATURE _____

CONFIGURATION ITEM NO. _____ DATE _____

CONTRACTOR REQUIREMENTS	YES	NO
1. Waiver/Deviation List Prepared	____	____
2. Qualification Test Procedures Submitted	____	____
3. Qualification Testing Completed	____	____
4. Qualification Test Results Compiled & Available	____	____
5. Facilities for Conducting FCA Available	____	____
6. Qualification Test Procedures Reviewed and Approved	____	____
7. Qualification Testing Witnessed	____	____
8. Qualification Test Data and Results Reviewed and Approved	____	____

COMMENTS _____

Figure 3
Page 1 of 11

Downloaded from http://www.everyspec.com

SAMPLE CERTIFICATION ATTACHMENT

FUNCTIONAL CONFIGURATION AUDIT (FCA)

FOR

CONFIGURATION ITEM NO. (S) _____

CONTRACT NO. _____

PRIME CONTRACTOR:	EQUIPMENT MANUFACTURERS:
_____	_____
_____	_____
_____	_____

APPROVED BY _____ (CONTRACTOR)

APPROVED BY _____ (CONTRACTING AGENCY)

DATE _____

DATE _____

Figure 3
Page 2 of 11

Downloaded from http://www.everyspec.com

DEFINITIONS:

COMMENT: A note explaining, illustrating, or criticizing the meaning of a writing. Items of this nature should be explored by the contractor and/or the Contracting Agency, but corrective action is NOT necessary to successfully accomplish a FCA.

DEFICIENCY: Deficiencies consist of two types: (1) conditions of characteristics in any hardware/software which are not in compliance with specified configuration, or (2) inadequate (or erroneous) configuration, identification which has resulted, or may result in configuration items that do not fulfill approved operational requirements.

Downloaded from http://www.everyspec.com

SCOPE/PURPOSE

Scope:

Functional Configuration Audit (FCA) was conducted on the following configuration item:

Configuration Item No.	Nomenclature	Part No.	Serial No.

PURPOSE: The purpose of this FCA was to verify that the configuration item's performance complies with the Type B Development Specification.

Figure 3
Page 4 of 11

Downloaded from http://www.everyspec.com

FUNCTIONAL CONFIGURATION AUDIT

CERTIFICATION SHEET NO. 1
(For Equipment/Computer Software)

Contract: _____ Date _____

Contractor: _____

Configuration Item No.: _____

_____

Qualification Test Procedures and Results. The qualification test/analysis results have been reviewed to ensure that testing is adequat properly done, and certified. (All test procedures and interface documents shall be reviewed to assure that the documents have been approved by the Contracting Agency. All test data sheets shall be reviewed to assure that the test was witnessed by a representative of the Contracting Agency.)

Attached is a list of the documents reviewed.

Check One

Procedures and results reviewed satisfy the requirements and are accepted. See Attachment __ for comments.

Attached is a list of deficiencies.

Signature(s) of FCA Team Member(s)

* _____ _____

_____ _____

_____ _____

_____ _____

_____ _____

_____ _____

*Sub-Team Chairperson

Figure 3
Page 5 of 11

Downloaded from http://www.everyspec.com

SPECIFICATION/TESTING REVIEW

Configuration Item No. _____ Nomenclature _____

Specification No. _____

Test Procedures _____

Spec Ref / TP Ref	Description	Test Result

Figure 3
Page 6 of 11

FCA DEFICIENCY SUMMARY LIST

CONFIGURATION ITEM NO. _____ NOMENCLATURE _____

CONFIGURATION ITEM NUMBER	REPORT REFERENCE	DESCRIPTION	RESPONSIBILITY FOR CORRECTION	PLACE OF INSPECTION	INSPECTED BY

Figure 3
Page 7 of 11

Downloaded from http://www.everyspec.com

Downloaded from http://www.everyspec.com

FUNCTIONAL CONFIGURATION AUDIT

CERTIFICATION SHEET NO. 2
(For Equipment/Computer Software)

Contract: _____ Date _____

Contractor: _____

Configuration Item No.: _____

_____

Review Deviations/Waivers. A review of all deviations/waivers to military specifications and standards that have been approved. The purpose is to determine the extent to which the equipment(s)/computer software undergoing FCA vary from applicable specifications and standards and to form a basis for satisfactory compliance with these specifications and standards.

In accordance with this paragraph, all applicable deviations/waivers have been reviewed with the following results:

Check One

☐ The equipment(s)/computer software listed on Certification Sheet No. 1 of this report complies with all applicable specifications and standards. See Attachment __ for comments.

☐ Attached is a list of discrepancies and/or comments.

Signature(s) of FCA Team Member(s)

* _____	_____
_____	_____
_____	_____
_____	_____
_____	_____
_____	_____

*Sub-Team Chairperson

Figure 3
Page 8 of 11

Downloaded from http://www.everyspec.com

APPENDIX I

A. Deviation/Waiver Review Team Instructions. All approved waivers and deviations to military specifications and standards shall be reviewed and recorded. Also, record any part of the FCA which fails to meet specifications or standards but is not an approved waiver/deviation.

B. Results of Team Review. List the deviations/waivers against the equipment/computer software being FCA'd that were reviewed.

Figure 3
Page 9 of 11

WAIVERS/DEVIATIONS

CONFIGURATION ITEM NO. _____ NOMENCLATURE _____

REFERENCE (Spec, STD, Etc.)	CCB OR MRB APPROVAL/DIRECTIVE	REQUIREMENT WAIVED	REMARKS

Figure 3
Page 10 of 11

Downloaded from http://www.everyspec.com

Downloaded from http://www.everyspec.com

SAMPLE CERTIFICATION ATTACHMENT

FORMAL QUALIFICATION REVIEW
(For Equipment/Computer Software)

Contract: _____ Date _____

Contractor: _____

Configuration Item No.: _____

_____

Formal Qualification Review. Qualification Test/Analysis results have been reviewed to verify that the actual performance of the configuration item complies with its development or requirements specification(s) and that sufficient test results are available to ensure the configuration item will perform in its system environment.

Attached is a list of the documents reviewed.

Check One

☐ Results reviewed satisfy FQR requirements and the configuration item is qualified for entry into the Government Inventory.

☐ Results reviewed are unsatisfactory/insufficient for FQR. FQR will be delayed until it is determined that sufficient information on the configuration items Qualification is available.

Signature(s) of FCA Team Member(s)

_____ _____

_____ _____

_____ _____

_____ _____

_____ _____

_____ _____

Figure 3
Page 11 of 11

Downloaded from http://www.everyspec.com

SAMPLE CERTIFICATION ATTACHMENT

SAMPLE PCA CHECKLIST

The following hardware, computer software, documentation shall be available, and the following tasks shall be accomplished at the PCA.

Hardware:

Computer Software:

Documentation:

		Yes	No
(1)	Approved final draft of the configuration item product specification.		
(2)	A list delineating both approved and outstanding changes against the configuration item.		
(3)	Complete shortage list.		
(4)	Acceptance test procedures and associated test data.		
(5)	Engineering Drawing Index.		
(6)	Operating, maintenance, and illustrated parts breakdown manuals.		
(7)	List of approved material review board actions on waivers.		
(8)	Proposed DD Form 250, "Material Inspection and Receiving Report".		
(9)	Approved nomenclature and nameplates.		
(10)	Manuscript copy of all CSCI manuals.		
(11)	Computer Software Version Description Document.		
(12)	Current set of listings and updated design descriptions or other means of design portrayal for each CSCI.		
(13)	FCA minutes for each configuration item.		

Figure 4
Page 1 of 20

Downloaded from http://www.everyspec.com

SAMPLE CERTIFICATION ATTACHMENT

SAMPLE PCA CHECKLIST (CONTINUED)

		Yes	No
Tasks:			
(1)	Define Product Baseline.	____	____
(2)	Specification Review and Validation.	____	____
(3)	Drawing review.	____	____
(4)	Review acceptance test procedures and results.	____	____
(5)	Review shortages and unincorporated design changes.	____	____
(6)	Review deviations/waivers.	____	____
(7)	Examine proposed DD 250.	____	____
(8)	Review contractor's Engineering Release and Change Control System.	____	____
(9)	Review system allocation document.	____	____
(10)	Review Software User's Manuals, Software Programmer's Manuals, Computer System Diagnostic Manual, Computer System Operator's Manual, and Firmware Support Manual.	____	____
(11)	Review CSCIs for the following:		
	(a) Top-level and lower-level Computer Software Component design descriptions or alternative design portrayals.	____	____
	(b) Top-level and lower-level Computer Software Component interface requirements.	____	____
	(c) Data base characteristics, storage allocation charts and timing and sequencing characteristics.	____	____
(12)	Review packaging plan and requirements.	____	____
(13)	Review status of Rights in Data.	____	____

Figure 4
Page 1a of 20

Downloaded from http://www.everyspec.com

SAMPLE CERTIFICATION ATTACHMENT

PHYSICAL CONFIGURATION AUDIT (PCA)

FOR

CONFIGURATION ITEM NO.(s) _____

CONTRACT NO. _____

PRIME CONTRACTOR:

_____

_____

_____

APPROVED BY _____ (DESIGNEE)
CONTRACTOR

DATE _____

EQUIPMENT MANUFACTURERS:

_____

_____

_____

APPROVED BY _____ (DESIGNEE)
CONTRACTING AGENCY

DATE _____

Figure 4
Page 2 of 20

Downloaded from http://www.everyspec.com

DEFINITION OF TERMS

COMMENT - A note explaining, illustrating, or criticizing the meaning of a writing. Items of this nature should be explored by the contractor and/or the Contracting Agency, but corrective action is NOT necessary to successfully accomplish a PCA.

DISCREPANCY - A not explaining, illustrating, or criticizing the difference between writings. A note showing the variance between what exists and what is acceptable. Items of this nature shall be rectified by the contractor prior to successful accomplishments of a PCA.

Downloaded from http://www.everyspec.com

SCOPE/PURPOSE

A Physical Configuration Audit (PCA) was conducted on the following end items of equipment/computer software:

CONFIGURATION ITEM	NOMENCLATURE	PART NUMBER	SERIAL NO.	NSN

The purpose of the PCA was to ensure accuracy of the identifying documentation and to establish a product baseline.

The establishment of a product baseline for equipment/computer software is not to be construed as meeting Contracting Agency requirements for delivery by the contractor of an operational system meeting approved acceptance criteria.

Downloaded from http://www.everyspec.com

PHYSICAL CONFIGURATION AUDIT

CERTIFICATION SHEET NO. 1
(For Equipment/Computer Software)

Contract: _____ Date _____

Contractor: _____

_____

_____

Product baseline. The following documents of the issue and date shown comprise the product baseline for the listed equipment(s)/ computer software:

SPEC NO.	ASSEMBLY TOP DRAWING NO.	ISSUE	EQPT./COMP. SOFTWARE NOMENCLATURE	CONFIGURATION ITEM NO.

Signature(s) of PCA Team Member(s)

** _____ _____

* _____ _____

_____ _____

_____ _____

_____ _____

_____ _____

**Team Chairperson
*Sub-Team Chairperson

Figure 4
Page 5 of 20

Downloaded from http://www.everyspec.com

PHYSICAL CONFIGURATION AUDIT

CERTIFICATION SHEET NO. 2
(For Equipment/Computer Software)

Contract: _____ Date _____

Contractor: _____

_____

_____

Specification Review and Validation. Specifications have been reviewed and validated to assure that they adequately define the configuration item and the necessary testing, mobility/transportability, and packaging requirements.

Check One

☐ The Type C Specifications are complete and adequately define the configuration item. They shall, therefore, constitute the product baseline. See Attachment __ for comments.

☐ The Type C Specifications are unacceptable. Attached is a list of discrepancies.

Signature(s) of PCA Team Member(s)

* _____	_____
_____	_____
_____	_____
_____	_____
_____	_____
_____	_____

*Sub-Team Chairperson

Figure 4
Page 6 of 20

Downloaded from http://www.everyspec.com

A. Specification Review and Validation Instructions. The detailed specifications listed in paragraph B. Below shall be reviewed for compliance with the applicable requirements. Each Specification shall serve as the basic document for configuration control of the subject configuration items. The information contained within the specifications shall be audited at the PCA.

B. Review and Validation Results:

1. Specifications Reviewed and Validated

SPEC NO.	PART NO.	DATE	EQPT./COMP. SOFTWARE NOMENCLATURE	CONFIGURATION ITEM NO.

2. Specifications Reviewed and Disapproved: (Provide attachment for causes.)

Downloaded from http://www.everyspec.com

PHYSICAL CONFIGURATION AUDIT

CERTIFICATION SHEET NO. 3
(Equipment)

Contract: _____ Date _____

Contractor: _____

_____

_____

Drawing Review. Drawings have been compared with the equipment to ensure that the latest drawing change letter has been incorporated into the equipment, that part numbers agree with the drawings, and that the drawings are complete and accurately describe the equipment.

Attachment __ is a list of the drawings reviewed.

Check One

☐ The drawings are complete and accurately describe the equipment. See attachment __ for comments.

☐ Attachment __ is a list of discrepancies.

Signature(s) of PCA Team Members(s)

* _____	_____
_____	_____
_____	_____
_____	_____
_____	_____
_____	_____

*Sub-Team Chairperson

Figure 4
Page 8 of 20

Downloaded from http://www.everyspec.com

A. Drawing Review Results. The following drawings were reviewed by the PCA drawing reviewing sub-teams:

DOCUMENT NUMBER	DOCUMENT TITLE

Figure 4
Page 9 of 20

Downloaded from http://www.everyspec.com

PHYSICAL CONFIGURATION AUDIT

CERTIFICATION SHEET NO. 4
(Equipment)

Contract: _____ Date _____

Contractor: _____

_____

_____

Acceptance Test Procedures and Results. The acceptance test results have been reviewed to ensure that testing is adequate, properly done, and certified.

Attachment __ is a list of the documents reviewed.

Check One

☐ Procedures and results reviewed satisfy the requirements and are accepted. See Attachment __ for comments.

☐ Attachment __ is a list of discrepancies.

