



BIJLAGEN

Vraagspecificatie Proces – Raamovereenkomst

Realisatie Variabel onderhoud stalen bruggen West Nederland Zuid
Project Over-Bruggen



Zaaknummer: **31196743**

Datum: 14 januari 2025

Colofon

Uitgegeven door	Ministerie van Infrastructuur en Waterstaat Rijkswaterstaat Programma's, Projecten en Onderhoud Wilhelminakade 9 3072 AP ROTTERDAM
Datum	14 januari 2025
Status	Definitief
Documentnummer	HB4701209 (pdf)
Versienummer	1.0

INHOUDSOPGAVE

Bijlage A	Risicolijst
Bijlage B	Integraal Veiligheidsplan
Bijlage C	Format Risicobeoordeling
Bijlage D	Bijlagen Bedrijfsvoering Elektrische Installaties - D1: NEN 3140 Veiligheidshandboek Rijkswaterstaat - D2: NEN 3140 Veiligheidshandboek Rijkswaterstaat addendum - D3: NEN 3840 Veiligheidshandboek Rijkswaterstaat
Bijlage E	Bedrijfsvoering Elektrische Installaties (BEI) van de Opdrachtgever
Bijlage F	Regelingenschema Kabels en Leidingen Derden
Bijlage G	Verkeersmanagement voor rijkswegen - Bijlage A: Informatievoorziening ter plaatse bij verkeersmaatregelen - Bijlage B: Werkbare Uren (WBU), Venstertijden Afsluitingen (VTA) en werkvensters - Bijlage C: Slot's
Bijlage H	Scheepvaartverkeersmanagement voor rijksvaarwegen - Bijlage A: Hindertabel voor rijkswateren - Bijlage B: Verkeersbegeleiding - Bijlage C: Template scheepvaartverkeersmanagementplan - Bijlage D: Stremmingmomenten - Bijlage E: Template verkeersmaatregelenplan
Bijlage I	Rijkswaterstaat Brede Afspraak Archeologie
Bijlage J	Rijkswaterstaat Brede Afspraak Maatschappelijk Verantwoord Inkopen
Bijlage K	Eisen duurzaam materieel
Bijlage L	Levering Areaalgegevens
Bijlage M	Cybersecurity Implementatierichtlijn Objecten v2.4
Bijlage N	J-STD-016
Bijlage O	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
Bijlage P	Invulinstructie format LV BRO
Bijlage Q	Melding inzet zelfstandige hulppersoon
Bijlage R	Aanvullende eigen verklaring inzake Russische partijen



BIJLAGE A - Risicolijst

Vraagspecificatie Proces – Raamovereenkomst

Realisatie Variabel onderhoud stalen bruggen West Nederland Zuid
Project Over-Bruggen



Zaaknummer: **31196743**

Datum: 14 januari 2025

Bijlage A - Risicolijst

Niet van toepassing op niveau van de Raamovereenkomst.

Per Nadere Overeenkomst wordt een bijlage A 'Risicolijst' toegevoegd.



BIJLAGE B – Integraal Veiligheidsplan

Vraagspecificatie Proces – Raamovereenkomst

Realisatie Variabel onderhoud stalen bruggen West Nederland Zuid
Project Over-Bruggen



Zaaknummer: **31196743**

Datum: 14 januari 2025

Bijlage B - Integraal Veiligheidsplan

Niet van toepassing op niveau van de Raamovereenkomst.

Per Nadere Overeenkomst wordt een bijlage B 'Integraal Veiligheidsplan' toegevoegd.



BIJLAGE C – Format Risicobeoordeling

Vraagspecificatie Proces – Raamovereenkomst

Realisatie Variabel onderhoud stalen bruggen West Nederland Zuid
Project Over-Bruggen



Zaaknummer: **31196743**

Datum: 14 januari 2025

Bijlage C - Format Risicobeoordeling

Deze bijlage 'Format Risicobeoordeling' geldt **generiek** voor alle Nadere Overeenkomsten.



RWS INFORMATIE -

Templates Achtergrondinformatie Risicobeoordeling

Template algemene informatie voor een risicobeoordeling
Template grenzen van de machine

Datum	27 juli 2017
Status	Template- Definitief

Colofon

Uitgegeven door Informatie	Expertteam Machineveiligheid Document is onderdeel van de Template Risicobeoordeling
Uitgevoerd door	Expertteam Machineveiligheid
Datum	27 juli 2017
Status	concept
Versienummer	1.2

Inhoud

Inleiding 7

1 Templates achtergrondinformatie risicobeoordeling 8

1.1 Algemeen 8

1.1.1 Template algemene informatie voor een risicobeoordeling 8

1.1.2 Template grenzen van de machine 10

2 Voorbeelden van ingevulde Templates 11

2.1 Algemeen 11

2.1.1 Voorbeeld informatie voor een risicobeoordeling 11

2.1.2 Voorbeeld grenzen van de machine 15

Inleiding

Doel template risicobeoordeling

Het doel van de template is 3-ledig;

1. Het vastleggen van een eenduidige methodiek en eenduidige wijze van documentatie (van een deel (zie scope)) van de risicobeoordeling NEN-EN-ISO 12100 van een van een object/machine;
2. Eenduidige documentatie van de risicobeoordeling ten behoeve van de levenscyclus van een object/machine;
3. Eenduidige documentatie van de risicobeoordeling over de aanleg en onderhoudsprojecten heen en over het RWS areaal heen.

Hierdoor kunnen risicobeoordelingen van verschillende projecten en/of objecten/machines objectiever met elkaar vergeleken worden.

Toelichting; Objecten/machines zoals beweegbare bruggen en natte kunstwerken worden (project-)specifiek ontwikkeld en hebben over het algemeen een andere (langere) levenscyclus dan de gemiddelde (seriematige en vrij in de handel verkrijgbare) machines.

Binnen die levenscyclus is het te verwachten dat een object/machine een aantal malen zal worden gerenoveerd en/of aangepast binnen groot onderhoud en daarbij is eenduidige documentatie van belang.

Deze template is niet bedoeld voor het documenteren van de ARBO RI&E en de daarbij behorende RI&E van een bestaande machine. Dit dient te geschieden binnen het Arbo managementsysteem van RWS-CD.

Voordat een Risicobeoordeling wordt uitgevoerd dient een aantal uitgangspunten van de machine te zijn vastgelegd. Dit is de zogenaamde achtergrondinformatie die benodigd is om een Risicobeoordeling goed uit te kunnen voeren.

Dit bestand

Dit bestand bevat de templates voor de;

1. Template algemene informatie voor een risicobeoordeling
2. Template grenzen van de machine

Dit bestand is opgenomen in een apart tabblad van het Exelbestand met daarin opgenomen de template voor de gevarenidentificatie, risicoschatting en -reductie.

1 Templates achtergrondinformatie risicobeoordeling

1.1 Algemeen

Voor het vastleggen van de achtergrondinformatie worden de volgende templates beschikbaar gesteld:

1. Template algemene informatie voor een risicobeoordeling
2. Template grenzen van de machine

1.1.1 Template algemene informatie voor een risicobeoordeling

Gebruik de onderstaande template om vast te leggen welke informatie is verzameld welke als input dient voor het uitvoeren van de risicobeoordeling:

Informatie voor een risicobeoordeling (EN-ISO 12100 §5.2)	
Datum: Documentnummer / versie: Machine / project: Onder verantwoordelijkheid van: Team samenstelling:	In te vullen door de verantwoordelijke voor de Risicobeoordeling.

Beschrijving van de machine (EN-ISO 12100 §5.2 punt a)	
Onderwerp	Omschrijving
Gebruikers	Beschrijf alle gebruikers die de brug of sluis gaan gebruiken
Processen	Beschrijf de processen van de gehele levensduur van de machine.
Ontwerptekeningen	Neem ontwerptekeningen in het document op van de beweegbare brug zodat vastgesteld kan worden waar zich mogelijke gevarenczones bevinden.
Energiebronnen	Beschrijf de energiebronnen van de brug, hun functie en eigenschappen.
Voorgaande ontwerp	Beschrijf ervaringen met de bestaande brug voor zover relevant.
Informatie voor het gebruik van de machine	Beschrijf kort de signalen en waarschuwingssinrichtingen, markeringen, symbolen, begeleidende documenten en de gebruiksaanwijzing die relevant zijn voor de gerenoveerde beweegbare brug of sluis.

Voorschriften, normen en andere toepasbare documenten (EN-ISO 12100 §5.2 punt b)	
Onderwerp	Omschrijving
Toepasselijke voorschriften	Welke voorschriften zijn van toepassing op het ontwerp van de brug of sluis (voor zover deze nog niet opgenomen zijn in stap 2)
Relevante normen	Welke relevante normen worden er gebruikt (voor zover nog niet opgenomen in stap 2)
Relevante technische specificaties	Beschrijf hier eventuele relevante technische specificaties van de brug of sluis welke nog niet genoemd zijn in stap 2
Relevante veiligheidsinformatiebladen	Beschrijf hier eventuele relevante informatiebladen welke nog niet genoemd zijn in stap 2

Gebruikservaring (EN-ISO 12100 §5.2 punt c)	
Onderwerp	Omschrijving
Ongevallen historie	<i>Hier moet iedere geschiedenis over ongevallen of incidenten van de brug of sluis welke gerenoveerd gaat worden of van een soortgelijke brug of sluis vastgelegd worden.</i>
Gebrekkig functioneren	<i>Hier moet iedere geschiedenis over gebrekkig functioneren van de brug of sluis welke gerenoveerd gaat worden of van een soortgelijke brug of sluis vastgelegd worden.</i>
Geschiedenis van schade aan de gezondheid door gebruik van of werken aan de machine	<i>Neem hier de geschiedenis van schade aan de gezondheid voortgekomen uit bijvoorbeeld emissie (lawaaï, trillingen, stof, rook en) en of gebruikte chemicaliën op.</i>
Ervaringen van gebruikers van soortgelijke machines	<i>Hier moeten de relevante ervaringen van gebruikers van een soortgelijke brug of sluis (of in het geval van modificatie of renovatie gebruikers van de bestaande brug of sluis) vastgelegd worden. Wanneer het praktisch is kan in deze stap ook de uitwisseling van informatie met de mogelijke (nieuwe) gebruikers van de brug of sluis vastgelegd worden.</i>

Relevante ergonomische beginselen (EN-ISO 12100 §5.2 punt d)	
Onderwerp	Omschrijving
Omschrijving van toepassing zijnde ergonomische beginselen	<i>Hier moeten de relevante ergonomische beginselen die van toepassing zijn op de brug of sluis beschreven worden. Hierbij moet gedacht worden aan bijvoorbeeld Bedienlocaties, handbediening, geluidsniveaus enzovoort.</i>

1.1.2 *Template grenzen van de machine*

Gebruik de onderstaande template om de grenzen van de machine vast te leggen:

Grenzen van de machine (EN-ISO 12100 §5.3)	
Datum:	In te vullen door de verantwoordelijke voor de Risicobeoordeling.
Documentnummer / versie:	
Machine / project:	
Onder verantwoordelijkheid van:	
Team samenstelling:	

Gebruiksgrenzen (EN-ISO 12100 §5.3.2)
Bedoeld gebruik
Beschrijf hier het bedoeld gebruik van de machine.
Redelijkerwijs voorzienbare verkeerde gebruik
Beschrijf hier het bedoeld gebruik van de machine.

Ruimtelijke grenzen (EN-ISO 12100 §5.3.3)
Beschrijf hier het bedoeld gebruik van de machine.
Tijdgrenzen (EN-ISO 12100 §5.3.4)
Beschrijf hier het bedoeld gebruik van de machine.
Andere grenzen (EN-ISO 12100 §5.3.5)
Beschrijf hier het bedoeld gebruik van de machine.

2 Voorbeelden van ingevulde Templates

2.1 Algemeen

In dit hoofdstuk zijn voorbeelden opgenomen van ingevulde templates uit Hoofdstuk 1. Voor het invullen van deze templates is een brug als voorbeeld genomen.

De voorbeelden voldoen niet volledig aan de uitgangspunten van de Landelijke Brug en Sluisstandaard.

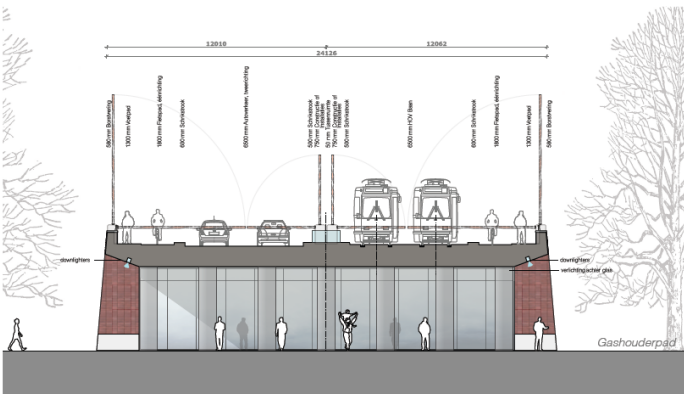
Uiteraard zijn de templates ook geschikt voor machines zoals: keersluizen, spuisluizen, schutsluizen, gemalen, etc.