Signature(s) of PCA Team Member(s)

* _____ _____

_____ _____

_____ _____

_____ _____

_____ _____

*Sub-Team Chairperson

Figure 4
Page 10 of 20

Downloaded from http://www.everyspec.com

PHYSICAL CONFIGURATION AUDIT

CERTIFICATION SHEET NO. 5
(For Equipment/Computer Software)

Contract _____ Date _____

Contractor: _____

_____

_____

Review of Shortages and Unincorporated Design Changes. The shortages and unincorporated design changes listed on the proposed DD Form 250, "Material Inspection and Receiving Report", and other records have been reviewed.

Check One

There are no shortages or unincorporated design changes.

Attachment __ is a list of shortages and/or unincorporated design changes, and the recommended corrective action required.

Signature(s) of PCA Team Member(s)

* _____ _____

_____ _____

_____ _____

_____ _____

_____ _____

*Sub-Team Chairperson

Figure 4
Page 11 of 20

Downloaded from http://www.everyspec.com

A. Review of Shortages and Unicorporated Design Changes. All shortages and unicorporated design changes listed on the proposed DD Form 250, "Material Inspection and Receiving Report", shall be reviewed by the Contracting Agency or their designated representatives for a determination of what changes should be accomplished in the field and what changes should be accomplished at the contractor's facility. The Contracting Agency shall also determine if the reported shortages and unincorporated changes are complete.

B. Results. List the shortages and unincorporated design changes that were reviewed in compliance with requirements.

Figure 4
Page 12 of

Downloaded from http://www.everyspec.com

PHYSICAL CONFIGURATION AUDIT

CERTIFICATION SHEET NO. 6
(For Equipment/Computer Software)

Contract: Date _____

Contractor: _____

_____

_____

Review Deviations/Waivers. A review of all deviations/waivers to military specifications and standards that have been approved. The purpose is to determine the extent to which the equipment(s)/computer software undergoing PCA vary from applicable specifications and standards and to form a basis for satisfactory compliance with these specifications and standards.

In accordance with this paragraph, all applicable deviations/waivers have been reviewed with the following results:

Check One.

The equipment(s)/computer software listed on Certification Sheet No. 1 of this report complies with all applicable specifications and standards. See Attachment __ for comments.

Attachment __ is a list of discrepancies and/or comments.

Signature(s) of PCA Team Member(s)

* _____	_____
_____	_____
_____	_____
_____	_____
_____	_____
_____	_____

*Sub-Team Chairperson

Figure 4
Page 13 of 20

Downloaded from http://www.everyspec.com

A. Deviation/Waiver Review Team Instruction. All approved waivers and deviations to military specifications and standards shall be reviewed and recorded. Also, record any part of the PCA which fails to meet specifications or standards but is not an approved waiver/deviation.

B. Results of Team Review. List the deviations/waivers against the equipment/computer software being PCA's that were reviewed.

Figure 4
Page 14 of 20

Downloaded from http://www.everyspec.com

PHYSICAL CONFIGURATION AUDIT

CERTIFICATION SHEET NO. 7
(For Equipment/Computer Software)

Contract: _____ Date _____

Contractor: _____

_____

_____

Examination of the Proposed DD 250. The DD Form 250 has been examined to ensure that it adequately defines the equipment/computer software and that unaccomplished tasks are inlcuded as deficiencies.

Check One

☐ The DD Form 250 adequately defines the equipment/computer software and all unaccomplished tasks are included as deficiencies.

☐ Attachment __ is a list of discrepancies and/or comments.

Signature(s) of PCA Team Member(s)

_____ _____

_____ _____

_____ _____

_____ _____

_____ _____

*Sub-Team Chairperson

Figure 4
Page 15 of 20

Downloaded from http://www.everyspec.com

A. Examination of the Proposed DD Form 250. The proposed DD Form 250 shall be examined for completeness and an accurate definition of the equipment/computer software. Unaccomplished tasks, shortages, and certain specified discrepancies uncovered at the PCA shall be included in the DD Form 250. If the equipment/computer software is to be shipped from the plant, the Program Office representative will recommend to the CAO that the DD Form 250 be executed in accordance with the terms of the contract.

B. Results. Include a statement that the proposed DD Form 250 was examined and was recommended.

Figure 4
Page 16 of 20

Downloaded from http://www.everyspec.com

PHYSICAL CONFIGURATION AUDIT

CERTIFICATION SHEET NO. 8
(For Equipment/Computer Software)

Contract: _____ Date _____

Contractor: _____

_____

_____

Review of Contractor's Engineering Release and Change Control System. The contractor's engineering release system and change control procedures have been reviewed to ensure that they are adequate to properly control the processing and formal release of engineering changes.

Check One

The contractor's engineering release system and change control procedures are adequate for the processing and formal release of engineering changes. See Attachment __ for comments.

Attachment __ is a list of deficiencies.

Signature(s) of PCA Team Member(s)

* _____	_____
_____	_____
_____	_____
_____	_____
_____	_____
_____	_____

*Sub-Team Chairperson

Figure 4
Page 17 of 20

Downloaded from http://www.everyspec.com

PHYSICAL CONFIGURATION AUDIT

CERTIFICATION SHEET NO. 9
(For Equipment/Computer Software)

Contract: _____ Date: _____

Contractor: _____

_____

_____

System Allocation Document Review. The following System Allocation book form drawings have been reviewed and validated to ensure that they adequately identify, and are compatible with, the shipping instructions.

Check One

☐ The System Allocation Document is complete and adequately defines the equipment/computer software scheduled for each location.

☐ The System Allocation Document is unacceptable. Attached is a list of discrepancies.

☐ This task is not required by contract.

Signature(s) of PCA Team Member(s)

* _____ _____

_____ _____

_____ _____

_____ _____

_____ _____

*Sub-Team Chairperson

Figure 4
Page 18 of 20

Downloaded from http://www.everyspec.com

A. System Allocation Document Instructions:

1. The System Allocation Documents, both Part I and Part II, applicable to the contract shall be reviewed to determine their accuracy and insure that they adequately describe the equipment/computer software.

2. The following information shall be recorded:

Part I.

a. System employment and configuration.
b. Specification reference.
c. Location.
d. Mission Equipment.
   Configuration Item Number
   Short Title
   Part Number
   Serial Number
e. Installed equipment/computer software.
   Configuration Item Number
   Short Title
   Part Number
   Serial Number
f. Drawing Title and Number
g. Number of sheets
h. Issue Number.

Part II.

a. Location.
b. Specification Number
c. Equipment/computer software nomenclature.
d. Configuration Item Quantity.
e. Assembly Drawing Number

3. Insure that the System Allocation Documents are compatible wi the priorities and shipping instructions.

B. System Allocation Document Review Results. The following System Allocation Documents were reviewed by the PCA Reviewing Sub-Team:

DOCUMENT NUMBER	DOCUMENT TITLE

Downloaded from http://www.everyspec.com

PHYSICAL CONFIGURATION AUDIT

CERTIFICATION SHEET NO. 10
(Equipment)

Contract: _____ Date _____

Contractor: _____

_____

1. Review of Logistics Support Plan for Pre-operational Support. The Logistics Support Plan for Pre-operational Support has been reviewed to ensure that it is adequate to support the acquisition phase and is compatible with the operational phase maintenance concept and support requirements.

Check One

☐ The contractor's Logistic Plan for pre-operational support will fulfill the acquisition phase requirements and is compatible with operational phase needs.

☐ Attachment __ is a list of deficiencies.

. Review of Long Lead Time Items and Provisioned Items Processed to PCA. Long Lead Time items released and items provisioned, prior to PCA have been reviewed to ensure that obsolete items resulting from pre-PCA design changes are purged from the system. Where basic items may be upgraded by rework or modification these actions have been verified as accomplished or in process based upon design change notice.

Check One

☐ Long lead time items and provisioned items processed, prior to PCA, are all of current configuration at time of PCA or are in work.

☐ Attachment __ is a list of deficiencies.

Signature(s) of PCA Team Member(s)

* _____ _____

_____ _____

_____ _____

_____ _____

*Sub-Team Chairperson

Figure 4
Page 20 of 20

Downloaded from http://www.everyspec.com

100. Application Guide for Tailoring MIL-STD-1521

100.1 Scope

This appendix sets forth guidance for the cost effective application of the requirements of this standard when this standard is contractually invoked during the acquisition process. This appendix serves as guidance for the activity responsible for the preparation of contract requirements and does not form a part of the contract.

100.2 Purpose

The guidelines contained herein implement the Department of Defense Directive 4120.21, Specification and Standards Application, which requires all DOD components to apply selectively and tailor military specifications and standards prior to their contractual imposition and:

a. Eliminate inapplicable and unnecessary requirements.

b. Provide for adding/modifying necessary technical review and audit factors not included in MIL-STD-1521.

c. Eliminate redundancy and inconsistency with other contract specifications and standards.

100.3 Objective

The objective of this guide is to establish the applications and limitations of tailoring MIL-STD-1521. MIL-STD-1521 is not a stand-alone document. It is dependent upon the work effort specified in the contractual requirements (e.g., SOW, etc.) The tailoring of specifications should take place in all phases of military procurement, but is especially applicable to the initial stages of solicitation package preparation and contract negotiation. Depending upon the type of end-item(s) under procurement, the reviews and audits outlined by MIL-STD-1521 may or may not be required for all programs.

100.4 Considerations for Tailoring

100.4.1 Relationship to the Statement of Work

The Program Manager must keep in mind that technical reviews provide visibility into the contractor's implementation of the work effort required under the terms of the SOW and the contract to assure timely and effective attention to the technical interpretation of contract requirements. The key to tailoring MIL-STD-1521 is to match the MIL-STD-1521 requirements against the details of the applicable SOW/Contractual task requirements. It will become immediately obvious that MIL-STD-1521 may contain

Downloaded from http://www.everyspec.com

technical review factors that are not applicable to the contract under consideration. (For example, if a contract does not include computer software, all references to the review of Computer Software materials in MIL-STD-1521 will not apply.) When MIL-STD-1521 is used, then a task containing the applicable requirements will be specified in the SOW. Review factors not set forth in MIL-STD-1521 but considered necessary because of the nature of the particular program should be added in the SOW. By carefully going through this evaluative process the technical review and audit requirements will become program specific rather than an all purpose document to be continually negotiated during contract performance.

100.4.2 Elimination of Redundancy and Ambiguity

While MIL-STD-1521 is the broad program document for technical reviews and audits, other standards in existence also require technical reviews or audits. For example, MIL-STDs for reliability, maintainability, system engineering and others can require reviews and/or audits. Review of these aspects of the design would also be required under MIL-STD-1521; therefore, if such standards are contractually stipulated together with MIL-STD-1521, the SOW should include a provision to show how and whether the technical review requirements of these other standards can be combined with technical reviews/audits in MIL-STD-1521. Combining reviews does not nullify other MIL-STD(s), "Plans", etc, which contain requirements for reviews/audits. The contract should require the minimal integrated, comprehensive technical design review effort that will provide the desired visibility and assurance of contract compliance.

100.4.3 Contractor Participation in Tailoring

When requiring a particular review or audit, it is important that the topics to be reviewed are aligned to the program requirements. Therefore, the offeror should be given an opportunity to recommend changes and identify topics/items he considers appropriate. The program office should request, in the instructions for proposal preparation, that the offeror recommend the MIL-STD-1521 topics/items and their related details to be covered at the various reviews or audits required by the SOW. This will allow the offeror to tailor the topics/items and details by additions and deletions for the particular review/audit. In addition, it must be recognized that effecive tailoring requires several points of review. The requirement, however, for the review/audit must be finalized prior to contract award.

100.4.4 Complexity

a. System/Segment/subsystem/configuration item complexity and type of program is central in determining both the need for and the number of such reviews. When developing a small

Downloaded from http://www.everyspec.com

non-complex system some reviews may not be required, or, if required, may be limited in Scope. The tailoring procedures discussed earlier should result either in the exclusion of MIL-STD-1521 or in a tailored MIL-STD-1521 that reflects a limited scope technical review effort. Conversely, in a very complex development the review process will increase in levels and numbers of reviews.

b. In addition to the above, the degree of application is dependent upon the configuration item state of development (example, new design vs. commercially available) or the degree of any modifications, if involved. For example: a newly developed item may require the majority of the review topics/items and audits, while a commercially available configuration item with the appropriate documentation, i.e., verified test results, specifications, drawings, etc. may require reviews or audits limited to its application to the program and its interfaces. In the case of modified designs one must consider the degree and effect of the modifications. Reviews and audits may be limited to the modifications and their interfaces.

100.5 Scheduling of Technical Reviews and Audits

The schedule for Technical Reviews and Audits is extremely important. If they are conducted too early, the item for review will not be adequately defined. Conversely, if the review is too late, the program commitments could have been made erroneously, and correction will be both difficult and costly. For planning purposes, a good method for scheduling technical reviews is to relate them to the documentation requirements. For example, schedule a PDR after the hardware Development Specification or Software Top Level Design Document and Software Test Plan are available, since the essence of the PDR is to assess the contractor's approach to meeting these requirements of these documents. Scheduling of audits are dependent not only on documentation availability but also on hardware/software availability, and the completion of the acceptance qualification tests. Table 1 contains a list of the primary documentation associated with each review or audit and the estimated time phasing:

TABLE 1
SCHEDULING TECHNICAL REVIEWS AND AUDITS

Review	Time Phase	Primary Documentation
SRR	Usually accomplished in the Concept Exploration phase. However, may be used in other phases when the	Various analysis and trade study reports used to develop the system/segment

Downloaded from http://www.everyspec.com

Review	Time Phase	Primary Documentation
	Concept Exploration phase is not accomplished.	requirements for the specification.
SDR	Usually in the Demonstration and Validation phase.	System/Segment Specification, preliminary Operational Concept Document, preliminary Software Requirements and Interface Requirements Specifications, analyses, trade studies, Drawings Level I DOD-D-1000.
SSR	Usually early in Full Scale Development	Software Requirements Specification, Interface Requirements Specifications, Operational Concept Document.
PDR	Usually accomplished in the Demonstration and Validation and/or Full Scale Development Phase	Development, Type B Performance Specification, Drawings Level I DOD-D-1000, Software Top Level Design Document, Software Test Plan, preliminary Computer Resources Integrated Support Document, preliminary Computer System Operator's Manual, preliminary Software User's Manual, preliminary Computer System Diagnostic Manual.
CDR	Usually accomplished in the Full Scale Development phase	Draft Product, Type C Specification, and referenced documentation, Drawings Level I or II DOD-D-1000, Software Detailed Design Document, Interface Design Document(s), Data Base Design Document(s),

Downloaded from http://www.everyspec.com

Review	Time Phase	Primary Documentation
		Software Test Description, Computer Resources Integrated Support Document, Software Programmer's Manual, Firmware Support Manual, Informal Test Descriptions/Test Procedures, Software Development File(s).
TRR	Usually accomplished in the Full Scale Development phase	Software Test Procedure, Informal software test results (of development tests).
FCA	Usually accomplished at end of Full Scale Development	Test plans, test descriptions, test procedures, Software Test Reports, Computer System Operator's Manual, Software User's Manual, Computer System Diagnostic Manual.
PCA	Usually accomplished early in the initial production when the developing contractor is preselected as the production contractor. However, may be accomplished at the end of Full Scale Development when the developing contractor is not preselected as the production contractor. And the PCA is repeated with each subsequent contractor or break in production.	Final Part II Specification/Type C Product Specifications and referenced documents and drawings. Drawings Level II or III DOD-D-1000. Software Product Specification, Version Description Document.

Although the time frame for reviews and audits is suggested above, they may vary depending on the particular program. The schedule for each review or audit may be requested from the offeror as part of his proposal, or as part of the system engineering management plan (which can be part of the proposal).

Downloaded from http://www.everyspec.com

110. Production Readiness Review (PRR)

110.1 For specific guidance, see AFSCR 84-2, Production Readiness Review.

Downloaded from http://www.everyspec.com

Custodian:
Air Force - 13

Preparing Activity:
Air Force - 13

Review Activity:
Air Force - 10,11,80,85

(Project CMAN-0-006)

Downloaded from http://www.everyspec.com

INSTRUCTIONS: In a continuing effort to make our standardization documents better, the DoD provides this form for use in submitting comments and suggestions for improvements. All users of military standardization documents are invited to provide suggestions. This form may be detached, folded along the lines indicated, taped along the loose edge *(DO NOT STAPLE)*, and mailed. In block 8, be as specific as possible about particular problem areas such as wording which required interpretation, was too rigid, restrictive, loose, ambiguous, or was incompatible, and give proposed wording changes which would alleviate the problems. Enter in block 6 any remarks not related to a specific paragraph of the document. If block 7 is filled out, an acknowledgement will be mailed to you within 30 days to let you know that your comments were received and are being considered.

NOTE: This form may not be used to request copies of documents, nor to request waivers, deviations, or clarification of specification requirements on current contracts. Comments submitted on this form do not constitute or imply authorization to waive any portion of the referenced document(s) or to amend contractual requirements.

(Fold along this line)

(Fold along this line)

OFFICIAL BUSINESS
PENALTY FOR PRIVATE USE $300

BUSINESS REPLY MAIL
FIRST CLASS PERMIT NO. 73236 WASH DC

POSTAGE WILL BE PAID BY THE U.S. AIR FORCE

COMMANDER, HEADQUARTERS ELECTRONIC
SYSTEMS DIVISION (HQ ESD)
ATTN: ALET, SYSTEMS ENGINEERING DIVISION
HANSCOM AFB, MA 01731

NO POSTAGE
NECESSARY
IF MAILED
IN THE
UNITED STATES

Downloaded from http://www.everyspec.com

STANDARDIZATION DOCUMENT IMPROVEMENT PROPOSAL

(See Instructions – Reverse Side)

1. DOCUMENT NUMBER	2. DOCUMENT TITLE
[illegible]	

NAME OF SUBMITTING ORGANIZATION	4. TYPE OF ORGANIZATION (Mark one)
	☐ VENDOR ☐ USER ☐ MANUFACTURER ☐ OTHER (Specify): _____
5. ADDRESS (Street, City, State, ZIP Code)	

6. PROBLEM AREAS

a. Paragraph Number and Wording:

b. Recommended Wording:

c. Reason/Rationale for Recommendation:

7. REMARKS

8. NAME OF SUBMITTER (Last, First, MI) – Optional	9. WORK TELEPHONE NUMBER (Include Area Code) – Optional
10. MAILING ADDRESS (Street, City, State, ZIP Code) – Optional	11. DATE OF SUBMISSION (YYMMDD)

DD FORM 1426 PREVIOUS EDITION IS OBSOLETE.

Downloaded from http://www.everyspec.com

MILITARY STANDARD
TECHNICAL REVIEWS AND AUDITS FOR SYSTEMS, EQUIPMENTS, AND COMPUTER SOFTWARE

TO ALL HOLDERS OF MIL-STD-1521B:

1. THE FOLLOWING PAGES OF MIL-STD-1521B HAVE BEEN REVISED AND SUPERSEDE THE PAGES LISTED:

NEW PAGE	DATE	SUPERSEDED PAGE	DATE
vi	19 Dec 1985	vi	4 June 1985
7/8	19 Dec 1985	7/8	4 June 1985
19	19 Dec 1985	19	4 June 1985
20	4 June 1985	(Reprinted without change)	
25	19 Dec 1985	25	4 June 1985
26	19 Dec 1985	26	4 June 1985
29	19 Dec 1985	29	4 June 1985
30	19 Dec 1985	30	4 June 1985
35	19 Dec 1985	35	4 June 1985
36	4 June 1985	(Reprinted without change)	
37	4 June 1985	(Reprinted without change)	
38	19 Dec 1985	38	4 June 1985
38a	19 Dec 1985	New page	
55	19 Dec 1985	55	4 June 1985
56	19 Dec 1985	56	4 June 1985
56a	19 Dec 1985	New page	
71	19 Dec 1985	71	4 June 1985
72	4 June 1985	(Reprinted without change)	
73	19 Dec 1985	73	4 June 1985
74	4 June 1985	(Reprinted without change)	
75	19 Dec 1985	75	4 June 1985
76	4 June 1985	(Reprinted without change)	
119	19 Dec 1985	119	4 June 1985
119a	19 Dec 1985	New page	
123	4 June 1985	(Reprinted without change)	
124	19 Dec 1985	124	4 June 1985
125	19 Dec 1985	New page	
126	19 Dec 1985	New page	
127	19 Dec 1985	New page	

2. Retain this notice and insert before table of contents.

3. Holders of MIL-STD-1521B will verify that page changes and additions indicated above have been entered. This notice page will be retained as a check sheet. This issuance, together with appended pages, is a separate publication. Each notice is to be retained by stocking points until the Military Standard is completely revised or canceled.

Custodians:
Air Force - 13

Preparing Activity:
Air Force - 13

Review Activities:
Air Force - 10, 11, 80, 85

DISTRIBUTION STATEMENT A. Approved for public release; distribution is unlimited.

Downloaded from http://www.everyspec.com

FIGURES

Section		Page
Figure 1	Engineering and Test Flow	16
Figure 2	Sample Action Item Form	17
Figure 3	Sample Certification Attachment (FCA)	85
Figure 4	Sample Certification Attachment (PCA)	96
Figure 5	Review Checklist for Engineering Data	124-125
Figure 6	Engineering Data Discrepancy Sheet	126

APPENDIXES

Appendix		Page
A.	System Requirements Review (SRR)	19
B.	System Design Review (SDR)	23
C.	Software Specification Review (SSR)	31
D.	Preliminary Design Review (PDR)	33
E.	Critical Design Review (CDR)	53
F.	Test Readiness Review (TRR)	69
G.	Functional Configuration Audit (FCA)	71
H.	Physical Configuration Audit (FCA)	75
I.	Formal Qualification Review (FQR)	83
J.	Application Guide for Tailoring MIL-STD-1521	117
K.	Production Readiness Review (PRR)	123

Downloaded from http://www.everyspec.com

3.10 Production Readiness Review (PRR). This review is intended to determine the status of completion of the specific actions which must be satisfactorily accomplished prior to executing a production go-ahead decision. The review is accomplished in an incremental fashion during the Full-Scale Development phase, usually two initial reviews and one final review to assess the risk in exercising the production go-ahead decision. In its earlier stages the PRR concerns itself with gross level manufacturing concerns such as the need for identifying high risk/low yield manufacturing processes or materials or the requirement for manufacturing development effort to satisfy design requirements. The reviews become more refined as the design matures, dealing with such concerns as production planning, facilities allocation, incorporation of producibility-oriented changes, identification and fabrication of tools/test equipment, long lead item acquisition etc. Timing of the incremental PRRs is a function of program posture and is not specifically locked in to other reviews.

OTHER DEFINITIONS

3.11 For further guidance on cost terminology see the latest edition of DODI 5000.33, Uniform Budget/Cost Terms and Definitions.

3.12 New titles are being phased in for the levels of maintenance. They are (with their former terms): On Equipment (Organizational), Off Equipment - On Site (Intermediate), Off Equipment - Off Site (Depot). See the latest edition of AFR 66-14, Equipment Maintenance Policies, Objectives, and Reponsibilities.

3.13 For definitions of the various levels of repair, see the latest edition of MIL-STD-280A, Definition of Item Levels, Item Exchangeability, Models, and Related Terms.

3.14 Configuration item. Hardware or software, or an aggregation of both, which is designated by the contracting agency for configuration management.

3.15 Engineering Data: Engineering documents such as drawings, associated lists, acompanying documents, manufacturer specifications, manufacturing planning documentation, and standards or other information prepared by a design activity and relating to the design, manufacture, procurement, test, or inspection of hardware items or services, as defined in DOD-STD-100 and DOD-D-1000.

Downloaded from http://www.everyspec.com

10. System Requirements Review (SSR).

10.1 General. The SRRs are normally conducted during the system Concept Exploration or Demonstration and Validation phase. Such reviews may be conducted at any time but normally will be conducted after the accomplishment of functional analysis and preliminary requirements allocation (to operational/maintenance/training Hardware Configuration Items (HWCIs), Computer Software Configuration Items (CSCIs), facility configuration items, manufacturing considerations, personnel and human factors) to determine initial direction and progress of the contractor's System Engineering Management effort and his convergence upon an optimum and complete configuration.

10.2 Purpose. The total System Engineering Management activity and its output shall be reviewed for responsiveness to the Statement of Work and system/segment requirements. Contracting agency direction to the contractor will be provided, as necessary, for continuing the technical program and system optimization.

10.3 Items to be Reviewed. Representative items to be reviewed include the results of the following, as appropriate:

a. Mission and Requirements Analysis

b. Functional Flow Analysis

c. Preliminary Requirements Allocation

d. System/Cost Effectiveness Analysis

e. Trade studies (e.g. addressing system functions in mission and support hardware/firmware/software).

f. Synthesis

g. Logistics Support Analysis

h. Specialty Discipline Studies (i.e., hardware and software reliability analysis, maintainability analysis, armament integration, electromagnetic compatibility, survivability/vulnerability (including nuclear), inspection methods/techniques analysis, energy management, environmental considerations).

i. System Interface Studies

j. Generation of Specification

k. Program Risk Analysis

l. Integrated Test Planning

Downloaded from http://www.everyspec.com

m. Producibility Analysis Plans

n. Technical Performance Measurement Planning

o. Engineering Integration

p. Data Management Plans

q. Configuration Management Plans

r. System Safety

s. Human Factors Analysis

t. Value Engineering Studies

u. Life Cycle Cost Analysis

v. Preliminary Manufacturing Plans

w. Manpower Requirements/Personnel Analysis

x. Milestone Schedules

10.3.1 The contractor shall describe his progress and problems in:

10.3.1.1 Risk identification and risk ranking (the interrelationship among system effectiveness analysis, technical performance measurement, intended manufacturing methods, and costs shall be discussed, as appropriate).

10.3.1.2 Risk avoidance/reduction and control (the interrelationships with trade-off studies, test planning, hardware proofing, and technical performance measurement shall be discussed, as appropriate).

10.3.1.3 Significant trade-offs among stated system/segment specification requirements/constraints and resulting engineering design requirements/ constraints, manufacturing methods/process constraints, and logistic/cost of ownership requirements/constraints and unit production cost/design-to-cost objectives.

10.3.1.4 Identifying computer resources of the system and partitioning the system into HWCIs and CSCIs. Include any trade-off studies conducted to evaluate alternative approaches and methods for meeting operational needs and to determine the effects of constraints on the system. Also include any evaluations of logistics, technology, cost, schedule, resource limitations, intelligence estimates, etc., made to determine their impact on the system. In addition, address the following specific trade-offs related to computer resources:

(Reprinted without change)

Downloaded from http://www.everyspec.com

f. Survivability/Vulnerability (including nuclear)

g. Reliability/Maintainability/Availability (R/M/A)

h. Electromagnetic Compatibility

i. Logistic Support Analysis to address, as appropriate, integrated logistics support including maintenance concept, support equipment concept, logistics support concept, maintenance, supply, software support facilities, etc. (MIL-STD-1388-1 and 2)

j. System Safety (emphasis shall be placed on system hazard analysis and identification of safety test requirements)

k. Securit;y

l. Human Factors

m. Transportability (including Packaging and Handling)

n. System Mass Properties

o. Standardization

p. Electronic Warfare

q. Value Engineering

r. System Growth Capability

s. Program Risk Analysis

t. Technical Performance Measurement Planning

u. Producibility Analysis and Manufacturing

v. Life Cycle Cost/Design to Cost Goals

w. Quality Assurance Program

x. Environmental Conditions (Temperature, Vibration, Shock, Humidity, etc).

y. Training and Training Support

z. Milestone Schedules

aa. Software Development Procedures

20.3.2 Results of significant trade studies, for example:

a. Sensitivity of selected mission requirements versus

Downloaded from http://www.everyspec.com

realistic performance parameters and cost estimates.

b. Operations design versus maintenance design, including support equipment impacts.

c. System centralization versus decentralization

d. Automated versus manual operation

e. Reliability/Maintainability/Availability

f. Commercially available items versus new developments

g. National Stock Number (NSN) items versus new development

h. Testability trade studies (Allocation of fault detection/isolation capabilities between elements of built-in test, on board/on-site fault detection/isolation subsystem, separate support equipment, and manual procedures)

i. Size and weight

j. Desired propagation characteristics versus reduction interference to other systems (optimum selection frequencies)

k. Performance/logistics trade studies

l. Life cycle cost reduction for different computer programming languages

m. Functional allocation between hardware, software, firmware and personnel/procedures

n. Life Cycle Cost/system performance trade studies to include sensitivity of performance parameters to cost.

o. Sensitivity of performance parameters versus cost

p. Cost versus performance

q. Design versus manufacturing consideration

r. Make versus buy

s. Software development schedule

t. On-equipment versus off-equipment maintenance tasks, including support equipment impacts

u. Common versus peculiar support equipment

20.3.3 Updated design requirements for operations/maintenance functions and items.

20.3.4 Updated requirements for manufacturing methods and processes.

Downloaded from http://www.everyspec.com

i. Maintenance related trade-off studies and findings (includes commercially available equipment, software fault diagnostic techniques)

j. Logistic cost impacts

k. Support procedures and tools for computer software which facilitate software modification, improvements, corrections and updates

l. Hardness critical items/processes

m. Support equipment concept.