2.1.1 Voorbeeld informatie voor een risicobeoordeling

Hieronder een voorbeeld van informatie welke als input voor een risicobeoordeling zou kunnen dienen:

Informatie voor een risicobeoordeling (EN-ISO 12100 §5.2)	
Datum:	10-10-2013
Documentnummer / versie:	ABk-X versie A
Beweegbare brug / sluis / project:	Nieuwe tafelbrug XX
Onder verantwoordelijkheid van:	Persoon A
Team samenstelling:	Persoon B Enz.

Beschrijving van de machine (EN-ISO 12100 §5.2 punt a)	
Onderwerp	Omschrijving
Gebruikers	- Landverkeer in de vorm van gemotoriseerd verkeer, Trams, fietsers, bromfietzers en voetgangers; - Scheepvaartverkeer in de vorm van recreatievaart en beroepsvaart (max klasse); - Brugbedieners (brugwachters); - Onderhoudspersoneel (onder te verdelen in o.a. mechanisch en elektrisch onderhoudspersoneel); - Schoonmakers facilitaire voorzieningen; - Schilders; - Servicemonteurs; - Inspecteurs; - Contractors; - Algemene bezoekers (zoals open dag of rondleiding etc.).
Processen	- De brug bedienprocessen zoals beschreven in de Landelijke Brug en Sluisstandaard aangevuld met de processen die daarin niet zijn opgenomen t,b.v.; - Reguliere bediening (op afstand); - Reguliere bediening (lokaal); - Buitengewone bediening; - Noodbediening technisch (lokaal); - Noodhandbediening hand (lokaal); - Storing; - Calamiteiten; - Onderhoud; - Onderhoudsbediening; - Modificatie;

	• Inspectie; • Buiten bedrijf stellen; • Ontmanteling.
Ontwerptekeningen	Aangezien deze initiële risicobeoordeling plaatsvindt in het beginstadium van de ontwerpfase van het project zijn er nog geen definitieve ontwerptekeningen. Wel zijn er reeds een aantal schetsen gemaakt waarmee een beeld gevormd kan worden van de uiteindelijke situatie. Hieronder een van deze schetsen:  Figuur 1: Schets
Energiebronnen	De brug beschikt over een elektrische krachtvoeding (3 fasen + N + PE 400V/50Hz) en een aantal stuurvoedingen waaronder 230VAC/50Hz. De hoofdverdeler welke is geplaatst in de ondergrondse technische ruimte, voorziet in de mogelijkheid om een mobiele noodstroom aggregaat aan te koppelen om tijdens spanningsuitval de brug te kunnen besturen. Middels de hoofdschakelaar is om te schakelen van 'netvoeding' via 'uit' naar 'mobiele noodstroomaggregaat'. De PLC's, land- en scheepvaart seinen, marifoon, audio, netwerkswitch en camera's zijn aangesloten op een UPS waardoor tijdens het wegvallen van de voedingsspanning, de brug automatisch in een noodstop gaat en alle landverkeerseinen en scheepvaartseinen op rood gaan. De bediener kan in deze situatie enkel de status en de camerabeelden van de brug bekijken en zowel de brug als de afsluitbomen niet bedienen. Naast de elektrische voeding beschikt de brug ook over een hydraulische energievoorziening welke gebruikt wordt voor de aandrijving van het val. De hydraulische aggregaten bevinden zich tevens in de technische ruimte (per brug één hydrauliek aggregaat). Bij calamiteiten kan een mobiele noodstroomaggregaat ingezet worden om de brug te kunnen besturen.
Voorgaande ontwerp	Van deze brug is geen voorgaand ontwerp beschikbaar.
Informatie voor het gebruik van de machine	Aangezien dit een nieuwe brug betreft welke een beweegbare brug van een ander type gaat vervangen, is er nog geen ervaring in het gebruik van de machine. Wel is bekend dat de brug op afstand bediend gaat worden vanuit een centrale bedienpost. Het val zal maximaal 1,5m hydraulisch omhoog gestuurd worden waarbij de

	doorvaarthoogte van 5,5m in gesloten stand naar 7m in geopende stand gaat.

Voorschriften, normen en andere toepasbare documenten (EN-ISO 12100 §5.2 punt b)	
Onderwerp	Omschrijving
Toepasselijke voorschriften	- Machinerichtlijn 2006/42/EG
Relevante normen	- NEN-EN-ISO 12100:2010: Veiligheid van machines – Algemene ontwerpbeginsselen - Risicobeoordeling en risicoreductie. - NPR-ISO-TR 14121-2:2012: Safety of machinery - Risk assessment - Part 2: Practical guidance and examples of methods - NEN-EN-IEC 60204-1:2006: Veiligheid van machines - Elektrische uitrusting van machines - Deel 1: Algemene eisen - NEN 6787:2003: Het ontwerpen van beweegbare bruggen - Veiligheid
Relevante technische specificaties	
Relevante veiligheidsinformatiebladen	Arbo Informatieblad AI-11 Machineveiligheid

Gebruikservaring (EN-ISO 12100 §5.2 punt c)	
Onderwerp	Omschrijving
Ongevallen historie	Er is op dit moment nog geen relevante ongevallenhistorie voorhanden.
Gebrekkig functioneren	
Geschiedenis van schade aan de gezondheid door gebruik van of werken aan de machine	
Ervaringen van gebruikers van soortgelijke machines	Bij de xx brug is het zicht van de bediener op de gevarenszones op het wegdek niet op orde. Dode hoeken waar een verkeersdeelnemer slecht te zien is. De afsluitboominstallatie van burg yy is vaak in storing. Deels veilig falen voor de machine zelf, maar het veroorzaakt verkeerskundig gevaarlijke situaties.

Relevante ergonomische beginselen (EN-ISO 12100 §5.2 punt d)	
Onderwerp	Omschrijving
Omschrijving van toepassing zijnde ergonomische beginselen	<i>Tijdens het ontwerp van de nieuwe brug wordt rekening gehouden met onder andere de volgende ergonomische aspecten:</i> - <i>Plaatsing bedieningselementen voor lokale bediening;</i> - <i>Positie en benodigde kracht handbediening / handaandrijving van brug en ASB;</i> - <i>Toegang tot verschillende plaatsen op / aan de brug voor onderhoud, storingen etc.;</i> - <i>Verlichting brugdek en weg;</i> - <i>Geluidsniveaus akoestische signalen;</i> - <i>Geluidsniveaus aandrijving / bewegingswerk;</i> - <i>Trillingen van onderdelen;</i> - <i>Extreme temperaturen bedieningsruimte en werkruimtes;</i>

2.1.2 Voorbeeld grenzen van de machine

Hieronder een voorbeeld van een beschrijving van de grenzen van de machine welke als input dienen voor de rest van de risicobeoordeling:

Grenzen van de machine (EN-ISO 12100 §5.3)	
Datum:	10-10-2013
Documentnummer / versie:	ABk-X versie A
Beweegbare brug / sluis / project:	Nieuwe tafelbrug XX
Onder verantwoordelijkheid van:	Persoon A
Team samenstelling:	Persoon B Enz

Gebruiksgrenzen (EN-ISO 12100 §5.3.2)
Bedoeld gebruik
<u>Algemeen</u> De nieuwe brug is een tafelbrug met een beperkte doorvaarthoogte in geopende stand. Van de brug is nog geen data aanwezig met betrekking tot het aantal brug openingen per dag. Het aantal te verwachten brugopeningen voor de nieuwe Tafelbrug is daarom gebaseerd op het aantal brugopeningen van een reeds bestaande brug in de vaarroute met dezelfde doorvaarthoogte als de nieuwe Tafelbrug en die is 1406 openingen per jaar wat neer zou komen op ongeveer vier brugopeningen per dag gemiddeld. De brug wordt het hele jaar gebruikt (met uitzondering van zon- en feestdagen in de winterperiode) . Het gemiddeld aantal brugopeningen per dag zal afhankelijk van het seizoen sterk variëren en zal in de zomerperiode fors hoger liggen. Voor de risicobeoordeling wordt daarom uitgegaan van de piekbelasting van 2112 brugopeningen per jaar wat neer komt op gemiddeld zes brugopeningen per dag. Een gemiddelde brug cyclus duurt (afhankelijk van onder andere het aantal te passeren vaartuigen) ongeveer vijf minuten. <u>Landverkeer</u> De brug bestaat uit twee vallen welke (tijdens reguliere bediening) altijd tegelijk bestuurd worden. Het eerste val bestaat uit een trottoir, een fietspad (één richting) en een dubbele rijbaan (tweerichting zonder afscheiding) waar een maximale snelheid geldt van 50km/u. De rijbaan en het fietspad zijn gescheiden middels een verhoogde schrikstrook. Het tweede val bestaat uit twee trambanen (één per rijrichting) met daarnaast een fietspad (één richting) en een trottoir. Ook hier is een verhoogde schrikstrook aanwezig tussen de trambaan en het fietspad. Hieronder een beschrijving van de vormen van landverkeer welke gebruik maken van de brug: - Tramverkeer De brug zal gebruikt gaan worden door Tram 19 die in beide richting verdeeld over twee trambanen gebruik zal maken van de brug met een gemiddeld aantal trams van 15 per dag. Tevens zullen stadsbussen ook gebruikmaken van de trambaan. - Snelverkeer (in de vorm van gemotoriseerd verkeer) De weg wordt gebruikt door automobilisten, motorrijders, vrachtverkeer, landbouwvoertuigen, bussen, hulpdiensten. - Fietzers

De brug is aan beide zijden voorzien van een fietspad. Het fietspad is bedoeld om in één richting gebruikt te worden door fietsers, brommers, scooters.

- Voetgangers

Aan beide zijden van de brug is een trottoir aanwezig welke in beide richtingen door voetgangers gebruikt kan worden.

Het is redelijkerwijs aan te nemen dat bovengenoemde bruggebruikers kennis hebben van de (wettelijke) verkeersregels, dat zij hun plaats op de weg kennen en verkeerslichten, verkeersborden begrijpen.

Scheepvaartverkeer

De brug welke over het Rijn-Schiekanaal (vaarwegklasse IV) ligt, wordt gebruikt in beide richtingen waarbij grote schepen in tegengestelde richting elkaar niet kunnen passeren. Het scheepvaartverkeer dat gebruik maakt van de brug is onder te verdelen in de volgende vormen:

- Beroepsvaart

De doorvaart van de brug wordt gebruikt door beroepsvaart met een maximale doorvaarthoogte van 7m. In gesloten toestand is de maximale doorvaarthoogte 5,5m maar is het in een aantal gevallen mogelijk voor beroepsvaart om de brug te passeren (eventueel door het laadruim vol te pompen met water wat soms gebeurt tijdens een langere stremming van de brug voor scheepvaartverkeer). De Beroepsvaart maakt over het algemeen het jaar rond gebruik van de brug.

- Recreatievaart

De doorvaart wordt tevens gebruikt door allerlei vormen van recreatievaart welke al dan niet onder de gesloten brug door kan varen. Hierbij moet gedacht worden aan roeiboten, jachten, sloepen, zeilboten enz. Het grootste gedeelte van de recreatievaart zal vooral in de zomerperiode van de brug gebruik maken.

Het is redelijkerwijs aannemelijk dat de beroepsvaart kennis heeft van de seinbeelden van de scheepvaartseinen en de doorvaartlichten. Voor een deel van de recreatievaart is dit echter minder vanzelfsprekend.

Bedienmodi

De brug is voorzien van een aantal verschillende bedieningsmogelijkheden welke uitgesplitst zijn in bediening op afstand en lokale bediening.

In Tabel 2.1 zijn de verschillende bedieningsmodi welke van toepassing zijn voor de brug vastgelegd.

Ingrijpen van bedieners in afwijkende situaties zoals bijvoorbeeld een storing is gebaseerd op het bereiken van een veilige situatie; de bediener stopt of noodstopt de brug (bewegingen), kijkt of de gevaarlijke situatie opgeheven is en stelt zelf of in samenwerking met de onderhoudsaannemer de brug weer in gebruik.

Er kan aangenomen worden dat aanwezige bezoekers de brug niet kunnen bedienen, enerzijds door technische voorzieningen, anderzijds door toezicht.

Onderhoud

Van het onderhoudspersoneel mag aangenomen worden dat zij een opleiding hebben genoten voor de werkzaamheden die zij uit moeten voeren. De brug (of delen van de brug) wordt periodiek onderhouden / gekeurd.

Redelijkerwijs voorzienbare verkeerde gebruik

Naast het bedoelde gebruik van de machine moet ook rekening gehouden worden met het redelijkerwijs voorzienbare verkeerde gebruik van de machine. Voor deze brug is onderstaand voorzienbaar verkeerd gebruik gedefinieerd onderverdeeld in de gebruikersgroepen landverkeer, scheepvaartverkeer, bediening en onderhoud.