20.3.12 System compliance with nuclear, non-nuclear and laser hardening requirements. High risk areas or design concepts requiring possible advances of the state-of-the-art as a result of survivability criteria shall be identified, and prepared approach(es) to the problem reviewed. Prepared test programs shall be reviewed for sufficiency and compatibility with the specified threat environment and existing simulation test facilities.

20.3.13 The optimization, traceability, completeness, and risks associated with the allocation technical requirements, and the adequacy of allocated system requirements as a basis for proceeding with the development of hardware and software configuration items. Include any available preliminary Software Requirements and Interface Requirements Specifications.

20.3.14 Manufacturing (HWCIs only).

20.3.14.1 Production feasibility and risk analyses addressed at the SRR shall be updated and expanded. This effort should review the progress made in reducing production risk and evaluate the risk remaining for consideration in the Full Scale Development Phase. Estimates of cost and schedule impacts shall be updated.

20.3.14.2 Review of the Production Capability Assessment shall include:

20.3.14.2.1 A review of production capability shall be accomplished which will constitute an assessment of the facilities, materials, methods, processes, equipment and skills necessary to perform the full scale development and production efforts. Identification of requirements to upgrade or develop manufacturing capabilities shall be made. Requirements for Manufacturing Technology (MANTECH) programs will also be identified as an element of this production assessment.

20.3.14.3 Present the management controls and the design/manufacturing engineering approach to assure that the equipment is producible.

Downloaded from http://www.everyspec.com

20.3.14.4 Present a review of trade-off studies for design requirements against the requirement for producibility, facilities, tooling, production test equipment, inspection, and capital equipment for intended production rates and volume.

20.3.14.5 The analysis, assessments and trade-off studies should recommend any additional special studies or development efforts as needed.

20.3.15. Engineering Data. Evaluate the contractor's drawing system, reviewing the drafting room manual, the preparation and review procedures, change control procedures, flowdown of requirements to subcontractors and vendors, and other aspects fundamental to the acceptability of Level 3 drawings. If available, review completed drawings from other programs or the normal company product line to determine compliance with the company procedures.

20.4 Post Review Action. After completing the SDR, the contractor shall publish and distribute copies of Review Minutes. The contracting agency officially acknowledges completion of the SDR as indicated in paragraph 4.2.4.

Downloaded from http://www.everyspec.com

quipment shall be made available for review by the contracting agency.

z. Firmware to be provided with the system: microprogram logic diagrams nd reprogramming/instruction translation algorithm descriptions, fabrication, ackaging (integration technology (e.g., LSI, MSI), device types (e.g., CMOS, MOS)), and special equipment and support software needed for developing, esting, and supporting the firmware.

aa. Life Cycle Cost Analysis

ab. Armament compatibility

ac. Corrosion prevention/control considerations

ad. Findings/Status of Quality Assurance Program

ae. Support equipment requirements.

0.2.2 CSCIs:

a. Functional flow. The computer software functional flow embodying all f the requirements allocated from the Software Requirements Specification and nterface Requirements Specification(s) to the individual Top-Level Computer ware Components (TLCSCs) of the CSCI.

b. Storage allocation data. This information shall be presented for ach CSCI as a whole, describing the manner in which available storage is llocated to individual TLCSCs. Timing, sequencing requirements, and relevant quipment constraints used in determining the allocation are to be included.

c. Control functions description. A description of the executive ontrol and start/recovery features for the CSCI shall be available, including ethod of initiating system operation and features enabling recovery from ystem malfunction.

d. CSCI structure. The contractor shall describe the top-level tructure of the CSCI, the reasons for choosing the components described, the evelopment methodology which will be used within the constraints of the vailable computer resources, and any support programs which will be required n order to develop/maintain the CSCI structure and allocation of data storage.

e. Security. An identification of unique security requirements and a escription of the techniques to be used for implementing and maintaining ecurity within the CSCI shall be provided.

rsedes page 35 of 4 June 1985

Downloaded from http://www.everyspec.com

f. Reentrancy. An identification of any reentrancy requirements and a description of the techniques for implementing reentrant rountines shall be available.

g. Computer software development facilities. The availability, adequacy, and planned utilization of the computer software development facilities shall be addressed.

h. Computer software development facility versus the operational system. The contractor shall provide information relative to unique design features which may exist in a TLCSC in order to allow use within the computer software development facility, but which will not exist in the TLCSC installed in the operational system. The contractor shall provide information on the design of support programs not explicitly required for the operational system but which will be generated to assist in the development of the CSCI(s). The contractor shall also provide details of the Software Development Library controls.

i. Development tools. The contractor shall describe any special simulation, data reduction, or utility tools that are not deliverable under the terms of the contract, but which are planned for use during software development.

j. Test tools. The contractor shall describe any special test systems, test data, data reduction tools, test computer software, or calibration and diagnostic software that are not deliverable under terms of the contract, but which are planned for use during product development.

k. Description and characteristics of commercially available computer resources, including any optional capabilities such as special features, interface units, special instructions, controls, formats, etc. Include limitations of commercially available equipment such as failure to meet human engineering, safety and maintainability requirements of the specification and identify deficiencies.

l. Existing documentation (technical orders, commercial manuals, etc.) for commercially available computer resources and copies of contractor specifications used to procure computer resources shall be made available for review by the contracting agency.

m. Support resources. The contractor shall describe those resources necessary to support the software and firmware during operational deployment of the system, such as operational and support hardware and software, personnel, special skills, human factors, configuration management, test, and facilities/space.

(Reprinted without change)

Downloaded from http://www.everyspec.com

n. Operation and support documents. The preliminary versions of the CSOM, SUM, CSDR, and CRISD shall be reviewed for technical content and compatability with the top-level design documentation.

o. Updated since the last review to all previously delivered software related CDRL items.

p. Review considerations applicable to 40.2.1 as appropriate.

40.2.3 Support Equipment (SE):

a. Review considerations applicable to paragraph 40.2.1 and 40.2.2 as appropriate.

b. Verify testability analysis results. For example, on repairable integrated circuit boards are test points avaliable so that failure can be isolated to the lowest level of repair (See Section 3 Definitions, for "Level of repair").

c. Verify that the Government furnished SE is planned to be used to the maximum extent possible.

d. Review progress of long-lead time SE items, identified through interim release and SE Requirements Document (SERD) procedures.

e. Review progress toward determining total SE requirements for installation, checkout, and test support requirements.

f. Review the reliability/maintainability/availability of support equipment items.

g. Identify logistic support requirements for support equipment items and rationale for their selection.

h. Review calibration requirements.

i. Describe technical manuals and data availability for support equipment.

j. Verify compatibility of proposed support equipment with the system maintenance concept.

k. If a Logistic Support Analysis (LSA) is not done, then review the results of SE trade-off studies for each alternative support concept. For existing SE and printed circuit boards testers, review Maintainability data resulting from the field use of these equipments. Review the cost difference between systems using single or multipurpose SE vs. proposed new SE. Examine technical feasibility in

(Reprinted without change)

Downloaded from http://www.everyspec.com

using existing, developmental, and proposed new SE. For mobile systems, review the mobility requirements of support equipment.

l. Review the relationship of the computer resources in the system/subsystem with those in Automatic Test Equipment (ATE). Relate this to the development of Built In Test Equipment (BITE) and try to reduce the need for complex supporting SE.

m. Verify on-equipment versus off-equipment maintenance task trade study results, including support equipment impacts.

n. Review updated list of required support equipment.

40.2.4 Engineering Data. Review Level 1 engineering drawings for ease of conversion to higher levels and, if available, review Level 2 and 3 drawings for compliance with requirements. The review of engineering data, as defined in paragraph 3.15, should consider the checklist items discussed in para 100.6, as properly tailored.

40.3 Evaluation of Electrical, Mechanical, and Logical Designs

40.3.1 HWCIs. The material of paragraph 40.2.1 above shall be evaluated to:

a. Determine that the preliminary detail design provides the capability of satisfying the performance characteristics paragraph of the HWCI Development specifications.

b. Estalbish compatibility of the HWCI operating characteristics in each mode with overall system design requirements if the HWCI is involved in multi-mode functions.

c. Establish the existence and nature of physical and functional interfaces between the HWCI and other items of equipment, computer software, and facilities.

40.3.2 CSCIs. The material of paragraph 40.2.2 above shall be evaluated to:

a. Determine whether all interfaces between the CSCI and all other configuration items both internal and external to the system meet the requirements of the Software Requirements Specification and Interface Requirements Specification(s).

b. Determine whether the top-level design embodies all the requirements of the Software Requirements Specification and Interface Requirements Specification(s).

Downloaded from http://www.everyspec.com

c. Determine whether the approved design methodology has been used for the top-level design.

d. Determine whether the appropriate Human Factors Engineering (HFE) principals have been incorporated in the design.

e. Determine whether timing and sizing constraints have been met throughout the top-level design.

f. Determine whether logic affecting system and nuclear safety has been incorporated in the design.

Downloaded from http://www.everyspec.com

(11) Survivability/Vulnerability (including nuclear)

(12) Producibility and Manufacturing

(13) Transportability, Packaging and handling

(14) Human Engineering and Biomedical Requirements (including Life Support and Crew Station Requirements)

(15) Standardization

(16) Design versus Logistics Trade-offs

(17) Support equipment requirements

d. Interface control drawings

e. Mock-ups, breadboards, and/or prototype hardware

f. Design analysis and test data

g. System Allocation Document for HWCI inclusion at each scheduled location.

h. Initial Manufacturing Readiness (for example, manufacturing engineering, tooling demonstrations, development and proofing of new materials, processes, methods, tooling, test equipment, procedures, reduction of manufacturing risks to acceptable levels).

i. Preliminary VECPs and/or formal VECPs

j. Life cycle costs

k. Detail design information on all firmware to be provided with the system.

l. Verify corrosion prevention/control considerations to insure materials have been chosen that will be compatible with operating environment.

m. Findings/Status of Quality Assurance Program

50.2.2 CSCIs.

a. Software Detailed Design, Data Base Design, and Interface Design Document(s). In cases where the CDR is conducted in increments, complete documents to support that increment shall be available.

b. Supporting documentation describing results of analyses, testing, etc., as mutually agreed by the contracting agency and the contractor.

Downloaded from http://www.everyspec.com

c. System Allocation Document for CSCI inclusion at each scheduled location.

d. Computer Resources Integrated Support Document.

e. Software Programmer's Manual

f. Firmware Support Manual

g. Progress on activities required by CSCI PDR (para 40.2.2).

h. Updated operation and support documents (CSOM, SUM, CSDM).

i. Schedules for remaining milestones.

j. Updates since the last review to all previously delivered software related CDRL items.

50.2.3 Support Equipment (SE):

a. Review requirements (paragraphs 50.2.1 and 50.2.2) for SE.

b. Verify maximum considerations GFE SE

c. Identify existing or potential SE provisioning problems

d. Determine qualitative and quantitative adequacy of provisioning drawings and data

e. Review reliability of SE

f. Review logistic support requirements for SE items

g. Review Calibration requirements

h. Review documentation for SE.

50.2.4. Engineering Data. Continuing from the results of the Preliminary Design Review (PDR), review engineering data as defined in para 3.15, as to suitability for intended use. The review should consider the checklist items discussed in para 100.6, as properly tailored.

50.3 Detailed Evaluation of Electrical, Mechanical, and Logical Designs

50.3.1 HWCIs. Detailed block diagrams, schematics, and logic diagrams shall be compared with interface control drawings to determine system compatibility. Analytical and available test data shall be reviewed to insure the hardware Development Specification has been satisfied.

Downloaded from http://www.everyspec.com

50.3.1.1 The contractor shall provide information on firmware which is included in commercially available equipment or to be included in equipment developed under the contract. Firmware in this context includes the microprocessor and associated sequence of micro-instructions necessary to perform the allocated tasks. As a minimum, the information presented during CDR shall provide

Downloaded from http://www.everyspec.com

70. Functional Configuration Audit.

70.1 General. The objective of the Functional Configuration Audit (FCA) shall be to verify that the configuration item's actual performance complies with its hardware Development or Software Requirements and Interface Requirements Specifications. Test data shall be reviewed to verify that the hardware or computer software performs as required by its functional/allocated configuration identification. For configuration items developed at Government expense, an FCA shall be a prerequisite to acceptance of the configuration item. For software, a technical understanding shall be reached on the validity and the degree of completeness of the Software Test Reports, and as appropriate, Computer System Operator's Manual (CSOM), Software User's Manual (SUM), and Computer System Diagnostic Manual (CSDM).

70.1.1 The FCA for a complex configuration item may be conducted on a progressive basis, when so specified by the contracting agency, throughout the configuration item's development and culminates at the completion of the qualification testing of the configuration item with a review of all discrepancies at the final FCA. The FCA shall be conducted on that configuration of the configuration item which is representative (prototype or preproduction) of the configuration to be released for production of the operational inventory quantities. When a prototype or preproduction article is not produced, the FCA shall be conducted on a first production article. For cases where configuration item qualification can only be determined through integrated system testing, FCA's for such configuration items will not be considered complete until completion of such integrated testing.