Landverkeer

Voor het redelijkerwijs voorzienbare verkeerde gebruik van de brug voor het landverkeer zijn de onderstaande punten benoemd:

- Snelverkeer rijdt wellicht harder dan de maximum toegestane snelheid van 50km/u.
- De tram rijdt mogelijk harder dan de maximum snelheid zeker bij het afrijden van het val (4-5% dalingspercentage)
- Verkeer kan de door de stopstreep aangegeven opstelplaatsen negeren en bijvoorbeeld doorrijden tot aan de afsluitboom.
- Er moet rekening gehouden worden met het feit dat zowel gemotoriseerde als niet gemotoriseerde verkeersdeelnemers af en toe de rode seinen negeren om de brug nog snel te kunnen passeren.
- Zowel voetgangers als fietsers zullen af en toe proberen om de dalende afsluitbomen nog snel te passeren (brugwachters zullen wellicht af en toe 'dreigen' met de afsluitbomen om het verkeer te dwingen te stoppen).
- Passanten (fietsers en of voetgangers kunnen besluiten tussen de afsluitboom en het val te wachten tot ze de brug kunnen passeren.
- Passanten (kinderen) zouden spelenderwijs aan de afsluitbomen kunnen gaan hangen bij het openen, in open afsluitbomen kunnen klimmen, of van het val in het water kunnen springen bij warm weer.
- Doordat de tafelbrug maar maximaal 1,5m omhooggaat en tevens redelijk langzaam beweegt, moet rekening worden gehouden met het feit dat (voornamelijk) voetgangers tijdens het draaien van de brug op het val klimmen en de brug op die manier passeren.
- Fietsers die besluiten een fietspad tegen de richting in te gebruiken (ook als de aanrijbomen aan de overkant al aan het sluiten zijn).
- Vooral in de zomerperiode kan er (ondanks dat het verboden is) gezwommen worden nabij de brug en kan men zelfs de brug gebruiken om vanaf te springen / duiken.

Scheepvaartverkeer

Voor het redelijkerwijs voorzienbare verkeerde gebruik van de brug voor het scheepvaartverkeer zijn de onderstaande punten benoemd:

- Een schipper kan besluiten het rode / spersein te negeren omdat hij denkt de brug nog net te kunnen passeren en anders een tijd moet wachten tot de volgende brugopening.
- Een schipper kan een inschattingsfout maken en denken onder de gesloten brug door te kunnen varen maar (bijvoorbeeld door een hoge waterstand) toch in aanvaring komen met het val.

Bediening

De bediener kan de brug "verkeerd" bedienen door o.a.:

- Het brugproces sneller willen afronden als gevolg van verkeersdruk door b.v. de brug al te gaan sluiten wanneer een schip deze nog niet volledig heeft gepasseerd;
- Zelf resetten en herstarten na een noodstop door de bediener als gevolg van bijvoorbeeld verkeersdruk;
- Plaatsen van overbruggingen bij defecten om toch door te kunnen draaien;
- De brug met een verkeerde bedieningsmodus bedienen waar die niet voor geschikt is (zoals bijvoorbeeld noodbediening i.p.v. reguliere bediening);
- Niet alle schouwmomenten in acht nemen;
- Bij het bedienen op afstand naar het verkeerde camerabeeld kijken;

- Per ongeluk een verkeerde knop indrukken (mogelijk tijdens buitengewone bediening).
- Aan beide zijden van de doorvaart de scheepvaartseinen op groen zetten zodat kleine schepen tegelijk de brug kunnen passeren. De keuze hiervoor ligt bij de bediener welke een fout kan maken en ook bij beroepsvaart de seinen aan beide zijden van de doorvaart op groen kan zetten.

Onderhoud

Het voorzienbare verkeerde gebruik voor onderhoudspersoneel moet gezocht worden in:

- Tijdens werkzaamheden op het val blijven staan als de brug gedraaid wordt;
- Het overbruggen van sensoren of veiligheidsfuncties t.b.v. testen, of om door te kunnen draaien;
- Componenten vervangen door componenten die daar niet voor geschikt zijn;
- Het niet gebruiken van voorgeschreven PBM's;
- Sleutels in sleutelschakelaars laten zitten;

Verkeerde onderhoud / veiligheidsprocedures volgen.

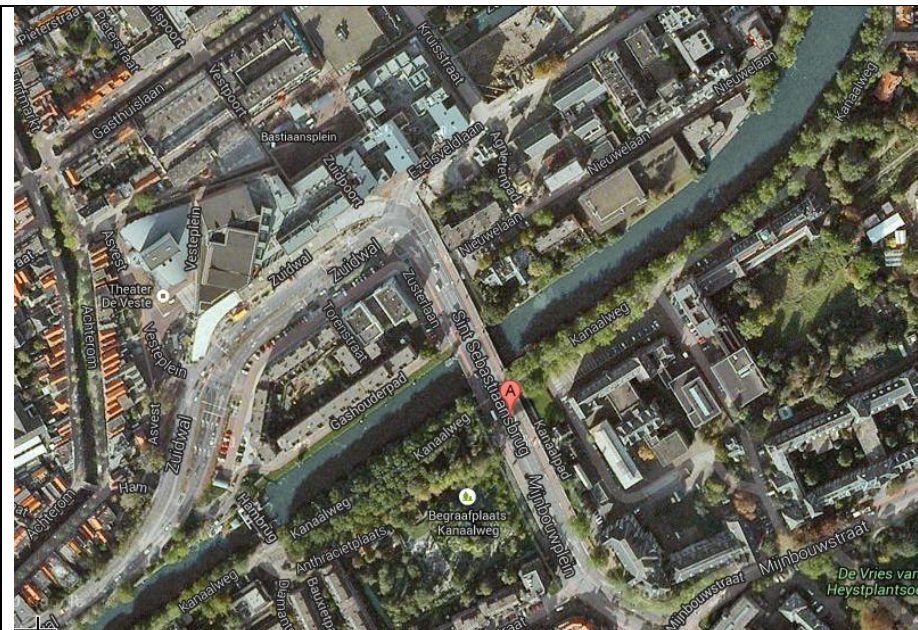
Bedienmodi	Locatie bediening	Periode / Frequentie	Bedienaars	Bedienmodi
<i>Reguliere bediening centraal</i>	Op afstand vanuit een centrale bedienpost . Er is vanuit deze bedienpost geen direct zicht op de brug, maar wordt gebruik gemaakt van camerabeelden. De nieuwe bedienplek wordt onderdeel van een duo werkplek.	Standaard bedienvorm welke tijdens normaal bedrijf van de brug gebruikt wordt (+/- 99% wordt gebruik gemaakt van deze bedienmodus)	Brugwachters	<i>Reguliere bediening centraal</i>
<i>Reguliere bediening lokaal</i>	Lokaal middels een draagbare bedienconsole te bedienen welke in een afsluitboomkast aangesloten kan worden.	Deze bedienmodus wordt gebruikt wanneer bijvoorbeeld door een storing of een defecte camera de brug niet centraal bediend kan / mag worden. Of	Brugwachters	<i>Reguliere bediening lokaal</i>

		tijdens onderhoud. (+/-4% wordt gebruikt gemaakt van deze bedienmodus)		
<i>Buitengewone bediening (Noodbediening)</i>	Noodbediening lokaal met behulp van een noodbedienpeer welke in een afsluitboomkast aangesloten kan worden. (In deze bedienmodus zal de brug op slechts 10% van de nominale snelheid draaien).	Deze vorm van bediening wordt gebruikt wanneer het niet mogelijk is om de brug vanuit de centrale bedienpost te bedienen of om functies van de brug te testen bij modificaties of storingen. (+/-0,9% wordt gebruik gemaakt van deze bedienmodus)	Brugwachters Onderhouds-personeel	<i>Buitengewone bediening (Noodbediening)</i>

Tabel 2.1

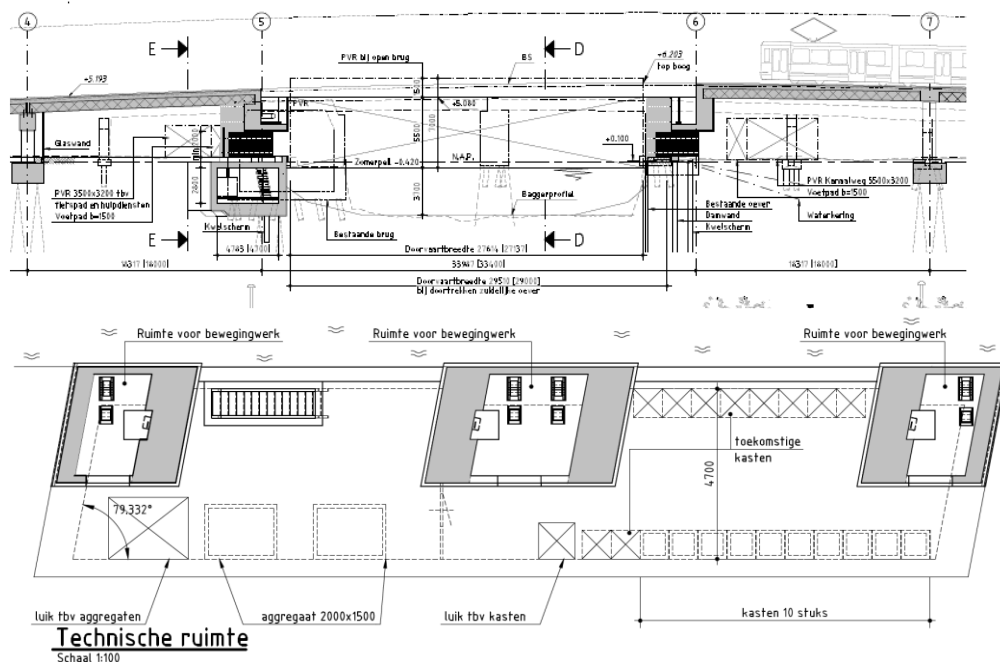
Ruimtelijke grenzen (EN-ISO 12100 §5.3.3)

In deze paragraaf staan de ruimtelijke grenzen van de nieuwe tafelbrug beschreven. De fysieke afmetingen van de brug staan reeds beschreven in de bijgevoegde situatieschetsen. Figuur 2 toont het bovenaanzicht van de huidige brug welke over het kanaal is gelegen. Deze bestaande brug wordt vervangen door een nieuwe brug welke bestaat uit twee onafhankelijk van elkaar te besturen bruggen die 'tegen elkaar' liggen.



– **Figuur 2: Bovenaanzicht bestaande brug**

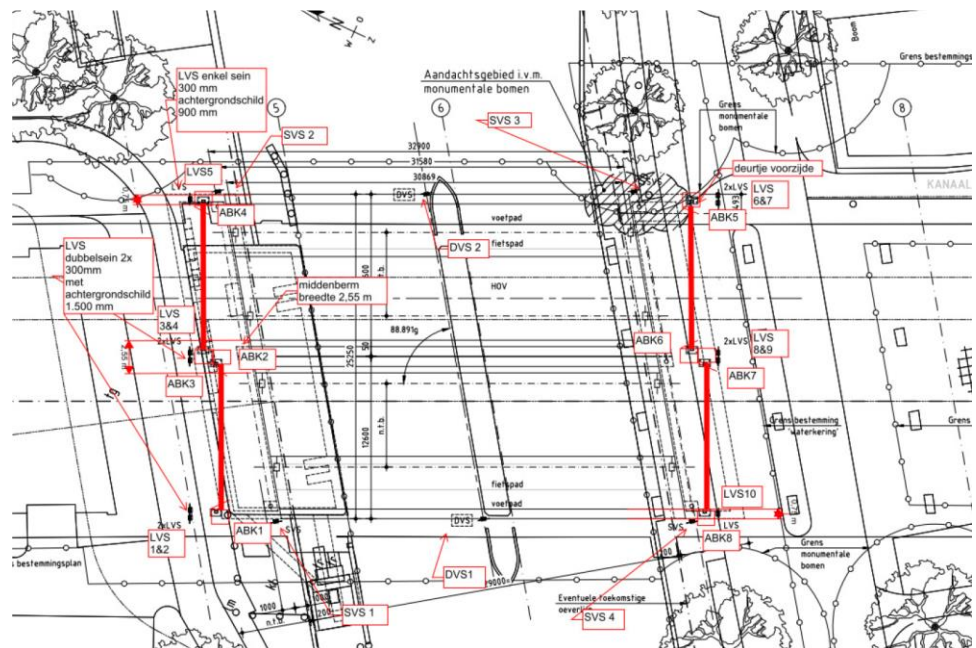
Beide brugdekken worden centraal bestuurd vanuit één technische ruimte. De bewegingswerken bestaande uit voornamelijk de hydraulische cilinders zijn gepositioneerd in de pijlers van de brug. Ondanks dat de besturing van beide bruggen is geïntegreerd, is het wel mogelijk om tijdens noodbediening slechts één brugdek tegelijk te besturen. Figuur 3 bestaat uit een aantal schetsen van de brugpijlers en de technische ruimte van de nieuwe brug.



– **Figuur 3: Schetsen brugpijlers en technische ruimte**

Beide zijden van de van het val kunnen afgesloten worden voor het verkeer door middel van afsluitbomen. Er zijn separate aan- en afrijbomen aanwezig voor het snelverkeer. Voor het afsluiten van de trottoirs en de fietspaden wordt gebruik gemaakt van dezelfde afsluitbomen als die voor het snelverkeer. Zie **Fout! V**

erwijzingsbron niet gevonden. voor een overzicht van de posities van de afsluitbomen.



– **Figuur 4: Schets afsluitbomen**

De brug beschikt over een aantal componenten welk mogelijk lastig bereikbaar zijn, maar wel periodiek onderhoud vergen zoals o.a. camera's, scheepvaartseinen, doorvaartlichten en de oplegging van het val. Hierbij kan het nodig zijn ladders, steigers, hoogwerkers enz. te gebruiken). Tevens kan het voor een aantal werkzaamheden nodig zijn dat de brug wordt afgesloten voor weg- of scheepvaartverkeer.

Tijdgrenzen (EN-ISO 12100 §5.3.4)

Technische levensduur

Voor een aantal delen van de brug is in de ontwerpfase een technische levensduur gehanteerd. Hieronder een overzicht van deze referentieperiodes:

Onderdeel van brug.	Technische levensduur
Staalconstructie val	100 jaar
Slijtlaag val	15 jaar
Conservering staal	15 jaar
Conservering staal (incl. afstralen van de conservering)	60 jaar
Aluminiseren + conservering staal	15 jaar
Afsluitbomen en -kasten	30 jaar
Aandrijving (hydraulisch)	25 jaar
Elektronica	10 jaar
Elektrische installatie	30 jaar
Camera's	10 jaar
Bekabeling	30 jaar
Glasvezelkabel	15 jaar
Lichtmasten	30 jaar
OVL armaturen LED	15 jaar
LED-lampen LVS, SVS	10 jaar
PC's / Beeldschermen	2,5 jaar

Touchscreen	5 jaar
Bovenleiding trambaan	x jaar
Tram-rails	x jaar

Onderhoud

Er zijn verschillende onderhoudstaken welke periodiek uitgevoerd (moeten) worden op de brug. Hieronder volgt een overzicht van de onderdelen welke een periodiek onderhoud vereisen met daarbij de frequentie hiervan.

Onderdeel van brug welke een periodiek onderhoud vereisen.	Onderhoud / inspectie frequentie
Hydrauliek cilinders	Informatie onderhoud onbekend.
Hydrauliek units Gelijkloopinrichting	Informatie onderhoud onbekend.
Gelijkloopinrichting	Per twee maanden smeren
Afsluitbomen	Informatie onderhoud onbekend.
Bruglichten	Informatie onderhoud onbekend.
Verlichting	Informatie onderhoud onbekend.
Scheepvaartseinen en doorvaartlichten	Informatie onderhoud onbekend.
Camera's	Informatie onderhoud onbekend.
Staalconstructie	Informatie onderhoud onbekend.
Tram rails	Informatie onderhoud onbekend.
Bovenleiding trambaan	Informatie onderhoud onbekend.

Naast het periodieke onderhoud van de brug zullen er in geval van een defect of een storing ook werkzaamheden aan onderdelen van de brug uitgevoerd moeten worden. Er wordt rekening gehouden met gemiddeld één storing per maand waarvoor meestal ook toegang tot de elektrische installatie nodig is.

Periodieke controles

De brug (of delen van de brug) zal regelmatig geïnspecteerd worden. Hierbij moet gedacht worden aan inspectie van de cilinders, staat staalconstructie (roest, scheuren enz.), de trambanen, bovenleiding en bijvoorbeeld de elektrische installatie (NEN 3140). Veiligheidsfuncties zoals noodstopsystemen zullen afhankelijk van hun ontwerpkeuze periodiek geïnspecteerd of getest worden om het vereiste veiligheidsniveau te garanderen.

Overige tijdgrenzen

Naast de periodieke onderhoudswerkzaamheden, inspecties en storingen zal er ook af en toe schoongemaakt moeten worden. Hoe dit periodiek ingevuld gaat wordt worden voor de nieuwe brug is nog niet bekend.

Andere grenzen (EN-ISO 12100 §5.3.5)Eigenschappen van de waterweg

Het Rijn-Schiekanaal met een vaarwegklasse van IV, heeft een doorvaartbreedte van 33m en is ter plaatse van de brug niet geschikt voor het passeren van meerdere (grote) schepen. De waterstand van het kanaal kan variëren. De stroming in het kanaal zal weinig variëren (geen invloed van getijden en er wordt niet noemenswaardig gespuid in de buurt van de brug).

Omgevingsinvloeden

De technische ruimte beschikt over een apart geconditioneerde ruimte waarin de voeding, de schakelkasten en de lokale bediening zijn ondergebracht. Deze geconditioneerde ruimte kan zowel in de zomer als de winter op temperatuur gehouden worden en is daardoor vrij van condens. De geconditioneerde ruimte beschikt over een buffervloer met een water niveau meting welke een alarm genereert wanneer het water in deze ruimte te hoog komt te staan. Dit water kan dan middels een externe pomp afgepompt worden.

Klimaatinvloeden

Het is aannemelijk dat een onweersbui af en toe de brug passeert. Bij een windkracht hoger dan 7bft zal de brug niet meer gedraaid worden. De windsnelheid wordt gemeten en bij bediening op afstand gevisualiseerd. Tijdens mist of laagstaande zon kan er slecht zicht zijn op de brug door zowel de gebruikers als de bedieners. De brugwachter zal beslissen of hij nog voldoende zicht heeft om de brug te kunnen bedienen.

Overige grenzen

De brug ligt naast een onderwijsinstelling. De brug zal daardoor veel gebruikt worden door studenten (te voet of op de fiets).

3 Revisielog

Versie		Aanpassingen (aanpassingen t.o.v. de vorige versie in blauw)
1.0		Oorspronkelijke template opgesteld voor D&F
1.1	Nov 2014	Eerste aanpassingen naar RWS layout.
1.2	Juli 2017	Huisstijl Overheid en inhoud RWS specifieker gemaakt. Info en refs naar niet gepubliceerde NEN 6787 verwijderd.



BIJLAGE D – Bijlagen Bedrijfsvoering Elektrische Installaties

Vraagspecificatie Proces – Raamovereenkomst

Realisatie Variabel onderhoud stalen bruggen West Nederland Zuid
Project Over-Bruggen



Zaaknummer: **31196743**

Datum: 14 januari 2025

Bijlage D - Bijlagen Bedrijfsvoering Elektrische Installaties

Deze bijlagen gelden **generiek** voor alle Nadere Overeenkomsten.

- Bijlage D1 NEN 3140 Veiligheidshandboek Rijkswaterstaat
- Bijlage D2 NEN 3140 Veiligheidshandboek Rijkswaterstaat addendum
- Bijlage D3 NEN 3840 Veiligheidshandboek Rijkswaterstaat



Rijkswaterstaat
Ministerie van Infrastructuur en Milieu

NEN 3140 Veiligheidshandboek Rijkswaterstaat

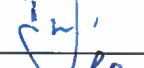
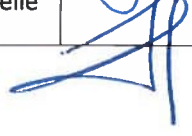
Werken met en aan laagspanningsinstallaties

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



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	Schermbank	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 hoogspanningsinstallaties]	22
5.6	Bedieningsdeskundige [alleen bij hoogspanningsinstallaties]	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 accuimten, accukasten en acculaadstations.....	33
8.3.4	Werkzaamheden in omgevingen met ontplofingsgevaar	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 voldoende 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 voldoende 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 voldoende 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 gevaarbron aanwezig is, alleen betreden mits hij onder toezicht staat van minimaal één voldoende 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 gevaarbron.

3.4.1 Werkzaamheden

Onder werkzaamheden verstaan we elke vorm van elektrotechnische of niet-elektrotechnische werkzaamheden waarbij een elektrische gevaarbron 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 gevarezone.

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

Toeziht 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

Toeziht 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 voortdurende controle van 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.

Definitie 5.2

Werkverantwoordelijke

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*).

Definitie 5.3

Vakbekwaam Persoon

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*).

Definitie 5.4

Voldoende Onderricht Persoon

(zie ook hoofdstuk 6)

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;



Opleiding / ervaring

- 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*).

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 voldoende 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 voldoende 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 voldoende 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 voldoende 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 voldoende 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 voldoende 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 voldoende 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 voldoende 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 voldoende 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 ingehuurd 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 waarschuwbord 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 voldoende onderricht zijn of moet onder toezicht van een vakbekwaam of voldoende onderrichte persoon staan.

Uitschakeling vóór of wederinschakeling na spanningsloos werken moet worden uitgevoerd door vakbekwame of voldoende 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 waarschuwborden nadat de volledige scheiding tot stand is gebracht. Er zal gezorgd moeten worden dat deze waarschuwborden niet onbedoeld worden verwijderd, bijvoorbeeld door een goede toegangsregeling voor de elektrische bedrijfsruimte waarin met waarschuwborden 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 accu-ruimten, 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.



Omhuulsels 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
- voldoende 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 gevaarbron 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 gevaarbron 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 aselekt, 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 onder spanning) 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:

- Beschikbaarheids-eisen 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 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

**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 juni 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



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



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	Schermbord	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	Hulprijst 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 voldoende 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 voldoende 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 gevaarbron aanwezig is, alleen betreden mits hij/zij onder toezicht staat van minimaal één voldoende 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 Gevaarzone

Onder de "gevaarzone" 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 gevarenszone.

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 gevarenszone.

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 gevarenszone.

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 **Schermb**

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 op 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 scheidsveld 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.

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).

Opleiding

Definitie

5.2

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. (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).

Definitie

5.3

Vakbekwaam Persoon [VP]

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 voldoende 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 voldoende 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 voldoende 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 voldoende 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 voldoende 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 voldoende 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 ingehuurd 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 waarschuwbord 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 voldoende 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 waarschuwborden nadat de volledige scheiding tot stand is gebracht. Er zal gezorgd moeten worden dat deze waarschuwborden 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 C13 worden 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 C13 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.

9.102 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 gevaarbron 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 ontleen 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 onder spanning) 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:

- Beschikbaarheidseisen 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 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 aardgamituren, 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 E – BEI van de Opdrachtgever

Vraagspecificatie Proces – Raamovereenkomst

Realisatie Variabel onderhoud stalen bruggen West Nederland Zuid
Project Over-Bruggen



Zaaknummer: **31196743**

Datum: 14 januari 2025

Bijlage E - Bedrijfsvoering Elektrische Installaties (BEI) van de Opdrachtgever

Deze bijlage 'Bedrijfsvoering Elektrische Installaties (BEI) van de Opdrachtgever' geldt **generiek** voor alle Nadere Overeenkomsten.



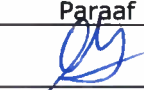
Handleiding

Bedrijfsvoering Elektrische Installaties

Invulling van de ARBO-verplichtingen inzake elektrische arbeidsveiligheid

Intern RWS-document

Datum 25 februari 2015
Versienummer 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
Vastgesteld	T.F.J. Van de Gazelle		13/3/15



Colofon

Uitgegeven door	Organisatorische Eenheden WVL en GPO
Informatie Project	G. Bruggink (GPO) Inrichting Bedrijfsvoering Elektrische Installaties
Uitgevoerd door	Martijn Faaij (Externe bij WVL), Gerrit Bruggink (GPO), Cees Wilschut (GPO)
Datum	25 februari 2015
Status	Definitief
Versienummer	2.0

Leden van werkgroep BEI:

Naam	Eenheid
Gerrit Bruggink	GPO
Cees Wilschut	GPO
Martijn Flinterman	GPO
Dirk de Groot	CD
Margriet Bentem	NN
Ab Brandsen	ON
Albert Buitenhuis	MN
Ron van den Ende	WNN
Peter Oskam	WNZ
Gert van Grinsven	PPO
Wies de Blok	ZD
André Smits	PPO
Paul Lemmens	ZN

Revisiehistorie

Versie	Datum	Beschrijving wijziging(en):	Gedistribueerd aan:
0.1	06-02-2012	Outline	
0.2	23-02-2012	Eerste concept	Werkgroep BEI
0.3	13-04-2012	Tweede concept	Werkgroep BEI
0.4	27-04-2012	Definitief concept Verwerking van review van de werkgroep BEI.	Opdrachtgever, PraBO coördinatoren, districtshoofden
0.5	01-06-2012	Definitief concept Verwerking van review van de werkgroep BEI.	LBB externe toetsing fase 2
0.6	19-06-2012	Verwerking van juridische review door mr. Drs. Ing. W. Moree van Joulz.	Intern
1.0	06-07-2012	Verwerking reviews J. Naber, P. Jansen en S. van der Linden. Verwerking n.a.v. gesprek met I. van der Hee.	Werkgroep BEI, opdrachtgever, PraBO coördinatoren, districtshoofden
1.1	30-11-2012	"Kader" vervangen door "Handleiding"	Werkgroep BEI, Opdrachtgever, PraBO coördinatoren, districtshoofden
1.2	29-05-2013	Enkele benamingen gesynchroniseerd	Opdrachtgever
1.3	08-07-2013	Aanpassingen aan OP2015, aanpassing BEI-organisatiemodel.	Opdrachtgever
2.0	25-02-2015	Afstemming met cursusboek BEI Definitief ter verspreiding binnen Rijkswaterstaat, overdracht aan COP BEI	RWS