70.1.2 Recommendations of configuration item acceptance or non-acceptance to the local contract management agency are based upon and governed by procedures and requirements outlined in subsequent paragraphs.

70.1.3. Continuing with the results of the Critical Design Review (CDR), review engineering data as defined in para 3.15, as to the suitability for intended use. The review should consider the checklist items discussed in para 100.6, as properly tailored.

70.2 Contract Requirements

70.2.1 The schedules for the FCA shall be recorded on the configuration item development record by the contractor. A configuration item cannot be audited without the contracting agency authentication of the functional and allocated baseline. In addition, the contractor shall submit the final draft Product Specification for the configuration item to be audited to the contracting agency for review prior to FCA.

70.3 Contractor Responsibility

70.3.1 Prior to the FCA date (for configuration items to be audited), the contractor shall provide the following information to the contracting agency (this information shall be provided in addition to the general requirements of Section 4.):

Downloaded from http://www.everyspec.com

a. Contractor representation(the test manager should be in attendance).

b. Identification of items to be audited:

(1) Nomenclature

(2) Specification identification number

(3) Configuration item number

(4) Current listing of all deviations/waivers against the configuration item, either requested of, or approved by the contracting agency.

(5) Status of Test Program to test configured items with automatic test equipment (when applicable).

70.4 Procedures and Requirements

70.4.1 The contractor's test procedures and results shall be reviewed for compliance with specification requirements.

70.4.2 The following testing information shall be available for the FCA team.

a. Test plans, specifications, descriptions, procedures, and reports for the configuration item.

b. A complete list of successfully accomplished functional tests during which pre-acceptance data was recorded.

c. A complete list of successful functional tests if detailed test data are not recorded.

d. A complete list of functional tests required by the specification but not yet performed. (To be performed as a system or subsystem test).

e. Preproduction and production test results.

70.4.3 Testing accomplished with the approved test procedures and validated data (witnessed) shall be sufficient to insure configuration item performance as set forth in the specification Section 3 and meet the quality assurance provisions/qualification requirements contained in the specification Section 4.

70.4.4 For those performance parameters which cannot completely be verified during testing, adequate analysis or simulation shall have been accomplished. The results of the analysis or simulations will be sufficient to insure configuration item performance as outlined in the specification.

(Reprinted without change)

Downloaded from http://www.everyspec.com

70.4.5 Test reports, procedures, and data used by the FCA team shall be made a matter of record in the FCA minutes.

70.4.6 A list of the contractor's internal documentation (drawings) of the configuration item shall be reviewed to insure that the contractor has documented the physical configuration of the configuration item for which the test data are verified.

70.4.7 Drawings of HWCI parts which are to be provisioned should be selectively sampled to assure that test data essential to manufacturing are included on, or furnished with, the drawings.

70.4.8. Configuration Items (CIs) which fail to pass quality assurance test provisions are to be analyzed as to the cause of failure to pass. Appropriate corrections shall be made to both the CI and associated engineering data before a CI is subjected to requalification.

70.4.9 A checklist shall be developed which identifies documentation and hardware and computer software to be available and tasks to be accomplished at the FCA for the configuration item. See Pre-FCA checksheet.

70.4.10 Retests or additional tests shall be performed to assure compliance with paragraph 70.4.3.

70.4.11 Acknowledge accomplishment of partial completion of the FCA for those configuration items whose qualification is contingent upon completion of integrated systems testing.

70.4.12 For CSCIs the following additional requirements shall apply:

a. The contractor shall provide the FCA team with a briefing for each CSCI being audited and shall delineate the test results and findings for each CSCI. As a minimum, the discussion shall include CSCI requirements that were not met, including a proposed solution to each item, an account of the ECPs incorporated and tested as well as proposed, and a general presentation of the entire CSCI test effort delineating problem areas as well as accomplishments.

b. An audit of the formal test plans/descriptions/procedures shall be made and compared against the official test data. The results shall be checked for completeness and accuracy. Deficiencies shall be documented and made a part of the FCA minutes. Completion dates for all discrepancies shall be clearly established and documented.

c. An audit of the Software Test Reports shall be performed to validate that the reports are accurate and completely describe the CSCI tests.

Downloaded from http://www.everyspec.com

d. All ECPs that have been approved shall be reviewed to ensure that they have been technically incorporated and verified.

e. All updated to previously delivered documents shall be reviewed to ensure accuracy and consistency throughout the documentation set.

f. Preliminary and Critical Design Review minutes shall be examined to ensure that all findings have been incorporated and completed.

g. The interface requirements and the testing of these requirements shall be reviewed for CSCIs.

h. Review data base characteristics, storage allocation data and timing, and sequencing characteristics for compliance with specified requirements.

70.5 Post Audit Actions

70.5.1 After completion of the FCA, the contractor shall publish and distribute copies of FCA minutes. The contracting agency officially acknowledges completion of the FCA as indicated in paragraph 4.2.4.

70.5.2 The accomplishment of the FCA shall be recorded on the configuration item Development Record by the contractor.

(Reprinted without change)

Downloaded from http://www.everyspec.com

80. Physical Configuration Audit (PCA)

80.1 General. The Physical Configuration Audit (PCA) shall be the formal examination of the as-built version of a configuration item against its design documentation in order to establish the product baseline. After successful completion of the audit, all subsequent changes are processed by engineering change action. The PCA also determines that the acceptance testing requirements prescribed by the documentation is adequate for acceptance of production units of a configuration item by quality assurance activities. The PCA includes a detailed audit of engineering drawings, specifications, technical data and tests utilized in production of HWCIs and a detailed audit of design documentation, listings, and manuals for CSCIs. The review shall include an audit of the released engineering documentation and quality control records to make sure the as-build or as-coded configuration is reflected by this documentation. For software, the Software Product Specification and Version Description Document shall be a part of the PCA review.

80.1.1 The PCA shall be conducted on the first article of configuration items and those that are a reprocurement of a configuration item already in the inventory shall be identified and selected jointly by the contracting agency and the contractor. A PCA shall be conducted on the first configuration item to be delivered by a new contractor even though PCA was previously accomplished on the first article delivered by a different contractor.

80.1.2 Formal approval by the contracting agency of the configuration item Product specification, and the satisfactory completion of a PCA results in establishment of the product baseline.

80.1.3 Recommendations of configuration item acceptance or nonacceptance to the responsible contract administration office (CAO) are based upon and governed by procedures and requirements outlined in subsequent paragraphs.

80.1.4 A final review shall be made of all operation and support documents (i.e., Computer System Operator's Manual (CSMOM), Software User's Maual (SUM), Computer System Diagnostic Manual (CSDM), Software Programmer's Manual (SPM), Firmware Support Manual (FSM)) to check format, completeness, and conformance with applicable data item descriptions.

80.1.5. Continuing with the results of the Punctional Configuration Audit (PCA), review engineering data as defined in para 3.15, as to the suitability for intended use. The review should consider the checklist items discussed in para 100.6, as properly tailored.

80.2 Contract Requirements

80.2.1 The schedules for the PCA shall be recorded on the configuration item Development Record by the contractor. A current set of listings shall be provided for each CSCI being audited. The contractor shall submit the final draft of the

Downloaded from http://www.everyspec.com

product specification for the configuration item to be audited to the contracting agency for review prior to PCA.

80.3 Contractor Responsibility

80.3.1 The contractor shall provide the following information to the contracting agency (this information shall be provided in accordance with the general instructions of Section 4 and the contractural requirements):

a. Contractor representation (the test manager should be in attendance).

b. Identification of items to be accepted by:

(1) Nomenclature

(2) Specification Identification Number

(3) Configuration item Identifiers

(4) Serial Numbers

(5) Drawing and Part Numbers

(6) Identification Numbers

(7) Code Identification Numbers

(8) Software inventory numbering system

c. A list delineating all deviations/waivers against the configuration item either requested or contracting agency approved.

80.3.2 The PCA cannot be performed unless data pertinent to the configuration item being audited is provided to the PCA team at time of the audit. The contractor shall compile and make this information available for ready reference. Required information shall include:

a. Configuration item product specification.

b. A list delineating both approved and outstanding changes against the configuration item.

c. Complete shortage list.

d. Acceptance test procedures and associated test data.

e. Engineering drawing index including revision letters.

(Reprinted without change)

Downloaded from http://www.everyspec.com

non-complex system some reviews may not be required, or, if required, may be limited in Scope. The tailoring procedures discussed earlier should result either in the exclusion of MIL-STD-1521 or in a tailored MIL-STD-1521 that reflects a limited scope technical review effort. Conversely, in a very complex development the review process will increase in levels and numbers of reviews.

b. In addition to the above, the degree of application is dependent upon the configuration item state of development (example, new design vs. commercially available) or the degree of any modifications, if involved. For example: a newly developed item may require the majority of the review topics/items and audits, while a commercially available configuration item with the appropriate documentation, i.e., verified test results, specifications, drawings, etc. may require reviews or audits limited to its application to the program and its interfaces. In the case of modified designs one must consider the degree and effect of the modifications. Reviews and audits may be limited to the modifications and their interfaces.

100.5 Scheduling of Technical Reviews and Audits

The schedule for Technical Reviews and Audits is extremely important. If they are conducted too early, the item for review will not be adequately defined. Conversely, if the review is too late, the program commitments could have been made erroneously, and correction will be both difficult and costly. For planning purposes, a good method for scheduling technical reviews is to relate them to the documentation requirements. For example, schedule a PDR after the hardware Development Specification or Software Top Level Design Document and Software Test Plan are available, since the essence of the PDR is to assess the contractor's approach to meeting these requirements of these documents. Scheduling of audits are dependent not only on documentation availability but also on hardware/software availability, and the completion of the acceptance qualification tests. Table 1 contains a list of the primary documentation associated with each review or audit and the estimated time phasing:

100.6. Tailoring Guidance for Engineering Data Reviews. Engineering Data reviews are conducted as part of the formal design reviews/audits in MIL-STD-1521. Use Figure 5, Review Checklist for Engineering Data, to help prepare for and conduct these reviews and audits. Note discrepancies on Figure 6, Engineering Data Discrepancy Sheet. Because reviews and audits are successively more detailed, more items on the checklist will apply as the program progresses. When all reviews and audits are completed, all items on the tailored checklist should be accomplished.

Downloaded from http://www.everyspec.com

TABLE I
SCHEDULING REVIEWS AND AUDITS

Review	Time Phase	Primary Documentation
SRR	Usually accomplished in the Concept Exploration phase. However, may be used in other phases when the	Various analysis and trade study reports used to develop the system/segment

Downloaded from http://www.everyspec.com

110. Production Readiness Review (PRR)

110.1 For specific guidance, see AFSCR 84-2, Production Readiness Review.

(Reprinted without Change)

Downloaded from http://www.everyspec.com

REVIEW CHECKLIST FOR ENGINEERING DATA

I. The following questions and considerations should be used prior to conducting an engineering data review. These are suggested guidelines, and should be used as such.

II. Pre-briefing preparation:
- a. Answer these questions:
  1. What is the purpose of the Review?
  2. What does the Contract require?
  3. How will the drawings be used?
- b. Arrange briefings:
  1. The Contractor shall brief the team on contractual requirements and status.
  2. The Engineering Data Management Officer (EDMO) or Chairperson should brief the team on the review procedures.
  3. Discuss corrective action procedures.

III. The Data Review:
- a. Build the package:
  1. Select sample of top assembly drawings.
  2. Look at Parts List of the top assembly or major subassembly drawings.
  3. Are other subassembly drawings listed in the top parts list?
  4. Are all drawings listed in the top parts list available?
  5. Are all drawings listed in the subassembly parts list available?
  6. Is manufacturing planning documentation available?
- b. Examine the engineering data for the following:
  1. Is the drawing legible and suitable for reproduction?
  2. Are processes/specifications listed?
  3. Look at notes on all drawings. Are all notes understandable? Are notes clear and concise?
  4. Are peculiar symbols, abbreviations, etc, explained?
  5. Are all dimensions and tolerances shown?
  6. Is the material identified?
  7. Are any reports referenced? If so, are they supplied in the package?
  8. Are copies of non-government specifications supplied as part of the package?
  9. Correct use of limited rights legends (DAR/FAR)?
  10. Are control drawings (particularly Source and Specification Control) properly used and marked? (DOD-STD-100)
  11. Are hardness critical items and hardness critical process markings correct?
  12. Are electrostatic discharge sensitive (ESDS) symbology and cautions included, as appropriate?
  13. Have changes been incorporated as required in the contract?

Downloaded from http://www.everyspec.com

14. Are index and data lists available and correct?
15. Is there a distribution statement on each piece of engineering data?
16. Have specific marking requirements (MIL-STD-130) been defined?
17. Are acceptance test requirements included on all subassembly/detail drawings for items that might be spared separately by competitive reprocurement?
18. Is the proper engineering design information included for the level of drawing stated in the contract?
19. Could a military standard or specification be used in lieu of drawings?
20. Are applicable security classifications marked correctly?
21. Are the contractual requirements adequate?
22. Does the drawing package appear to be adequate to support the intended end use (i.e. logistics support, competitive reprocurement, etc)?

c. Record all deficiencies/discrepancies on the Engineering Data Discrepancy Sheet (see Figure 6) in sufficient detail to completely define the problem and action required for compliance.

At the end of the review, the EDMO (or Review Team Chief) collects all discrepancy sheets, signs them, and determines appropriate disposition. After resolution of discrepancies, the sheets will be filed in the Engineering Data Files.