Inhoud

1	Inleiding	4
1.1	Doel	4
1.2	Achtergrond	4
1.3	Leeswijzer	5
1.3.1	Documentstructuur	5
2	Uitgangspunten.....	7
3	Inrichting BEI Rijkswaterstaat	10
3.1	Opsplitsing verantwoordelijkheden Installatieverantwoordelijke.....	11
3.2	Technisch Installatieverantwoordelijke is in principe eigen personeel.....	13
3.3	COP BEI	14
3.3.1	Beheer	14
3.3.2	Opleidingen.....	14
3.3.3	Monitoring/toezicht	15
3.4	Mogelijkheid voor escalatie	15
3.5	Regionale Technisch adviseur/deskundige	15
3.6	BEI-organisatiemodel	15
3.7	Overige personen binnen de BEI	18
3.8	Gebouwen, objecten en arbeidsmiddelen.....	19
3.8.1	Gebouwen niet in eigendom van Rijkswaterstaat	19
3.8.2	Objecten die gebruikt worden door private partij	19
3.8.3	Objecten die beheerd worden door provincies, gemeenten of rederijen..	19
3.8.4	Arbidsmiddelen (anders dan zijnde objecten)	19
Bijlage A	Referenties	21
Bijlage B	Begrippen en afkortingen	22
Bijlage C	Taken, verantwoordelijkheden en bevoegdheden BEI	26
C.1	Installatieverantwoordelijke	26
C.2	Werkverantwoordelijke	28
C.3	Vakbekwaam Persoon	29
C.4	Voldoende Onderricht Persoon.....	29
C.5	Ploegleider (hoogspanningsinstallatie)	30
C.6	Bedieningsdeskundige (hoogspanningsinstallatie)	30
C.7	Leek	30
Bijlage D	Aanwijzingsformulieren.....	31
D.1	Functioneel Installatiebeheerder (F-IB)	31
D.2	Technisch Installatieverantwoordelijke (T-IV).....	31
D.3	Voldoende onderricht persoon (VOP)	31
	Aanwijzingsbrief F-IB.....	32
	Aanwijzingsbrief T-IV	34
	Aanwijzingsbrief VOP.....	36
Bijlage E	Toetsen van een (uitbestede) BEI	38
E.1	Toetsen ONB-werkplan BEI	38
E.2	Aanvangstoets.....	38
E.3	Periodieke toets.....	38
E.4	Herhalingstijd	38
E.5	Bevindingen en rapportage	39



1 Inleiding

1.1 Doel

Deze handleiding heeft tot doel invulling te geven aan de wettelijke verplichting van Rijkswaterstaat – als werkgever – de arbeidsveiligheid van de werknemer in de nabijheid van door RWS beheerde elektrische installaties, zoals elektrische installaties in de kunstwerken (tunnels, bruggen, sluizen, etc.) en langs de weg (wegkantstations, openbare verlichting, etc), en bij gebruik van elektrische arbeidsmiddelen te waarborgen. De elektrische arbeidsveiligheid wordt gewaarborgd door de inrichting van een adequate bedrijfsvoering van elektrische installaties (BEI).

Het primaire doel van deze inrichting is het voorkomen van ongevallen bij de werknemers van Rijkswaterstaat en werknemers van opdrachtnemers.

Daarnaast draagt het bij aan bedrijfsmatige efficiëntie en aan hogere beschikbaarheid elektrische installaties.

Onderliggend document geeft de randvoorwaarden voor de inrichting van de adequate bedrijfsvoering.

RWS conformeert zich voor de veilige bedrijfsvoering van elektrische installaties en elektrische arbeidsmiddelen zoveel mogelijk aan de normen NEN 3140:2011 en NEN 3840:2011.

1.2 Achtergrond

Bij het gebruik van en het werken in nabijheid of aan elektrische installaties en bij het gebruik van elektrische arbeidsmiddelen bestaat een zeker risico op letsel. Letsel kan worden veroorzaakt door onder andere:

- elektrische schokken;
- elektrische verbrandingen;
- brand voortkomend uit elektrische energie;
- explosies voortkomend uit elektrische energie; of
- krachten die vrijkomen bij kortsluitingen.

Om deze risico's te beperken moeten elektrische installaties en elektrische arbeidsmiddelen voldoen aan een groot aantal veiligheidseisen dat vermeld staat in verschillende normen, regels en richtlijnen.

Wettelijke verplichting

Als werkgever heeft Rijkswaterstaat vanuit de ARBO-wet (zie [Wetten.nl]) en EU richtlijn arbeidsmiddelen (zie Europese verordening en richtlijnen [Eurlex.europa.eu]) de verplichting te zorgen voor een veilige werkplek. Één van de aspecten die daarbij een belangrijke rol speelt is de veiligheid in de nabijheid van elektrische installaties en bij gebruik van elektrische arbeidsmiddelen. In het ARBO-besluit staan hierover de volgende relevante artikelen:

- Elektrische installaties zijn veilig (art. 3.4);
- Werkzaamheden aan, met en nabij installaties worden veilig uitgevoerd (art. 3.5).

De regels gelden zowel voor de werknemers van Rijkswaterstaat en opdrachtnemers die dagelijks gebruik maken van de installaties als de werknemers van Rijkswaterstaat en opdrachtnemers die gepland of incidenteel onderhoud plegen en/of projecten uitvoeren.



De veiligheid van elektrische installaties en elektrische arbeidsmiddelen kan worden gewaarborgd door het inrichten van een adequate bedrijfsvoering van elektrische installaties. Deze inrichting is vormvrij zolang de veiligheid conform de wettelijke verplichting gewaarborgd is. Door de BEI in te richten conform een geharmoniseerde (inter)nationale norm kan gebruik gemaakt worden van jarenlange ervaring en expertise die in zo'n norm is verankerd. Bovendien wordt zodoende gezorgd voor aansluiting met marktpartijen die werkzaamheden verrichten aan of in nabijheid van elektrische installaties van RWS.

Normen

De normen die richting geven aan de inrichting van de BEI zijn de NEN-EN 50110, met de nationale bijlagen [NEN 3140] (BEI - Laagspanning) en [NEN 3840] (BEI - Hoogspanning). De versies NEN 3140:2011 en NEN 3840:2011 hebben de NEN-EN 50110 integraal opgenomen.

Deze normen beschrijven onder andere een aantal functies die expliciet moeten worden toegewezen aan personen om de BEI adequaat in te richten (de veiligheid te waarborgen):

- Installatieverantwoordelijke;
- Werkverantwoordelijke;
- Vakbekwaam persoon;
- Voldoende onderricht persoon;
- Ploegleider (alleen NEN 3840);
- Bedieningsdeskundige (alleen NEN 3840);
- Leek.

De normen beschrijven onder andere opleidingseisen en de taken, verantwoordelijkheden en bevoegdheden die personen met bovengenoemde functies hebben. De toewijzing van functies moet expliciet via schriftelijke aanwijzing plaatsvinden.

NB. Het Rijksfunctiegebouw kent deze functies niet, hierdoor noemen wij deze NEN 3140-functies in deze handleiding "Titels".

Zie Bijlage C voor een verdere toelichting.

Uniforme werkwijze

Er is behoefte aan een uniforme werkwijze bij de inrichting van de BEI:

- Vanuit efficiëntie: voor elke regio of district worden (noodgedwongen) eigen oplossingen gekozen omdat een landelijk ontbreekt. Dit leidt tot niet-uniforme werkwijzen, uitrustingen en inrichting en leidt tot minder efficiënte inzet van middelen;
- Vanuit veiligheid: Een standaard inrichting van de BEI draagt bij aan veilige arbeidsomstandigheden.
- Vanuit beschikbaarheid: De BEI draagt bij aan standaardisatie van aandachtspunten doordat de diverse Organisatorische Eenheden meer informatie gaan uitwisselen en ervaringen gaan delen. Dit laatste leidt tot het gebruik oplossingen op het gebied van processen en/of technische oplossingen. Goed werkende en beproefde processen en technische oplossingen leiden tot verbetering van de beschikbaarheid.

1.3 Leeswijzer

1.3.1 Documentstructuur

Dit document kent de volgende hoofdstukindeling:

Hoofdstuk 1	Is de inleiding op het document;
Hoofdstuk 2	Beschrijft de uitgangspunten die worden gehanteerd bij de uitwerking van de BEI;



Hoofdstuk 3 Geeft de richtlijnen voor de inrichting van BEI binnen Rijkswaterstaat.

Dit document kent de volgende bijlagen

Bijlage A	Beschrijft de in dit document aangehaalde documenten;
Bijlage B	Geeft een toelichting op gebruikte begrippen en afkortingen;
Bijlage C	Beschrijft de taken, verantwoordelijkheden en bevoegdheden binnen BEI aan de hand van de normen NEN 3140 en NEN 3840;
Bijlage D	Bevat templates voor aanwijzingsformulieren voor de verschillende titels binnen BEI;
Bijlage E	Bevat procedures voor het toetsen van een (externe) BEI.



2 Uitgangspunten

In dit hoofdstuk staan de belangrijkste uitgangspunten die ten grondslag liggen aan een adequate bedrijfsvoering van elektrische installaties centraal. Hierbij gaat het om die uitgangspunten die dermate essentieel zijn voor de bedrijfsvoering van elektrische installaties dat ze in deze handleiding thuishoren. In hoofdstuk 3 worden deze uitgangspunten waar nodig verder uitgewerkt. De volgende uitgangspunten en acties komen tegemoet aan de organisatiebehoeften en aan reductie van knelpunten:

1. Binnen Rijkswaterstaat is de HID van een Landelijke of Regionale Eenheid – als hoogste ARBO-verantwoordelijke binnen zijn of haar Eenheid - verantwoordelijk voor het vormgeven van de inrichting van een adequate bedrijfsvoering van elektrische installaties. Rijkswaterstaat heeft de verantwoordelijkheden in het kader van ARBO vastgelegd in het [Handboek arbo]. De HID van een Landelijke of Regionale Eenheid wordt hierin aangewezen als hoogste ARBO-verantwoordelijke binnen zijn of haar Eenheid. Aangezien de elektrische arbeidsveiligheid onderdeel is van de ARBO, valt het inrichten van een adequate BEI onder de verantwoordelijkheid van de HID.
2. Rijkswaterstaat conformeert zich zoveel mogelijk aan de normen die gelden voor een adequate inrichting van de bedrijfsvoering van elektrische installaties.
Bij de inrichting van een adequate BEI conformeert Rijkswaterstaat zich aan de normen [NEN-EN 50110], [NEN 3140] en [NEN 3840]. Waar nodig kiest Rijkswaterstaat een specifieke inrichting die past binnen het beleid van de eigen organisatie. De punten 3 t/m 9 gaan hier verder op in.
3. 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.



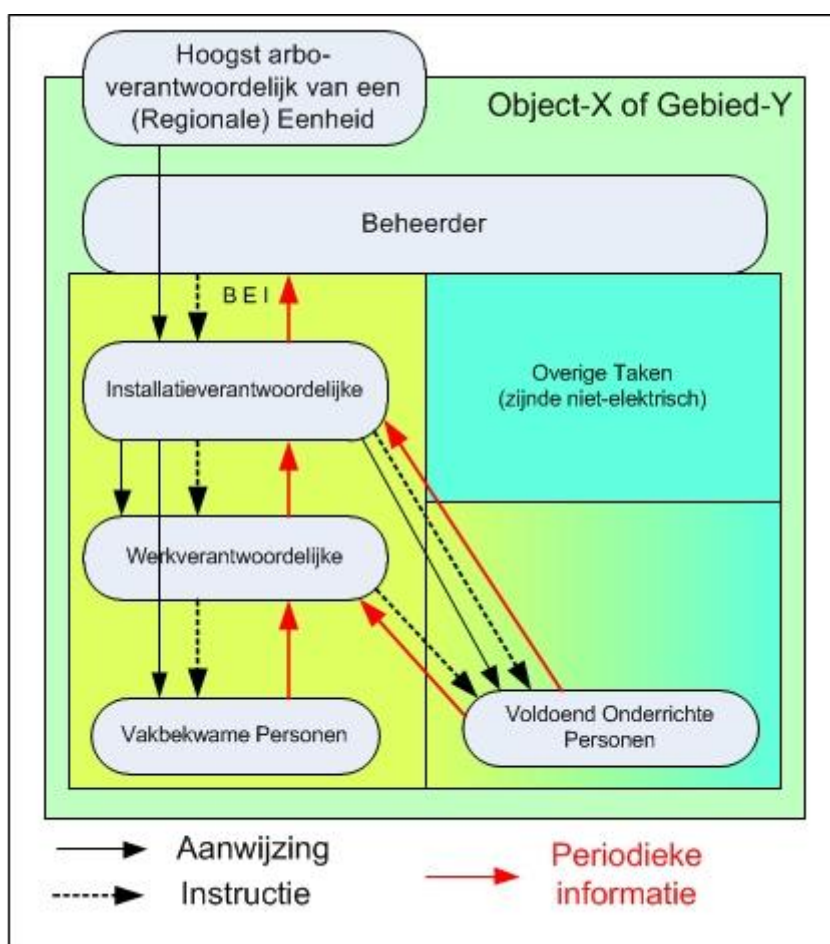
4. Rijkswaterstaat kiest ervoor de F-IB en T-IV in principe bij eigen personeel te beleggen.
Zodra het areaal tijdens werkzaamheden is opengesteld voor primaire processen is het van belang dat RWS invloed heeft op de uitvoering van de BEI. In die gevallen moeten de taken en verantwoordelijkheden van de F-IB bij de objectbeheerder zijn belegd. In de huidige RWS-organisatie is de objectbeheerder het districtshoofd (areaal district) of een afdelingshoofd (gebouwen, ICT, ...).
In principe wordt de T-IV binnen RWS worden belegd, behalve bij DBFM. In bestaande situaties kan hiervan afgeweken worden als dit nog niet in te regelen valt.
Als het areaal tijdens werkzaamheden voor langere tijd buiten gebruik is genomen, kunnen de taken en verantwoordelijkheden van de IV worden belegd bij de opdrachtnemer.
5. Rijkswaterstaat kiest verschillende organisatiemodellen voor de inrichting van de BEI passend bij verschillende contractvormen en typen installaties.
Er worden verschillende organisatiemodellen gekozen voor prestatiecontracten, Design & Construct contracten en DBFM contracten. Bovendien zijn er een aantal typen installaties die een afwijkend organisatie-model vereisen.
6. Rijkswaterstaat belegt het beheer van het kader, opleidingen en monitoring /toezicht op uitvoering van de BEI bij de COP BEI. Om de BEI Rijkswaterstaat-breed uniform in te richten en ingericht te houden is het belangrijk om op landelijk niveau een aantal zaken te regelen.
Het betreft taken als beheer, opleidingen en monitoring/toezicht.
7. Rijkswaterstaat richt een landelijk overleg in.
De inrichting van een landelijk overleg zorgt ervoor dat de verschillende T-IV, regionale adviseurs/deskundigen en mensen van de COP BEI ervaringen met elkaar kunnen delen. Daarnaast kunnen mensen uit de regio voorstellen doen voor veranderingen in de RWS BEI. F-IB's hebben de mogelijkheid om waar nodig hierbij aan te sluiten.
8. Rijkswaterstaat kiest voor een expliciete escalatiemogelijkheid voor de T-IV.
Indien de F-IB in de ogen van de T-IV niet voldoende maatregelen neemt om de BEI op een voldoende veilig niveau te houden, kan de T-IV escaleren.
Een interne T-IV kan escaleren naar de verantwoordelijke directeur. Een externe T-IV kan in eerste instantie escaleren naar het IPM-team en in tweede instantie kan de contractverantwoordelijke van de opdrachtnemer escaleren naar de contractverantwoordelijke van de opdrachtgever.
9. De F-IB wordt bijgestaan door een technisch adviseur /deskundige. Aangezien het van de F-IB niet wordt gevraagd dat uitgebreide elektrotechnische kennis aanwezig is, wordt hij – in het geval de T-IV bij een marktpartij is belegd – voor bepaalde keuzes op technisch gebied bijgestaan door een regionaal of landelijk technisch adviseur/deskundige.



10. Voor uitvoering van de elektrotechnische werkzaamheden is een NEN 3140 Veiligheidshandboek RWS opgesteld. Deze geeft voor zowel interne als externe medewerkers van Opdrachtnemers aanwijzingen hoe te handelen ten einde aan de BEI te voldoen.

3 Inrichting BEI Rijkswaterstaat

Binnen Rijkswaterstaat is de HID verantwoordelijk voor het vormgeven van de inrichting van een adequate bedrijfsvoering van elektrische installaties (*Uitgangspunt 1*). Rijkswaterstaat conformeert zich daarbij aan de normen [NEN-EN 50110], [NEN 3140] en [NEN 3840] (*Uitgangspunt 2*). In dit hoofdstuk wordt aangegeven hoe de norm wordt toegepast binnen Rijkswaterstaat. Voor verschillende situaties (contractvormen, type object) is een eigen inrichting nodig.



Figuur 1: Standaard inrichting van BEI conform [NEN 3140].

Toepassing NEN normen

De hoogste ARBO-verantwoordelijke dient er zorg voor te dragen dat de beheerder van een object of gebied hieraan een goede invulling geeft en kan geven. Hiervoor is het noodzakelijk een vertaling te maken van de in de NEN normen geschetste functies naar functionarissen binnen de RWS organisatie en de diverse contractvormen met bijbehorende taken en verantwoordelijkheden en risico's voor RWS en de ON.



3.1 Opsplitsing verantwoordelijkheden Installatieverantwoordelijke

De TV&B van de Installatieverantwoordelijke (zie Bijlage C.1) worden opgedeeld naar een functionele en een technische verantwoordelijkheid (*Uitgangspunt 3*).

Maatschappelijk belang netwerken

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.

Belang netwerk vs 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.

Opsplitsen in F-IB en T-IV

In het beleid voor het uitvoeren van een goede BEI is er gekozen voor opsplitsing van de taken en verantwoordelijkheden van de IV naar een functionele installatiebeheerder [F-IB] en een technische installatieverantwoordelijke [T-IV]. De taken hiervan worden hierna ingevuld en kunnen naar behoefte per object opnieuw worden verdeeld als maar per object is beschreven wie waar verantwoordelijk voor is. De eindverantwoordelijkheid van de BEI van de objecten ligt bij de F-IB.

F-IB

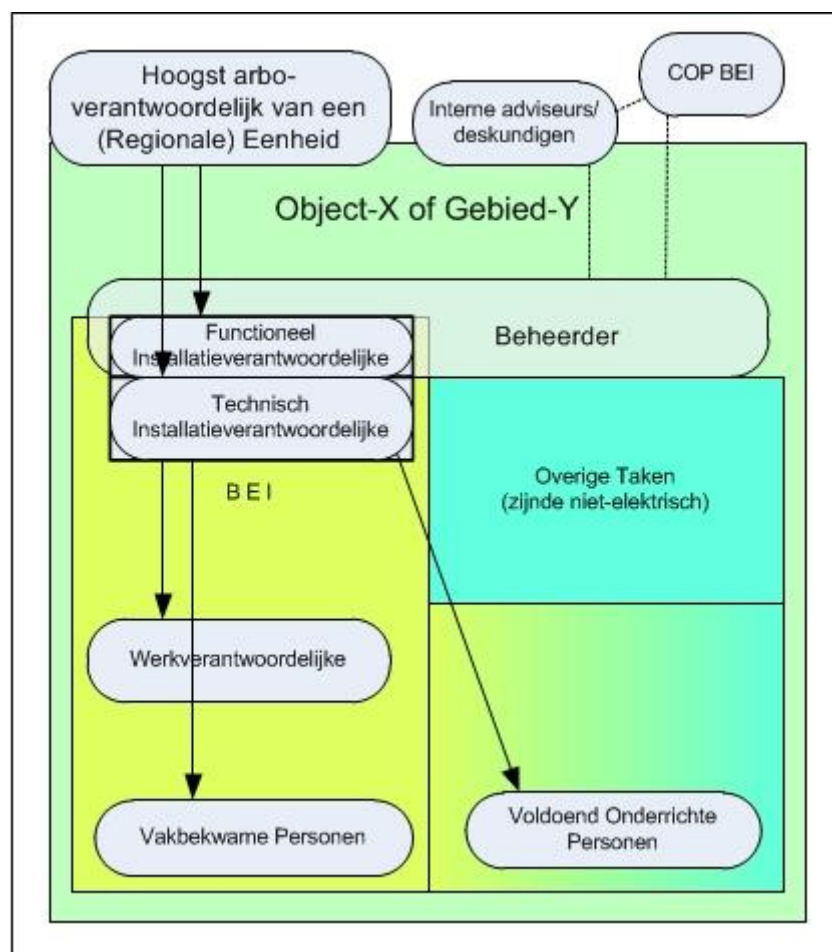
De verdeling van de taken over de F-IB en T-IV moet zo zijn, dat voor de taken en verantwoordelijkheden van F-IB geen specifieke kennis van de elektrotechniek noodzakelijk is, maar alleen organisatorische (functionele). De F-IB kan zich waar nodig inhoudelijk bij laten staan door interne adviseurs/deskundigen vanuit de COP BEI (landelijke steunpunt inzake BEI) (zie paragraaf 3.5 en 3.3). De F-IB vertegenwoordigt in ieder geval de maatschappelijke belangen van de netwerken en kan daarom niet worden uitbesteed.

T-IV

De specifieke kennis van elektrotechniek en de installaties zit bij de T-IV. De T-IV vertegenwoordigt in ieder geval de arbeidsveiligheid van de elektrische installaties en elektrische arbeidsmiddelen.

Bij langere afwezigheid van de T-IV wordt in overleg met de F-IB een "gedelegeerd-T-IV" door de T-IV aangesteld, die alle verantwoordelijkheden van de T-IV gedurende diens afwezigheid heeft.

In onderstaande figuur is de relatie tussen de verschillende titels inzichtelijk gemaakt:



Figuur 2: Inrichting van BEI met opgesplitste titels voor IV.

(de pijlen voor instructie en periodieke informatie (zie Figuur 1) zijn hier bewust weggelaten)

Gedeelde
verantwoordelijkheid,
werkverantwoordelijke
vast onderhoud
coördineert

Wanneer meerdere opdrachtnemers werkzaamheden (bijv. vast onderhoud en variabel onderhoud) uitvoeren aan een object en/of deelgebied is er veelal sprake van elektrische installaties die zich in nabijheid van elkaar bevinden of zelfs met elkaar verbonden zijn. In zulke gevallen is het van belang dat de verantwoordelijken van de betrokken partijen (T-IV en WV) met elkaar communiceren en dat een coördinerend werkverantwoordelijke wordt benoemd (conform NEN 3140 en NEN 3840 par. 4.3). De opdrachtnemer van het vast onderhoud wordt aangewezen als coördinerende partij.

Opleidingen

De F-IB is er verantwoordelijk voor dat de noodzakelijke opleidingen en trainingen door de personen van zijn organisatie, die te maken hebben of krijgen met de BEI, worden gevolgd. Indien de T-IV is belegd bij een persoon buiten de organisatie, zal de T-IV er op moeten toezien dat de personen die – binnen zijn eigen organisatie – onder hem vallen de noodzakelijke opleidingen, trainingen en/of instructies krijgen voor de elektrische installatie waaraan ze verbonden zijn.



Aanwijzing RWS-
personeel als VOP

De externe T-IV heeft te maken met RWS-personeel dat binnen het object of gebied werkzaam is en mogelijk blootgesteld wordt aan elektrische gevaren (zie ook paragraaf 3.7). De externe T-IV heeft de verantwoordelijkheid dit RWS-personeel als VOP te instrueren, mits deze is aangewezen door de bevoegde RWS-functionaris.

Rapportage

De F-IB is verantwoordelijk voor toezicht op de verplichting tot schriftelijke rapportage waaraan de T-IV dient te voldoen in overeenstemming met de BEI. Dit toezicht kan worden uitgevoerd door een interne of externe toetser.

Communicatie

Communicatie omvat elke wijze van overdracht van informatie naar personen. Overdracht van informatie kan op de volgende wijzen plaatsvinden:

- mondeling;
- schriftelijk;
- visueel.

Alle informatie die nodig is voor een veilige bedrijfsvoering moet worden gecommuniceerd.

Daarnaast zal de T-IV ten minste 2 maal per jaar de F-IB informeren over de status van de veiligheid van de elektrische installatie van elk object of gebied dat onder zijn beheer valt. Bij calamiteiten en incidenten zal dit direct geschieden.

3.2 Technisch Installatieverantwoordelijke is in principe eigen personeel

Uitgangspunt is dat waar Rijkswaterstaat de verantwoordelijkheid draagt voor het beheer van zijn objecten, de taken en verantwoordelijkheden van de T-IV bij het eigen personeel worden belegd (*Uitgangspunt 4*).

Hierbij treedt het probleem op dat niet altijd personeel beschikbaar is met de juiste opleiding en ervaring. Wanneer geen bekwaam personeel beschikbaar is kunnen de taken en verantwoordelijkheden van de T-IV (tijdelijk) bij een marktpartij worden belegd. Hierbij is het van belang om te bepalen wat het risico is dat wordt gelopen wanneer de taken en verantwoordelijkheden van de T-IV wordt uitbesteed. Zo moet bij faalkansgerelateerde objecten (Stormvloedkeringen, zoals bijv. de Oosterscheldekering of Maeslantkering), de regie en verantwoordelijkheid binnen de eigen organisatie worden gehouden. In deze gevallen mogen de taken en verantwoordelijkheden van de T-IV niet in de markt worden gezet.

De controle op de uitvoering van uitbesteede taken zal door middel van toetsen door het IPM-team moeten worden uitgevoerd. Wanneer het een contract betreft waar geen IPM-team is betrokken ligt de verantwoordelijkheid voor controle bij de objectbeheerder.

De toetsing op het functioneren van de T-IV bij een opdrachtnemer door het IPM-team dient op aangeven van de objectbeheerder te geschieden. Hierbij mag een risicoafweging in kader van tijd en geld geen doorslaggevende rol zijn. De objectbeheerder is vertegenwoordigd bij de voorbereiding van de toets op het functioneren van T-IV.

NB Bedenk dat Veiligheid niet valt uit te besteden. Veiligheid is een verantwoordelijkheid van de opdrachtgever en de opdrachtnemer samen (zie Klaver 5 uit [Kader Veiligheidsmanagement]).



3.3 COP BEI

Om de BEI Rijkswaterstaat-breed uniform in te richten en ingericht te houden is het belangrijk om op landelijk niveau een aantal zaken te regelen (*Uitgangspunt 6*).

Het betreft taken als:

- Beheer documenten;
- Opleidingen;
- Monitoring/toezicht.

De COP BEI wordt bemenst door deskundigen uit de diverse Landelijke en Regionale Eenheden.

De samenstelling bestaat uit een aantal mensen vanuit de verschillende Landelijke en Regionale Eenheden onder leiding van een voorzitter met gezag. De taken worden in navolgende paragrafen toegelicht.

3.3.1 Beheer

Om de BEI actueel te houden is het van belang deze te beheren. Het beheer van de BEI is een taak van de COP BEI.