Downloaded from http://www.everyspec.com

Sheet __ of __

FIGURE 6

_____
(PROGRAM NAME)

Engineering Data Discrepancy Sheet

(To be used with the Review Checklist)

PRIME AND SUBCONTRACTOR/VENDOR NAME:_____

TYPE OF REVIEW:_____

REVIEWER'S NAME	DRAWING/DOCUMENT NUMBER	REV	DATE

DISCREPANCIES

ACTION REQUIRED/COMPLIANCE DUE DATE_____

PROGRAM OFFICE EDMO (or Team Chief) Signature_____

AIR LOGISTICS EDMO SIGNATURE_____

ACTION AGENCY: ____Contractor ___Program Office
____Contract Administration Office ___Other

This block to be used by Action Agency

DISCREPANCIES CORRECTED BY: _____ _____
(Signature) (Date)

After resolution, return to the Program Office EDMO

Downloaded from http://www.everyspec.com

Custodian:
Air Force - 13

Preparing Activity:
Air Force - 13

Review Activity:
Air Force - 10, 11, 80, 85

(Project CMAN-0-006)

Bijlage X Handboek Werk in Uitvoering Landzijde

Rijkswaterstaat
Ministerie van Infrastructuur en Waterstaat

Bijlage X Handboek Werk in Uitvoering Landzijde

Bijlage bij Vraagspecificatie Proces

D&C Vervanging Verlichting Schipholtunnel
Zaaknummer: 31212908

RWS Bedrijfsvertrouwelijk



DEFINITIEF
26 november 2024
versie 2.4

Handboek Werk in Uitvoering Landzijde

Voor het Operationeel Gebied van Luchthaven Schiphol

Welcome to Amsterdam Airport

Schiphol

Inhoudsopgave

1 Inleiding **3**
1.1 Begrippen 3
1.2 Bijlagen 3
1.3 Contactpersonen 3

2 Procedure aanmelden werkzaamheden **4**

3 Uitgangspunten werk in uitvoering en verkeersmaatregelen **6**

4 Eisen bereikbaarheid tijdelijke situatie **8**

5 Eisen aan verkeersafzetting **11**

6 Eisen aan werkterrein en aannemersterrein **13**

7 Algemene voorwaarden tijdelijke verkeersmaatregelen Schiphol.

1 Inleiding

De wegen aan het landzijdige gedeelte van de Luchthaven Schiphol zijn primair bestemd voor de operationele en ondersteunende processen van Amsterdam Airport Schiphol.

In verband met enerzijds de groei van de Luchthaven en anderzijds het onderhoud aan de wegen en omgeving, wordt regelmatig een aanslag op de beschikbare capaciteit van de wegen gedaan.

Om ervoor te zorgen dat zowel de operationele processen als de bouwprocessen doorgang kunnen vinden is het noodzakelijk om globaal aan te geven waar bij het maken van de plannen en bestekken rekening mee moet worden gehouden. Op deze wijze kan reeds in een vroeg stadium inzicht worden verkregen in de te nemen (nood)maatregelen en de wijze waarop de processen beheersbaar kunnen blijven.

1.1 Begrippen

In dit Handboek worden meerder begrippen gebruikt die, om verwarring te voorkomen, hieronder worden toegelicht:

Aankomstpassage	Het wegenstelsel op aankomstniveau (maaiveld) voor de terminals bestaande uit de huidige A-, B-, C-, en D-baan.
Vertrekpassage	Het wegenstelsel op vertrekniveau (+1) voor de terminals (voorrijwegen) bestaande uit de huidige Dienstenbaan en de Particuliere baan.
Operationeel gebied	Verblijfsgebied, waarbij langzaam verkeer en snel verkeer mengen/kruisen.
Aannemersterrein	Het terrein waar de bouwkeet, parkeren aannemer, containers, opslag etc. staan. Het is mogelijk dat dit niet binnen of nabij het werkterrein is gelegen.
Werkterrein	Het terrein waar het werk wordt gerealiseerd.

1.2 Bijlagen

Bij dit document zijn de volgende bijlagen van toepassing:

- 20170119_Straatnamen_wijken_categorie_indeling

1.3 Contactpersonen

Afdeling	Functie	Naam	Telefoonnummer
LPD	Werkencoördinator Landzijde	P. van der Lans	0610913532
LPD	Wegbeheerder	P. van der Lans	0610913532

2 Procedure aanmelden werkzaamheden

2.01	Aanmelden werkzaamheden Luchthaven Schiphol
Eis	Werkzaamheden aan de openbare ruimte op Luchthaven Schiphol dienen te worden aangemeld middels een ICD vergunning aanvraag via Schiphol Intranet Een ICD-Works Landside (voormalige OVA-Landside) is een werkvergunning voor het uitvoeren van werkzaamheden op, of werkzaamheden met consequenties voor het Landzijdige deel van Schiphol. Om een ICD-Works Landside in behandeling te kunnen nemen is een beschrijving van de werkzaamheden, verwachte consequenties en documenten zoals verkeersmaatregelentekening en/of locatie benodigd. Hiervoor is een account noodzakelijk. Voor het aanvragen van een account en informatie over de aanvraag kunt u een email sturen naar OVAChange_support@schiphol.nl Als het account niet meer nodig is dan kan het worden afgemeld bij *OVAChange_support@schiphol.nl* De Werkencoördinator Landzijde beoordeelt deze aanvraag op diverse punten en zal indien nodig, naar aanvulling vragen. Als de aanvraag in status authorised staat kunnen de betreffende werkzaamheden in uitvoering genomen worden. De werken worden uitgevoerd volgens de **AlgemenevoorwaardenlijstTVMSchiphol** die als bijlage bij de icd aanvraag wordt toegevoegd
Toelichting	*Ter voorkoming van ongecontroleerde activiteiten, afsluitingen of maatregelen aan het wegensysteem op Schiphol met congestie en klachten tot gevolg.*

2.02	Verkeersmaatregelen opgemaakt door deskundig bureau
Eis	Bij werkzaamheden op of langs de weg, waarbij het nemen van verkeersmaatregelen noodzakelijk is, dienen de tijdelijke verkeersmaatregelen door een deskundig bureau te worden voorbereid en ontworpen.
Toelichting	- Tijdelijke verkeersmaatregelen dienen geplaatst te worden naar de richtlijnen van het CROW 96-b zijnde niet autosnelwegen

2.03	Procedure aanmelden projecten
Eis	Voor het aanmelden van projecten dient de volgende procedure in acht te worden genomen: a) Werkzaamheden dienen **uiterlijk 20 werkdagen** voor uitvoering, middels een icd vergunning aanvraag, aangemeld te zijn bij de Werkencoördinator Landzijde. b) De Werkencoördinator Landzijde toets en besluit, eventueel onder welke aanvullende voorwaarden de werkzaamheden kunnen worden uitgevoerd. Bij goedkeuring stelt de Werkencoördinator Landzijde de icd in status authorised. c) De tijdelijke verkeersmaatregelen die ingezet worden maken deel uit van het toetsingsproces. Deze wordt, namens de Gemeente Haarlemmermeer via een 'Toestemmingsformulier uitvoering werken en tijdelijke verkeersmaatregelen' afgegeven en maakt deel uit van de icd vergunning.

	d) Zodra een project gereed is worden de werkzaamheden afgemeld bij de Werkencoördinator Landzijde
Toelichting	-

2.04	Producteisen aanmelding projecten
Eis	De aanmelding voor projecten dient ten minste het volgende te bevatten: a) een logistiek draaiboek (BLVC) of werkplan met plan van aanpak van de in te zetten verkeersmaatregelen, bouwroutes, hijsmaterieel, werkterrein en impact op het operationele proces; b) overzichtstekeningen van de verkeersmaatregelen voor elke fase en elke tekening/fase voorzien van datum en tijden. c) een overall planning en faseringsplan.
Toelichting	-

2.05	Procedure aanmelden storingen en spoedeisende projecten
Eis	Voor het aanmelden van storingen en spoedeisende projecten dient de volgende procedure in acht te worden genomen: a) Plotseling opkomende werkzaamheden, die geen uitstel dulden, worden telefonisch gemeld bij Werkencoördinator Landzijde. b) De Werkencoördinator Landzijde geeft aan onder welke voorwaarden de werkzaamheden kunnen worden uitgevoerd. In eerste instantie mondeling, later bevestiging per e-mail. c) De Werkencoördinator Landzijde zorgt zo nodig voor de communicatie naar direct betrokkenen. d) Zodra de werkzaamheden gereed zijn worden deze afgemeld bij de Werkencoördinator Landzijde.
Toelichting	*Onder storingen en spoedeisende projecten wordt verstaan: ongeplande werkzaamheden als zijnde herstel- en reparatiewerkzaamheden die een impact hebben op het operationele proces en geen uitstel dulden.*

2.06	Producteisen aanmelding storingen en spoedeisende projecten
Eis	De aanmelding voor storingen en spoedeisende projecten dient ten minste het volgende te bevatten: a) plan van aanpak van werkzaamheden en eventuele verkeersmaatregelen. b) overzichtstekening van de verkeersmaatregelen indien nodig (te bepalen door de Werkencoördinator Landzijde).
Toelichting	*Bij spoed eerst mondeling, later bevestiging per e-mail.*

3 Uitgangspunten werk in uitvoering en verkeersmaatregelen

3.01	Behoud operationele processen
Eis	Het wegenstelsel op Luchthaven Schiphol dient de operationele processen van de Luchthaven Schiphol te ondersteunen en werkzaamheden en/of tijdelijke verkeersmaatregelen mogen die operationele processen niet onmogelijk maken, beperken of verstoren.
Toelichting	De wegen aan het landzijdige gedeelte van de Luchthaven Schiphol zijn primair bestemd voor de operationele en ondersteunende processen van Amsterdam Airport Schiphol.

3.02	Operatie heeft voorrang.
Eis	Het operationele proces van de Luchthaven Schiphol mag in beginsel niet worden verstoord.
Toelichting	Het verkeer op het landzijdige gedeelte van het Luchthaventerrein wordt in zijn geheel beschouwd als operationeel verkeer. Zij is immers altijd ondersteunend aan het luchthavenproces.

3.03	Veiligheid van weggebruikers en wegwerkers staan voorop.
Eis	De veiligheid van alle weggebruikers dient te worden gewaarborgd. Dit impliceert dat de genomen maatregelen nooit mogen leiden tot een onveilige situatie.
Toelichting	Hierbij geldt met name dat de genomen maatregel begrijpelijk en duidelijk moet zijn voor de weggebruiker. Het maken van manoeuvres die leiden tot onveilig weggedrag, met als oorzaak een onduidelijke of onveilige verkeerssituatie dient te worden vermeden.

3.04	Leidraad bij werken in uitvoering is Publicatie 96B van het CROW.
Eis	De Publicatie 96B van CROW dient in zijn geheel als leidraad voor verkeersmaatregelen en afzettingen te worden gebruikt.
Toelichting	In bijzondere gevallen kan in overleg met de Werkencoördinator Landzijde onder stringente voorwaarden van de richtlijn worden afgeweken, waarbij de veiligheid nimmer in het gedrang mag komen.

3.05	Voortijdige goedkeuring verkeersmaatregelen.
Eis	Alle voor het Werk benodigde verkeersmaatregelen en afzettingen dienen vooraf door de Werkencoördinator Landzijde van Schiphol te zijn goedgekeurd middels een getekend exemplaar van het “Toestemmingsformulier uitvoering werken en tijdelijke verkeersmaatregelen”,
Toelichting	

3.05a	Goedkeuring aanwezig op het werk.
Eis	Een goedkeuring (schriftelijk als digitaal) dient ten alle tijden aanwezig en aantoonbaar te zijn ten tijde van de uitvoering op het werk.

Toelichting	Zonder schriftelijke goedkeuring mogen geen verkeersmaatregelen en afzettingen geplaatst worden en mag niet met de aan deze verkeersmaatregelen hangende werkzaamheden worden gestart.

3.06	Beschikbare capaciteit afstemmen op gebruik
Eis	De beschikbare capaciteit op het wegenstelsel, in het bijzonder van Stroomwegen en Gebiedsontsluitingswegen, dient te worden afgestemd op het daadwerkelijke gebruik van de wegen ten behoeve van bouwlogistiek.
Toelichting	-

3.07	Functie wegen op Schiphol
Eis	De wegen op Luchthaven Schiphol dienen hun functie te behouden en mogen niet zonder meer buiten gebruik worden gesteld.
Toelichting	Tenzij de scope van het contract en de eisen voor specifieke wegvakken anders voorschrijft.

3.08	Alternatieve verbinding
Eis	In geval van het noodzakelijk uit gebruik moeten nemen van weggedeeltes of rijstroken van de wegen, busbanen, fietsverbindingen en voetgangersverbindingen dient eerst een alternatieve en getoetste verbinding in gebruik te zijn.
Toelichting	Tenzij de scope van het contract en de eisen voor specifieke verbindingen anders voorschrijft.

3.09	Bevoegdheid Wegbeheerder
Eis	De Wegbeheerder en/of diens plaatsvervanger heeft als verantwoordelijke van de openbare wegen op Luchthaven Schiphol te allen tijde de bevoegdheid om werkzaamheden en/of tijdelijke verkeersmaatregelen te doen stoppen en/of nader maatregelen te verlangen. Opgedragen acties door de Wegbeheerder of diens plaatsvervanger dienen ter stond opgevolgd te worden.
Toelichting	-

4 Eisen bereikbaarheid tijdelijke situatie

4.01	Waarborgen bereikbaarheid van alle locaties op Schiphol.
Eis	Alle gebouwen, faciliteiten en opstelplaatsen hulpdiensten op Luchthaven Schiphol dienen altijd voor voetgangers, hulpverleningsdiensten en leveranciers bereikbaar te zijn.
Toelichting	*De tijdelijke maatregelen dienen zodanig te worden uitgevoerd dat de bereikbaarheid voor met name voetgangers op een deugdelijke wijze wordt gegarandeerd. (bijvoorbeeld toepassen van loopschotten of industrieplaten)*

4.02	Waarborgen bereikbaarheid Doorlaatposten
Eis	De Doorlaatposten op Luchthaven Schiphol dienen te allen tijde beschikbaar te zijn voor hulpdiensten, Douane en Kmar, dan wel in overeenstemming met de Werkencoördinator Landzijde voor alternatieve bereikbaarheid van de Doorlaatpost.
Toelichting	-

4.03	-
Eis	-
Toelichting	-

4.04	Niet afsluiten Stroomwegen en Gebiedsontsluitingswegen
Eis	De Stroomwegen en Gebiedsontsluitingswegen mogen nimmer totaal afgesloten worden.
Toelichting	*Tenzij de scope van het contract en de eisen voor specifieke verbindingen anders voorschrijft.*

4.05	Tijdslots wegen
Eis	De wegen op Schiphol-Centrum mogen niet buiten gebruik worden genomen gedurende de maanden april t/m september.
Toelichting	*Tenzij de scope van het contract en de eisen voor specifieke verbindingen anders voorschrijft.*

4.06	Tijdslots wegen
Eis	"De wegen op Schiphol-Centrum mogen binnen de volgende tijdslots per wegcategorie in capaciteit verminderd worden (niet zijnde afsluitingen): - Stroomwegen dagelijks tussen 23.00 en 05.00 uur. - Gebiedsontsluitingswegen dagelijks tussen 21.00 en 05.00 uur. - Erftoegangswegen: i.o.m werken coördinator Landside - Vertrekpassage: in de maanden november tot en met april dagelijks tussen 22.00 en 05.00 uur. - Aankomstpassage: A-baan dagelijks tussen 23.00 en 05.00 uur. B-baan dagelijks tussen 23:00 en 05.00 uur.