Onder het beheer vallen de verantwoordelijkheden om:

- Ontwikkelingen op het gebied van wet- & regelgeving (specifiek het ARBO-besluit) te volgen en de BEI aan te passen op wijzigingen;
- Ontwikkelingen op het gebied van normen (specifiek NEN 3140 en NEN 3840) te volgen en de BEI aan te passen op wijzigingen;
- Ontwikkelingen op het gebied van RWS beleid (bijv. nieuwe vormen van contracten) te volgen en de BEI aan te passen op wijzigingen;
- Ontwikkelingen op het gebied van de RWS organisatie (bijv. OP2015) te volgen en de BEI aan te passen op wijzigingen.

Doel van het beheer van de BEI is het blijven garanderen van de arbeidsveiligheid binnen de wettelijke verplichtingen, conformerend aan de geldende normen, passend op het RWS beleid en de RWS organisatie.

3.3.2 Opleidingen

Om de BEI goed in te richten moeten de aangewezen personen hun kennis aantoonbaar op peil brengen en houden. Hiertoe moeten er opleidingen en trainingen worden ontwikkeld of ingekocht. Het zorgen voor beschikbaarheid van opleidingen en trainingen is een landelijke taak.

Er moet in samenwerking met het Corporate Learning Centre (CLC) een curriculum opgezet en beheerd worden.

Daarnaast dient training op het bewuste object(en) en gedegen actuele kennis van het object geborgd te zijn en gehouden te worden, zowel binnen Rijkswaterstaat als bij opdrachtnemers.

“Training in het werk”, bijvoorbeeld het periodiek instructie voor behoud van schakelbevoegdheid in hoogspanning, zal worden uitbesteed aan specialistische opleidingsinstituten.

Binnen de Regionale Eenheden en zijn de F-IB verantwoordelijk voor de opleidingsplannen van T-IV, WV, VP en VOP, voor zover deze personen in dienst zijn bij Rijkswaterstaat.



3.3.3 Monitoring/toezicht

Om zeker te stellen dat de BEI – en daarmee de wettelijke verplichting – wordt nageleefd, moet op naleving worden toegezien. Het is een taak van de COP BEI om toe te zien op de naleving van de BEI door de Regionale Eenheden. Dit kan worden ingevuld door het opleggen van een rapportageverplichting aan de Regionale Eenheden en het (laten) uitvoeren van audits. De rapportage van de audit gaat naar de HID van de regio. Bevindingen uit de audit zullen moeten worden opgevolgd. Afhankelijk van de aard en ernst van de bevindingen moeten er maatregelen worden getroffen. Twee weken na de bevindingen zal er een verbetermaatregel en een plan van aanpak gereed moeten zijn. Één maand na de bevinding zal opnieuw getoetst worden. Bij het niet opvolgen van de maatregelen zal geëscaleerd worden naar de DG.

3.4 Mogelijkheid voor escalatie

Indien de F-IB in de ogen van de T-IV niet voldoende maatregelen neemt om de BEI op een voldoende veilig niveau te houden, kan de T-IV escaleren (Uitgangspunt 8).

Wanneer de taken en verantwoordelijkheden van de T-IV binnen RWS zijn belegd kan rechtstreeks naar de verantwoordelijke directeur van de betreffende Eenheid.

Indien de T-IV is uitbesteed aan een opdrachtnemer, dan kan de T-IV van de opdrachtnemer rechtstreeks contact opnemen met het IPM-team dat het contract beheerst. Escaleert het IPM-team niet dan kan de T-IV escaleren naar de ondertekenaar van het ON-deel van het contract, zodat deze escaleert naar de ondertekenaar van het OG-deel van het contract

Doel hiervan is het bewust krijgen van de status van de elektrische arbeidsveiligheid binnen de organisatie.

3.5 Regionale Technisch adviseur / deskundige

De technische adviseur/deskundige adviseert de F-IB bij het nemen van beslissingen op technisch gebied (Uitgangspunt 9).

De technische adviseur/deskundige moet in staat zijn de werkzaamheden en/of adviezen van een T-IV van de opdrachtnemer of van het eigen personeel (collegiale toets) te beoordelen. Hij moet minstens op hetzelfde technische niveau kunnen opereren als de T-IV.

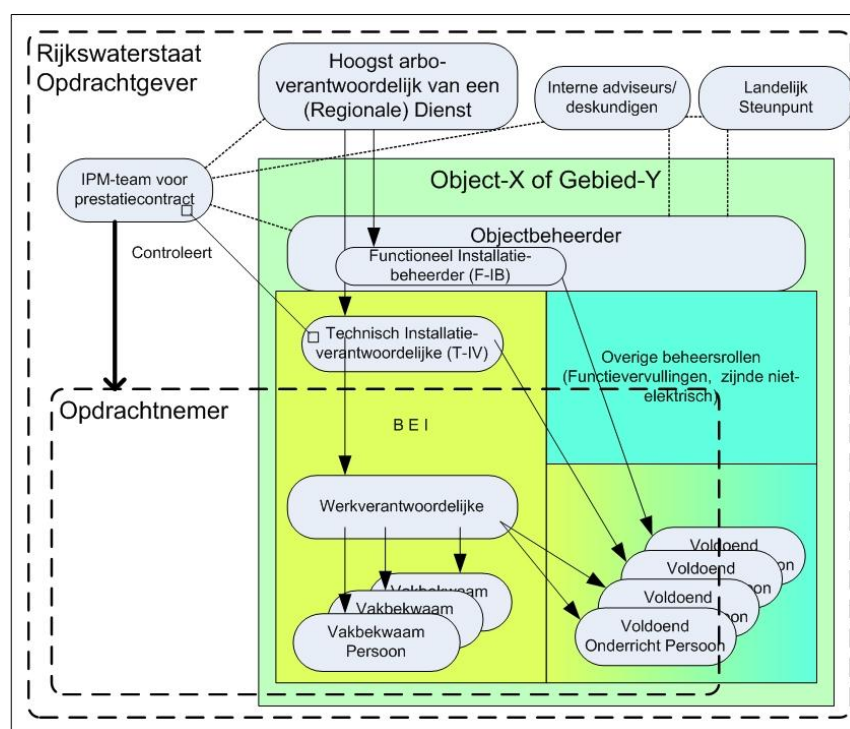
De technische adviseur/deskundige komt uit de RWS organisatie of is een onafhankelijk (ingehuurd) adviseur.

De technische adviseurs/deskundigen moeten de bereidheid hebben om buiten de eigen Eenheid te adviseren.

De technische adviseurs worden niet aangewezen als IV/WV/VOP, tenzij dit voor specifieke taken die zij daar uitvoeren bij objecten nodig is.

3.6 BEI-organisatiemodel

De HID van een Landelijke of Regionale Eenheid is binnen de Eenheid verantwoordelijk voor de arbeidsomstandigheden (ARBO). Vanuit deze verantwoordelijkheid heeft de HID de taak om een adequate BEI in te richten als invulling van de wettelijke verplichting uit het ARBO-besluit. De HID is verantwoordelijk voor het aanwijzen van de functionele installatieverantwoordelijke(n).



Figuur 3a: BEI-Organisatiemodel (RWS T-IV)

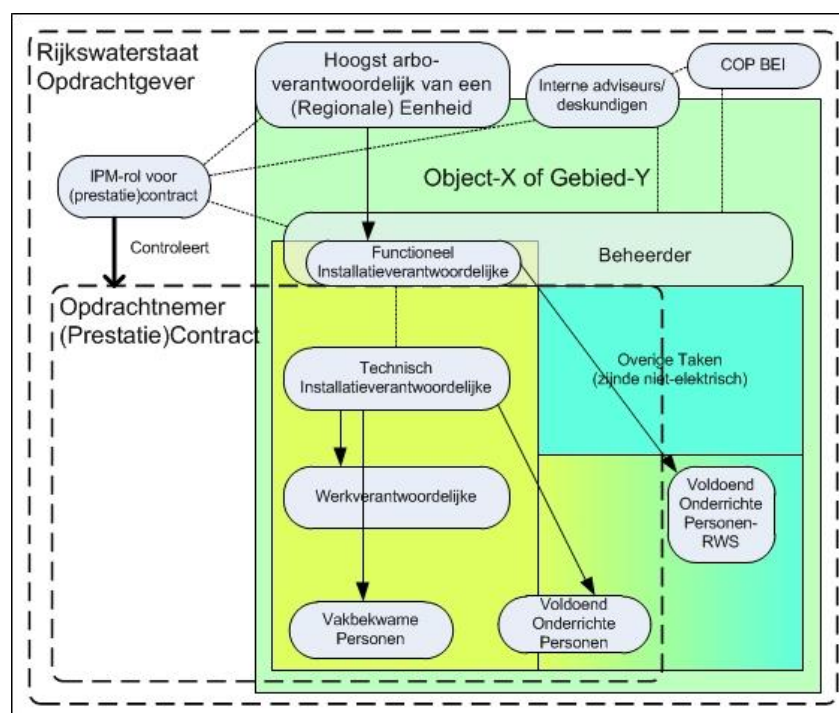
Zodra er werk wordt uitbesteed, zal dit op basis van een contract geschieden. Verder dient bij overdracht van T-IV naar een externe partij (rechtspersoon) geregeld te worden dat de rechtspersoon een natuurlijk persoon aanwijst. De verschillende contractvormen geven verschillende wijze van benoemingen van F-IB en T-IV (*Uitgangspunt 5*).

De volgende contractvormen worden onderscheiden:

- Prestatiecontract;
- Engineering en Construct (E&C);
- Design en Construct (D&C);
- Design Build Finance Maintain (DBFM).

Uitgangspunten:

1. F-IB wordt door opdrachtgever ingevuld.
 2. T-IV kan tijdens aanleg/groot onderhoud (D&C-contact, mits vrij van primaire processen) bij de opdrachtnemer, maar eventueel ook in de beheerfase (uitfasen).
 3. T-IV bij DBFM contracten ligt bij de opdrachtnemer.
- In dit geval ziet het organisatiemodel er als volgt uit:



Figuur 3b: BEI-Organisatiemodel (externe T-IV)

Invulling van de titels:

- F-IB
 - De HID wijst de objectbeheerder aan;
 - De objectbeheerder wordt aangewezen als F-IB. In de huidige RWS-organisatie is de objectbeheerder het districtshoofd (areaal district) of een afdelingshoofd (gebouwen, ICT, ...). De bevoegde RWS-functionaris wijst de T-IV aan, tenzij deze bij de ON wordt belegd. In dat geval stemt de F-IB, na overleg met de ON en het IPM-team over de geschiktheid van de natuurlijke persoon, in met de aanwijzing door de ON.
- T-IV
 - Een beschikbare medewerker van de opdrachtgever van het contract wordt aangewezen door of namens de HID als T-IV. De T-IV neemt deel aan het technische team van het IPM-team. De T-IV doet voorstellen t.b.v. technische aanpassing van de installaties en beoordeelt voorstellen van de opdrachtnemer en beslist hierover. De beslissing van de T-IV moet worden overgenomen door het IPM-team en de F-IB en gecontracteerd worden bij de opdrachtnemer.
De T-IV moet instemmen met de aanwijzing van de WV van de opdrachtnemer. De RWS-T-IV bewaakt de aanwijzingen van de WV, VP en VOP door de ON;
 - Als er geen medewerker van opdrachtgever beschikbaar is of in het geval van een D&C- of DBFM-contract zal een medewerker van de opdrachtnemer van het contract worden aangewezen als T-IV door de opdrachtnemer. Deze persoon wordt aangedragen door de opdrachtnemer en moet over het juiste kennis- en ervaringsniveau beschikken. Deze externe T-IV doet voorstellen t.b.v. technische aanpassing van de installaties en de F-IB (bijgestaan door de interne deskundigen) beoordelen de voorstellen van de opdrachtnemer en beslist hierover. De beslissing van de F-IB moet worden overgenomen door het IPM-team en



het IPM-team zorgt voor het contracteren bij de opdrachtnemer en bewaakt de uitvoering hiervan.

- IPM team
 - Het IPM team is verantwoordelijk voor de beheersing van het contract door middel van SCB (Systeemgerichte Contractbeheersing). Het IPM team ziet toe of de opdrachtnemer bij uitbesteding van T-IV een Werkplan-BEI (zie NEN 3140 Veiligheidshandboek RWS) opzet overeenkomend het contract (zie Bijlage E) en eerst hierna kan de Objectbeheerder instemmen met de opdrachtnemer als T-IV en ontheft de voorgaande T-IV schriftelijk van zijn taak in deze;
 - Het IPM team controleert de opdrachtnemer op naleving van de BEI en het kwaliteitsdocument van de opdrachtnemer waarin hij het proces van elektrische bedrijfsvoering beschrijft (zie Bijlage E);
 - Indien er werkzaamheden plaatsvinden in het kader van verschillende contracten op hetzelfde object, zal het IPM-team zorgdragen dat in één van de contracten er één coördinerend T-IV is. Deze zal de overlapping- en raakvlakbeheersing tot zijn taak krijgt. In de overige contracten moet de verplichting tot afstemmen zijn geregeld.
- WV
 - Normaal gesproken is dit de WV van de opdrachtnemer van het prestatiecontract (zie ook paragraaf 3.1).
 - Indien er werkzaamheden plaatsvinden in het kader van verschillende contracten op hetzelfde object, zal het IPM-team zorgdragen dat in één van de contracten er één coördinerend WV is. Deze zal de overlapping- en raakvlakbeheersing tot zijn taak krijgt. In de overige contracten moet de verplichting tot afstemmen zijn geregeld.
- VOP
 - In het geval van personeel van Rijkswaterstaat (bijvoorbeeld wegininspecteurs) dat dienst doet binnen het areaal van de opdrachtnemer, zal deze een aparte aanwijzing voor hun werkzaamheden krijgen. Bij een externe T-IV betekent dat, dat deze medewerkers worden aangewezen door de bevoegde RWS-functionaris (zie ook paragraaf 3.7) en instructie krijgen van de externe T-IV. Het is de bedoeling dat een gevaarlijke situatie kan worden onderscheiden en indien mogelijk op eenvoudige wijze kan worden voorkomen. Er is echter geen werkgeversrelatie tussen de opdrachtnemer het RWS-personeel.