	C-baan in de maanden oktober tot en met maart dagelijks tussen 20.00 en 08.00 uur, en in de maanden april tot en met september dagelijks tussen 23.00 en 07.00 uur D-baan dagelijks tussen 23.00 en 07.00 uur. In uitzonderlijke gevallen kan hier van af geweken worden indien dit noodzakelijk wordt geacht. Een en ander in nauw overleg met de Werkencoördinator Landzijde.
Toelichting	-

4.07	Tijdslots wegen
Eis	Voor de categorie van de betreffende wegen op Luchthaven Schiphol dient het overzicht in **Bijlage A** aangehouden te worden.
Toelichting	*Het overzicht in **bijlage A** betreft een dynamisch document welke in beheer is bij ASM in samenwerking met OPS. Periodiek en bij grote wijzigingen wordt dit overzicht geactualiseerd. Informatie hieromtrent bij de Werkencoördinator Landzijde*

4.08	Tijdslots Parkeergarages
Eis	De toegangen en uitgangen van de parkeergarages mogen tussen 22.00 en 06.00 uur in operationeel aantal poorten gehalveerd worden.
Toelichting	In uitzonderlijke gevallen kan hier van af geweken worden indien dit noodzakelijk wordt geacht. Een en ander in nauw overleg met de Werken coördinator Landzijde

4.09	Duur van tijdelijke verkeersmaatregelen
Eis	De 'tijdelijke verkeersmaatregelen' mogen op Luchthaven Schiphol maximaal 4 maanden van toepassing zijn. Bij langer dan deze 4 maanden dienen de verkeersmaatregelen geïntegreerd en afgestemd zijn op het bestaande verkeersmanagement in zowel inrichting, capaciteit en wayfinding.
Toelichting	*Verkeersmaatregelen die langer dan de gestelde periode van toepassing zijn hebben geen 'tijdelijk' karakter en behoeven mogelijk een Verkeersbesluit. Gele bewegwijzering zal dan vervangen moeten worden door blauw bewegwijzering.*

4.10	Tijdelijk verplaatsen van faciliteiten en objecten
Eis	Het als gevolg van werkzaamheden en tijdelijke verkeersmaatregelen blokkeren of verwijderen van faciliteiten en objecten dienen deze naar een nabij gelegen bereikbare locatie te worden verplaatst of opgevangen. Locatie wordt i.o.m Werken Coördinator Landside bepaalt
Toelichting	*Bijvoorbeeld bushaltes, fietsenstalling, motorstalling, opstelplaatsen van hulpdiensten, brandkranen, etc.*

4.11	OV-busdiensten
Eis	-
Toelichting	-

4.12	Bereikbaarheid en beschikbaarheid parkeercapaciteit
Eis	De parkeercapaciteit op Schiphol-Centrum mag niet ten koste gaan van de Werkzaamheden, dan wel in overeenstemming met de Werkencoördinator Landzijde voor alternatieven of uitzonderingsgevallen.

Toelichting	*De parkeercapaciteit op Schiphol-Centrum is reeds schaars.*

5 Eisen aan verkeersafzetting

5.01	Informeren weggebruiker
Eis	De tijdelijke verkeersmaatregelen dienen door middel van informatieborden, tijdelijke bewegwijzering en/of verkeersregelaars de weggebruikers te informeren over de werkzaamheden, omleidingsroutes en het niet kunnen gebruiken van navigatiesystemen.
Toelichting	Tijdelijke verkeersmaatregelen dienen geplaatst te worden naar de richtlijnen van het CROW 96-b zijnde niet autosnelwegen

5.02	Uitvoering bebording
Eis	De uitvoering van de tijdelijke bebording dienen conform het RVV 1990 c.q. overeenkomstig de richtlijnen voor bebakening niet-autosnelwegen (WIU-serie) te zijn, zowel voor wat betreft uitvoering als maatvoering.
Toelichting	-

5.03	Plaatsing afzetting
Eis	Het afzettingsmateriaal dient zorgvuldig en stabiel geplaatst te worden, waarbij er zoveel mogelijk voor wordt gezorgd, dat de gebruikte palen recht staan en de borden haaks op de rijrichting staan.
Toelichting	-

5.04	Inspecteren afzetting
Eis	Het afzettingsmateriaal dient dagelijks te worden geïnspecteerd op gebreken, beschadigingen en plaatsing en indien nodig te worden aangepast/hersteld.
Toelichting	-

5.05	Zichtbaarheid afzetting
Eis	Het afzettingsmateriaal dient zowel bij daglicht als in donker duidelijk en tijdig zichtbaar te zijn voor de weggebruiker. Eventueel dient extra verlichting te worden aangebracht.
Toelichting	-

5.06	Reflecterende afzettingsmateriaal en bebording
Eis	Al het afzettingsmateriaal en de tijdelijke bebording dient te zijn voorzien van reflecterend materiaal (minimaal klasse 2). Gemoffeld of geschilderd afzettingsmateriaal of tijdelijke bebording is niet toegestaan.
Toelichting	-

5.07	Wegdraaien verkeersmaatregelen
Eis	In perioden dat niet zichtbaar gewerkt (*maar het werk nog niet is afgerond*) worden de maatregelen of verwijzingen, die dan niet meer van toepassing zijn zodanig gedraaid, dat het voor het verkeer duidelijk is dat de normale verkeerssituatie weer van kracht is.

	De al geldende verkeerborden, maatregelen en verwijzingen die in de verkeersruimte van het aangewezen werkgebied vallen en conflicterend zijn met de tijdelijke maatregelen, dienen optisch onttrokken te worden (dicht). Na einde van de tijdelijke maatregelen dienen deze verkeerborden, maatregelen en verwijzingen weer “open” gezet te worden
Toelichting	

5.08	Verwijderen verkeersmaatregelen einde werk
Eis	**Direct na afloop van de werkzaamheden dienen alle betreffende tijdelijke verkeersmaatregelen z.s.m. te worden verwijderd.**
Toelichting	-

5.09	Afzetting trottoirs en fietspaden
Eis	Bij graafwerkzaamheden in trottoirs en/of fietspaden dient het werkgebied geheel afgezet te worden door middel van geschakelde dranghekken.
Toelichting	-

5.10	Geen gebruik afzetlint
Eis	Het gebruik van afzetlint is niet toegestaan
Toelichting	-

6 Eisen aan werkterrein en aannemersterrein

6.01	Veiligheid Werkterrein en Aannemersterrein
Eis	De veiligheid binnen en rondom de Werkterreinen en Aannemersterreinen dienen altijd te worden gewaarborgd. Dit is de verantwoordelijkheid van de aannemer. Voor wat betreft de veiligheid buiten het werkgebied heeft de werken coördinator toetsende rol.
Toelichting	Veiligheid zowel tijdens als buiten de werktijden voor weggebruikers en werknemers.

6.02	Afzetting Werkterrein binnen Operationeel gebied
Eis	Het Werkterrein binnen het Operationeel gebied dient te worden afgezet met bouwhekken en in afstemming met de Werkencoördinator Landzijde voorzien van gaasdoek. Van gaasdoek kan worden afgeweken als het plaatsen van bouwhekken leidt tot gevaarlijke verkeerssituaties.
Toelichting	Doel van bouwhekken met gaasdoek is bieden van bescherming en het onttrekken van zicht op de bouwplaats. Echter zijn ze windgevoelig. Derhalve in afstemming.

6.03	Afzetting Aannemersterrein
Eis	Het Aannemersterrein dient te worden afgezet met bouwhekken en in afstemming met de Werkencoördinator Landzijde voorzien van gaasdoek. Van gaasdoek kan worden afgeweken als het plaatsen van bouwhekken leidt tot gevaarlijke verkeerssituaties.
Toelichting	Doel van bouwhekken met gaasdoek is bieden van bescherming en het onttrekken van zicht op de bouwplaats. Echter zijn ze windgevoelig. Derhalve in afstemming.

6.04	Afzetting Werkterrein en/of Aannemersterrein nabij terminal
Eis	De Werken Coördinator Landside kan eisen dat het Werkterrein en/of Aannemersterrein in de omgeving van de Terminals met houten schotten afgezet dient te worden met minimaal eenzelfde hoogte als bouwhekken.
Toelichting	-

6.05	Toegepaste bouwhekken en houten schotten
Eis	De toegepaste bouwhekken en houten schotten dienen: - een veilige, representatieve, robuuste en stevige scheiding te vormen met de openbare ruimte; - het Werkterrein en Aannemersterrein af te schermen tegen onbevoegden; - de omgeving te beschermen tegen onveilige situaties die samenhangen met werkzaamheden.
Toelichting	-

6.06	Voorkomen en beperken van overlast
Eis	Overlast naar de omgeving door werkzaamheden dient te worden voorkomen dan wel te worden beperkt.

Toelichting	Bijvoorbeeld overlast door verlichting, geluid, trillingen, stof, stank, etc.

6.07	Werken binnen het Werkterrein
Eis	Alle werkzaamheden en laden lossen dienen zo veel mogelijk binnen het Werkterrein plaats te vinden.
Toelichting	Bij afwijking dient dit te zijn overlegd met Werken Coördinator Landside

6.08	Activiteiten binnen het Aannemersterrein
Eis	Alle keten, parkeren, opslag, laden en lossen etc. dienen zo veel als mogelijk plaats te vinden binnen het Aannemersterrein.
Toelichting	Bij afwijking dient dit te zijn overlegd met Werken Coördinator Landside

6.09	Ontsluiting van Werkterrein en/of Aannemersterrein
Eis	De ontsluiting van het Werkterrein en/of Aannemersterrein dient zo veel als mogelijk zodanig te zijn ingericht dat bouwverkeer vooruit op- en afrijd.
Toelichting	Bij afwijking dient dit te zijn overlegd met Werken Coördinator Landside

6.10	Capaciteit ontsluiting Werkterrein en/of Aannemersterrein
Eis	De capaciteit van de ontsluiting van het Werkterrein en/of Aannemersterrein is afgestemd op het verwachte bouwverkeer in relatie tot het verkeer op de aansluitende wegen.
Toelichting	De ontsluiting van het Werkterrein en/of Aannemersterrein moet ingericht zijn om het aantal verwachte vrachtwagens te kunnen afwikkelen.

6.11	Opstelruimte toegang tot Werkterrein
Eis	De toegang tot het Werkterrein dient ruimte te bieden voor het opstellen van tenminste één vrachtwagen zodat er geen opstoppingen ontstaan op de aansluitende wegen.
Toelichting	Indien van toepassing. Bij afwijking dient dit te zijn overlegd met Werken Coördinator Landside

7 Algemene voorwaarden tijdelijke verkeersmaatregelen Schiphol

Informeren

- u informeert de directe omgeving tenminste 20 dagen vóór aanvang werkzaamheden over de aard van het werk,
- u plaatst minimaal 14 dagen vóór start werkzaamheden vooraankondigingsborden;
- indien de werkzaamheden eerder klaar zijn dan de afgesproken einddatum, dient u dit te melden bij de operationeel coördinator werken Schiphol
- u dient bij grote en/of gefaseerde werkzaamheden wekelijks een update van de werkzaamheden te versturen naar de operationeel coördinator werken Schiphol
- u dient uw werkzaamheden af te stemmen met bedrijven waarvan de toegang tot hun parkeerplaats en/of bedrijf beperkt of niet toegankelijk is;

Onttrekken van parkeerplaatsen

- indien u parkeerplaatsen onttrekt, dient u minimaal 14 dagen van tevoren, waarop u aangeeft dat een parkeerplaats voor de duur van x komt te vervallen;
- u dient voor het parkeerverbod gebruik te maken van een E04 bord;
- indien u gebruik maakt van een onderbord met ondertekst “wegsleepregeling”, dan bent u zelf verantwoordelijk voor het wegslepen;

Veiligheid

- u dient te allen tijde 3,5 meter doorrijdbreedte naast het werkvak te garanderen voor het passeren van nood- en hulpdiensten en lijnbussen, tenzij anders overeengekomen met deh (deze voorwaarde geldt niet bij wegafsluitingen);
- nood- en hulpdiensten moeten ten alle tijden het werkvak kunnen passeren, tenzij anders is overeengekomen met de operationeel coördinator werken Schiphol;
- indien u werkzaamheden uitvoert nabij of direct naast nooduitgang(en) en andere vluchtwegen van naastgelegen gebouwen/percelen, dient u deze ten alle tijden vrij van obstakels te houden;
- u dient ervoor te zorgen dat de werklocatie bereikbaar blijft voor nood- en hulpdiensten middels een verharde ondergrond;
- u dient ervoor te zorgen dat locaties die alleen bereikbaar zijn via het werkvak (o.a. in- en/uitritten bedrijven) bereikbaar blijven voor nood- en hulpdiensten middels een verharde ondergrond;
- indien u werkzaamheden uitvoert in de nabijheid van essentiële voorzieningen moet de toegankelijkheid en bereikbaarheid gegarandeerd worden;
- u dient altijd minimaal 3 mtr afstand te behouden tot hekwerk die aan Airside grenst;

Omgeving

- u dient bij eventuele schade aan de openbare ruimte dit zelf te herstellen. Schiphol kan hiervoor niet aansprakelijk worden gesteld, tenzij anders bepaald;
- u dient het terrein/omgeving schoon en netjes achter te laten na afloop van de werkzaamheden;
- indien u gebruikt maakt van rijplaten waar de voetgangers overheen lopen, houdt u deze dagelijks schoon en veilig. De rijplaten moeten van kunststof zijn;
- indien u bouwhekken plaatst, controleert u dagelijks of deze goed verankerd zijn en zorgt u ervoor dat de deze veilig staan;
- indien u geen voorschouw doet, zijn alle ontstane schades voor uw rekening;

- het ophalen van huisvuil en bedrijfsafval wijzigt niet; de aannemer draagt zorg voor locaties waar centraal rolcontainers kunnen worden aangeboden;
- u dient openbare voorzieningen, zoals onder andere brievenbussen, prullenbakken, bedrijfsverzamelpunten (in geval van ontruiming) en dergelijke bereikbaar te houden of tijdelijk te verplaatsen;

Tijdelijke verkeersmaatregelen

- u plaatst de tijdelijke verkeersmaatregelen conform de goedgekeurde TVM- tekening(en);
- de toe te passen tijdelijke verkeersmaatregelen dienen te voldoen aan CROW-publicatie 527 'Maatregelen op niet-autosnelwegen - werk in uitvoering 96b 2020', tenzij anders is overeengekomen met de operationeel coördinator werken Schiphol;
- de werkzaamheden vinden uitsluitend doordeweeks plaats buiten de geldende spitstijden, namelijk van 09.30 uur -15.30 uur, tenzij anders is overeengekomen met de operationeel coördinator werken Schiphol;
- indien blijkt dat u extra verkeersmaatregelen moet plaatsen/inzetten t.b.v. de verkeersveiligheid en/of doorstroming van het verkeer, wordt de (eind)nota vergoed door de uitvoerende partij en niet door Schiphol;
- u dient ervoor te zorgen dat de tijdelijke verkeersmaatregelen na afloop van de werkzaamheden/ fasering van de openbare weg zijn en er regulier doorgang is voor alle weggebruikers. Indien mogelijk, afhankelijk van de werkzaamheden, dient u buiten de afgesproken werktijden uw maatregelen (deels) van de weg te halen;
- u loopt regelmatig de tijdelijke verkeersmaatregelen na of deze nog goed staan;
- u mag de tijdelijke bebording niet binnen een straal van 1 meter bij openbare verlichting/verkeerslichten of kasten plaatsen. Bewegwijzeringsborden en verkeersborden alleen afplakken met goedgekeurde zwarte afdektape (Nitto SPV3103H tape of gelijkwaardig);

Inzet verkeersregelaars

- u gebruikt uitsluitend beroepsmatige (gecertificeerde) verkeersregelaars;
- u dient de aanwezige verkeersregelaars duidelijke instructies mee te geven. De posities van de verkeersregelaars moeten te allen tijde bemand blijven. Bij pauzes en/of calamiteit(en) moeten zij vervangen worden door een andere collega verkeersregelaar/ coördinator verkeersregelaar;
- indien u wegen afsluit dienen de verkeersregelaars het werkgebied goed kennen, zodat zij iedereen goed kunnen informeren;

Werken nabij een VRI, brug of spoorwegovergang

- u dient de detectielussen vrij van voertuigen en materieel te houden. Bij twijfel kunt u om een VRI-tekening vragen. Indien vorengenoemde onvermijdelijk is, moet u dit spoedig aangeven, zodat de VRI gedurende het werk uitgezet kan worden;
- u dient altijd afstemming te zoeken met de VRI-beheerder bij asfaltwerkzaamheden en graafwerkzaamheden in de berm om schade te voorkomen en in geval van schade deze snel weer te kunnen laten herstellen;
- u dient ervoor te zorgen dat kruispunt(en), spoorwegovergang(en) en/of beweegbare delen van de brug vrij blijft van stilstaande voertuigen;
- regulier goederenvervoer over de weg mag maximaal 50 ton wegen (tenzij bebording anders aangeeft). Zwaarder dan dat brengt schade aan wegdek, bruggen en viaducten;

Materieel, materialen & opslag

- opslag van materieel en materialen, dient u af te stemmen met de werken coördinator Schiphol;
- u plaatst rijplaten om de ondergrond te verstevigen in de berm waar u uw materieel opstelt;
- de container dient duidelijk zichtbaar te zijn en mag niet uitsteken op de rijbaan;

- de container dient geplaatst te worden in één parkeervak of in de berm, maar mag zich niet bevinden op de rijbaan;
- de container is voorzien van markeringen conform de richtlijnen van het CROW;
- de container is voorzien van icd nr, naam en telefoonnummer van de eigenaar en/of gebruiker;
- de container bevat geen gevaarlijke of licht-ontvlambare stoffen, kadavers of huishoudelijk afval;
- u dient ervoor te zorgen dat de wagen die de container aflevert stapvoets en onder begeleiding van een verkeersregelaar de container gaat laden en lossen;
- ten tijde van het gebruik, plaatsen en ophalen van de container, houdt u rekening met het eventueel aanrijden van nood- en hulpdiensten en/of het openbaar vervoer. U borgt hierbij tevens de doorgang voor het overig verkeer;

Hijswerkzaamheden

- de last van de kraan mag niet over de openbare weg draaien;
- u dient ervoor te zorgen dat het voor gemotoriseerd verkeer, fietsers alsmede voetgangers onmogelijk is om tijdens de hijswerkzaamheden onder de hijslast te kunnen komen;
- u maakt gebruik van stempelplaten, om beschadiging aan openbare grond én instabiliteit te voorkomen;
- u houdt rekening met veiligheidsaspecten, zoals voldoende omgevingscommunicatie, het met de machine of last raken van obstakels en het uit de hijsgereedschappen vallen van lasten of delen ervan;

Overig

- u bent zelf verantwoordelijk voor het aanvragen van de juiste ontheffingen/vergunningen/toestemmingen anders dan de tijdelijke verkeersmaatregelen;
- u dient altijd de icd vergunning bij u te hebben, hetzij digitaal of hard copy, kunt u de icd vergunning niet tonen wordt het werk stilgelegd;
- Op Schiphol is het gebruik van afzetlint als afzetting van een werkplek of bouwgebied ten strengste verboden.

Bijlage Y Coördinatie van voorgeschreven Zelfstandige Hulppersonen

Y.1. Eisen aan coördinatie

Y.1.1 Algemeen

1.1.1 De Opdrachtnemer dient de Werkzaamheden met betrekking tot de coördinatie te verrichten, zodanig dat het werk en de werkzaamheden van voorgeschreven Zelfstandige Hulppersonen, worden afgestemd op de Werkzaamheden die voortvloeien uit de Overeenkomst. De Opdrachtnemer dient zorg te dragen dat de Werkzaamheden en het werk en de werkzaamheden van voorgeschreven Zelfstandige Hulppersonen op een tijdige, doelmatige, veilige, publieksgerichte en een voor de Opdrachtgever economisch meest verantwoorde wijze worden gerealiseerd en gecommuniceerd.

B-1.1.2 In lid Y.2 is een overzicht weergegeven van voorgeschreven Zelfstandige Hulppersonen waarvoor de Opdrachtnemer Werkzaamheden dient te verrichten met betrekking tot coördinatie van werken en werkzaamheden.

1.1.3 De Opdrachtnemer dient de Opdrachtgever met bekwame spoed te informeren indien de Opdrachtnemer niet kan voldoen aan de coördinatieverplichting door toedoen van een voorgeschreven Zelfstandige Hulppersoon.

Y.1.2 Opstellen plan coördinatie

1.2.1 De Opdrachtnemer dient een plan voor de coördinatie van werk en werkzaamheden door voorgeschreven Zelfstandige Hulppersonen op te stellen en hieraan invulling te geven, zodanig dat voldaan wordt aan de eisen die voortvloeien uit de Overeenkomst.

1.2.2 De Opdrachtnemer dient in het plan “Coördinatie van werk en werkzaamheden door voorgeschreven Zelfstandige Hulppersonen” ten minste uit te werken:

a. toegang verschaffen tot en begeleiding in het Areaal;
b. coördinatie Veiligheid en Gezondheid (V&G coördinatie);
c. coördinatie elektrotechnische werkzaamheden;
d. coördinatie cybersecurity werkzaamheden;
e. uit en in bedrijf nemen van installaties of objecten;
f. communicatie met beherend, begeleidend en bedienend personeel;
g. coördinatie van werkvergunningen, ontheffingen, beschikkingen en/of toestemmingen
h. coördinatie van testen binnen het tunnelareaal.

Y.1.3 Toegang verschaffen en begeleiding in het Areaal

1.3.1 De Opdrachtnemer dient de Werkzaamheden te verrichten voor het verschaffen van toegang tot en het begeleiden van voorgeschreven Zelfstandige Hulppersonen op objecten en terreinen in het Areaal.

1.3.2 De Opdrachtnemer dient de Werkzaamheden te verrichten voor het (in bruikleen) verstrekken en beheren van middelen die toegang geven tot objecten en terreinen in het Areaal.

1.3.3 De Opdrachtnemer dient onbevoegden te gelasten objecten of terreinen c.q. het Areaal te verlaten en zich te vervoegen bij de Opdrachtgever.

1.3.4 De Opdrachtnemer dient nadere object specifieke veiligheidsinstructies aan voorgeschreven Zelfstandige Hulppersonen te verzorgen, voorafgaand aan de uitvoering van werkzaamheden door voorgeschreven Zelfstandige Hulppersonen.

Y.1.4 Veiligheid en gezondheid

1.4.2 De Opdrachtnemer dient de medewerkers van voorgeschreven Zelfstandige Hulppersonen die onveilig handelen of een onveilige situatie creëren, te gelasten de onveilige handeling of situatie per direct op te heffen dan wel te staken. Indien de aanwijzing niet wordt opgevolgd, dan dient de Opdrachtnemer dit direct ter kennis te brengen van de Opdrachtgever.

Y.1.5 Cybersecurity werkzaamheden

1.5.1 De Opdrachtnemer dient de Werkzaamheden met betrekking tot de coördinatie van cybersecuritywerkzaamheden te verrichten, zodanig dat de ICT- en IA geen verhoogd risico lopen met betrekking tot cybersecurity.

Y.1.6 Elektrotechnische werkzaamheden

1.6.1 De Opdrachtnemer dient de Werkzaamheden met betrekking tot de coördinatie van elektrotechnische werkzaamheden te verrichten, zodanig dat deze op een veilige wijze en conform bijlage B “Integraal Veiligheidsplan” bij de Vraagspecificatie verlopen.

Y.1.7 Veiligstellen en uit- en inbedrijfname van objecten en installaties

1.7.1 De Opdrachtnemer dient de Werkzaamheden met betrekking tot het veiligstellen en/of de uit- en inbedrijfname van objecten en installaties te verrichten, ten behoeve van de Opdrachtnemer, inclusief voorgeschreven Zelfstandige Hulppersonen.

Y.1.8 Communicatie met beherend, begeleidend en bedienend personeel

1.8.1 De Opdrachtnemer dient de Werkzaamheden met betrekking tot communicatie over werkzaamheden met beherend, begeleidend en bedienend personeel van de Opdrachtgever te verrichten, zodanig dat deze te allen tijde hun rol en verantwoordelijkheid kunnen vervullen.

1.8.2 De Opdrachtnemer dient de Werkzaamheden met betrekking tot communicatie te verrichten, zodanig dat ten minste invulling wordt gegeven aan:

a. Het, indien noodzakelijk, betrekken van beherend en/of begeleidend personeel tijdens voorbereiding van werkzaamheden en/of Werkzaamheden;
b. het melden aan de ter plaatse bevoegde regioverkeersleider en bedienend personeel van aanwezigheid van medewerkers van de Opdrachtnemer,

inclusief voorgeschreven Zelfstandige Hulppersonen bij betreding van objecten.

1.8.3 Geplande Werkzaamheden van de Opdrachtnemer, inclusief voorgeschreven Zelfstandige Hulppersonen dienen 1 week voorafgaand aan de Werkzaamheden gemeld te worden aan de bevoegde regioverkeersleider door middel van een e-mailbericht.

1.8.4 Alle communicatie voortkomend uit de coördinatieverplichting dient verzorgd te worden door de sleutelfunctionaris als bedoeld in §2.3 (IV053) van de Vraagspecificatie Proces.

Y.1.9 Aanvraag en afgifte (werk)vergunningen, ontheffingen, beschikkingen en/of toestemmingen

1.9.1 De Opdrachtnemer dient de Werkzaamheden met betrekking tot de coördinatie van de aanvraag en afgifte van (werk)vergunningen, ontheffingen, beschikkingen en/of toestemmingen te verrichten zodanig dat de voortgang van de werkzaamheden niet wordt belemmerd.

1.9.2 De Opdrachtnemer dient de Werkzaamheden met betrekking tot de coördinatie van aanvraag en afgifte van publiekrechtelijke en privaatrechtelijke toestemmingen te verrichten zodanig dat ten minste invulling gegeven wordt aan het op verzoek van de Opdrachtgever:

a. beoordelen van de bevoegdheid, juistheid en volledigheid van de aanvraag;
b. verifiëren of de aanvraag conform de coördinatieafspraken is;
c. ter kennis brengen van de Opdrachtgever van de bevindingen met betrekking tot de aanvraag;
d. adviseren van de Opdrachtgever met betrekking tot verlenen van het aangevraagde.

B-1.9.3 De Opdrachtgever is te allen tijde als bevoegde de partij die vergunningen, ontheffingen, beschikkingen en/of toestemmingen afgeeft.

Y.1.10 Testen binnen het tunnelareaal

1.10.1 De Opdrachtnemer dient de Werkzaamheden met betrekking tot de coördinatie van testwerkzaamheden te verrichten, zodanig dat het Functioneren en Presteren van de gehele keten binnen het tunnelareaal is gewaarborgd.

Y.2. Overzicht voorgeschreven zelfstandige hulppersonen

Project / Contractnr.	Voorgeschreven zelfstandige hulppersoon	Werkzaamheden
31182252	Conclusion B.V. te Utrecht	diensten en/of leveringen als genoemd in de bijlage Q “Producten en Diensten Catalogus Netwerken CIV” van de VSP
31165657	EQUANS Infra & Mobility B.V	onderhoudswerkzaamheden met betrekking tot het verhelpen van storingen en afhandelen van calamiteiten