Belangrijkste reden voor aanwijzing van een F-IB binnen Rijkswaterstaat is de verantwoordelijkheid van de objectbeheerder voor het presteren van het areaal. De objectbeheerder draagt verantwoordelijkheid voor risicogestuurde borging van het prestatieniveau en de veiligheid van de objecten, continuïteit van het areaalbeheer en aansluiting in de zogenaamde raak- en koppelvlakken ten behoeve van integrale RWS-processen, -belangen en -verantwoordelijkheden. De elektrische arbeidsveiligheid is slechts één van de vele aspecten die hierin een rol spelen (zie ook [Leidraad integrale veiligheid]). Het is niet wenselijk dat een opdrachtnemer een maatregel neemt t.b.v. de elektrische arbeidsveiligheid zonder dat de belangen van de RWS netwerken hierin zijn gekend.

3.7 Overige personen binnen de BEI

Machinist op (zee)schip

Voor de machinisten op (zee)schepen gelden, indien geen specifieke voorschriften beschikbaar zijn, de NEN 3140 en NEN 3840. *(bron: NEN 3140 en NEN 3810, par. 1 Zij worden in dat geval door de beheerder van de schepen aangewezen als Vakbekwaam Persoon, daar zij in het geval van uitvoeren van reparatieklussen op zee opgeleid moeten zijn.)*



Weginspecteur en mobiel
verkeersleider

Mensen die in de praktijk, bijvoorbeeld bij incidenten, te maken kunnen krijgen met onderspanning staande delen moeten die kunnen herkennen en, zo mogelijk, veiligstellen. Dit betekent dat deze mensen daarvoor moeten worden opgeleid, getraind en/ of instructie voor hebben gehad. Deze mensen, vaak weginspecteurs en mobiel verkeersleiders moeten worden benoemd als VOP.

Bij de uitbesteding van een vaarweg en/of autoweg/rijksweg kan een weginspecteur of mobiel verkeersleider van Rijkswaterstaat aangewezen worden door een opdrachtnemer.

3.8 Gebouwen, objecten en arbeidsmiddelen

3.8.1 *Gebouwen niet in eigendom van Rijkswaterstaat*

Van de gebouwen die niet in eigendom zijn van RWS moeten de vaste elektrische installaties periodiek worden geïnspecteerd door de eigenaar van de gebouwen/installaties (Rijksgebouwendienst of private partij). RWS is mede verantwoordelijk voor een veilige BEI en het contractteam dient zich er van te vergewissen of dit soort inspecties plaatsvinden. De verplaatsbare installaties en apparatuur binnen de gebouwen en eigendom van RWS dient RWS zelf te laten inspecteren. De inspectiefrequentie wordt bepaald aan de hand van de handvatten die de NEN normen hiervoor bieden (zie NEN 3140 Bijlage I.)

3.8.2 *Objecten die gebruikt worden door private partij*

Er zijn objecten in eigendom van Rijkswaterstaat die door een andere partij worden gebruikt. Het betreft bijvoorbeeld een aantal van de inrichtingen op de complexen van aanleginrichtingen voor veerponten waarvan het Rijk concessies uitgeeft.

NB de gebouwen op de aanleginrichting terreinen zijn gebouwd in opdracht van reder en zijn eigendom van de reder (zie paragraaf 3.8.1).

De aanleginrichtingen en terreinen worden door middel van een huurovereenkomst aan de gebruiker ter beschikking gesteld. Hierbij zal het Beheer en Onderhoud bij RWS blijven en in een prestatiecontract worden ondergebracht. De gebouwen van derden vallen buiten deze concessie.

3.8.3 *Objecten die beheerd worden door provincies, gemeenten of rederijen*

Binnen RWS kennen we nog een groot aantal objecten, waarbij het beheer en bediening is ondergebracht bij een provincie, gemeente of ProRail. Zij krijgen hiervoor een periodieke vergoeding. Er is geen IPM-projectteam dat deze objecten en de BEI ervan controleert. Deze objecten kunnen worden beschouwd als gebouwen waarbij RWS de eigenaar is en de provincie of gemeente de gebruiker (zie paragraaf 3.8.1).

De hoogst ARBO-verantwoordelijke van RWS wijst, afhankelijk van de gebruiksovereenkomst, of iemand van RWS of iemand van de gebruikende partij aan als F-IB. De taken en verantwoordelijkheden van de T-IV kunnen bij deskundig eigen personeel (indien beschikbaar) worden belegd of een marktpartij. Bij de rederij wordt door de F-IB een Werkverantwoordelijke aangewezen, die zorgt draagt voor het uitvoeren van een adequate BEI. RWS zal moeten toetsen, afhankelijk van de overeenkomst via SCB of anderszins, of wordt voldaan aan de BEI.

3.8.4 *Arbeidsmiddelen (anders dan zijnde objecten)*

Arbeidsmiddelen moeten gekeurd worden conform NEN 3140. Het betreft arbeidsmiddelen die zijn verbonden met het elektriciteitsnet door middel van een



wandcontactdoos en stekker. Deze zijn eenvoudig te scheiden van het elektriciteitsnet waarna ze spanningsloos zijn en daarmee (elektrisch) veilig. RWS dient aantoonbaar te maken dat er een RI&E is, compleet met een inspectierapporten en een verbeterplan.

Ten behoeve van storingswachtdienst moeten er bedieninstructies, onderhoudsinstructies, werkinstructies en huisregels beschikbaar zijn, zodat alle onderhouds- en bedieningspersoneel (in/extern) weet wat ze moeten doen en wat er van ze verwacht wordt.



Bijlage A Referenties

In dit document wordt gerefereerd aan een aantal andere documenten:

Referentie	Titel	Versie (status)	Datum
[Wetten.nl]	Nederlandse wet- & regelgeving (http://www.wetten.nl)	-	-
[Eurlex.europa.eu]	Europese verordening en richtlijnen (http://eur-lex.europa.eu)	-	-
[Leidraad aansprakelijkheid]	Leidraad ambtenaar en strafrecht		November 2010
[Leidraad integrale veiligheid]	Leidraad integrale veiligheid	2.0 (Definitief)	Oktober 2009
[Kader Veiligheidsmanagement]	Kader Veiligheidsmanagement Rijkswaterstaat Eén RWS, elke dag veiliger	4.8 (Vastgesteld)	14 september 2011
[Handboek arbo]	Handboek Arbomanagement RWS	-	1 februari 2011
[Rijksfunctiegebouw]	Functiegebouw Rijk (http://www.functiegebouwrjksoverheid.nl)	-	-
[NEN 3140]	Nederlandse norm NEN 3140: Bedrijfsvoering van Elektrische installaties - Laagspanning	3140:2011	Maart 2011
[NEN 3840]	Nederlandse norm NEN 3840: Bedrijfsvoering van Elektrische installaties - Hoogspanning	3840:2011	Mei 2011
[NEN-EN 50110]	Europese norm NEN-EN 50110: Bedrijfsvoering van Elektrische installaties	50110-1:2005	Juli 2005



Bijlage B Begrippen en afkortingen

Begrip	Bron	Toelichting
Aanrakingsveilig	NEN 3140, par. 3.3.101	Aanrakingsveilig is een actief deel waarvan de beschermingsgraad van ten minste IPXXB of IP2X is.
Actief deel	NEN 3140, par. 3.1.102 NEN 3840, par. 3.1.202	Een actief deel is en 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.
Afscherming	NEN 3140, par. 3.5.2 NEN 3840, par. 3.5.2	Een afscherming is een voorziening die bescherming biedt tegen directe aanraking vanuit elke gebruikelijke richting van benadering.
Bedieningsdeskundige	NEN 3840, par. 3.2.203	Een bedieningsdeskundige is een persoon die is aangewezen als direct verantwoordelijk persoon voor bedieningshandelingen, waarbij deze handelingen worden gecoördineerd vanuit één punt.
Bedrijfsvoering (van elektrische installaties)	NEN 3140, par. 3.1.2 NEN 3840, par. 3.1.2	De bedrijfsvoering van elektrische installaties betreft het 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.
BEI		Bedrijfsvoering van Elektrische Installaties.
COP BEI		Community of Practices BEI
Elektrisch arbeidsmiddel	NEN 3140, par. 3.1.101	Een elektrisch arbeidsmiddel is een op de werkplek gebruikt arbeidsmiddel, hulpmiddel of persoonlijk beschermingsmiddel dat een elektrisch gevaar kan opleveren of verminderen. NB 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.
Elektrisch gevaar	NEN 3140, par. 3.1.5 NEN 3840, par. 3.1.5	Een elektrisch gevaar is de mogelijkheid op letsel of schade aan de gezondheid, veroorzaakt door elektriciteit. NB Tot de gevaren van elektriciteit worden gerekend: • aanraking; • brand; • explosie; • elektromagnetische velden en krachten; • onbedoeld inschakelen en uitschakelen; • vlambogen.
Elektrische bedrijfsruimte	NEN 3840, par. 3.1.201	Een elektrische bedrijfsruimte is een ruimte of plaats waarin elektrisch materieel is geïnstalleerd: • dat geen volledige bescherming heeft; • dat voornamelijk is bestemd voor het bedrijf van een elektrische installatie; of • waar het gevaar van explosie of vlambogen bestaat.



Begrip	Bron	Toelichting
Elektrische installatie	NEN 3140, par. 3.1.1 NEN 3840, par. 3.1.1	Een elektrische installatie is het samenstel van al het elektrisch materieel voor de opwekking, het transport, de omzetting, de distributie en het gebruik van elektrische energie, inclusief bronnen van opgeslagen energie zoals accu's, batterijen en condensatoren
Elektrische installatie	Arbobesluit, art. 3.1, sub a	Een elektrische installatie is een samenstel van elektrisch materieel, leidingen en bijbehoren van leidingen.
Elektrisch materieel	Arbobesluit, art. 3.1, sub b	Elektrisch materieel betreft de delen of gedeelten van een elektrische installatie die dienen voor de opwekking, het transport en de toepassing van elektrische energie.
Elektrotechnische werkzaamheden	NEN 3140, par. 3.4.2 NEN 3840, par. 3.4.2	Onder elektrotechnische werkzaamheden wordt verstaan de activiteiten aan, met of nabij een elektrische installatie, zoals beproeven, meten, repareren, vervangen, aanpassen, uitbreiden, installeren en inspecteren.
Extra lage spanning	NEN 3140, par. 3.6.1	Extra lage spanning is een spanning die normaal niet hoger is dan 50 V bij wisselspanning of 120 V zonder rimpel bij gelijkspanning NB Hieronder vallen SELV-, PELV- en FELV-ketens. Zie NEN 1010.
F-IB		Functioneel Installatiebeheerder
Functioneel Installatiebeheerder		De functioneel installatiebeheerder binnen RWS is een persoon die de functionele taken van de installatieverantwoordelijke, zoals gedefinieerd in de NEN 3140/3840, vervult. Dit betreft de taken en verantwoordelijkheden met betrekking tot het beschikbaar stellen van financiële middelen om de operationele taken van de installatieverantwoordelijkheid te kunnen invullen. Deze persoon hoeft geen elektrotechnische achtergrond te hebben.
Gevarenzone	NEN 3140, par. 3.3.2 NEN 3840, par. 3.3.2	De gevaarzone is een bepaalde ruimte rondom actieve delen. NB Tot het onder spanning werken behoren alle werkzaamheden waarbij een persoon óf actieve delen aanraakt óf zich in de gevaarzone bevindt óf met delen van het lichaam of met gereedschappen, hulpmiddelen en beschermingsmiddelen waarmee wordt gewerkt in de gevaarzone terecht kan komen.
Hoogspanning	NEN 3840, par. 3.6.3	Hoogspanning is een spanning die normaal hoger is dan 1000 V bij wisselspanning of 1500 V bij gelijkspanning.
Hoogspanning	Arbobesluit, art. 3.1, sub e	Hoogspanning is een spanning waarvan de waarde bij wisselspanning hoger is dan 1000 Volt effectief tussen de fasen of 600 Volt effectief tussen een fase en aarde en bij gelijkspanning hoger is dan 1500 Volt tussen de polen of 900 Volt tussen een van de polen en aarde.
HS	NEN 3840, par. 3.6.3	Hoogspanning
Installatieverantwoordelijke	NEN 3140, par. 3.2.2 NEN 3840, par. 3.2.2	De 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. NB Delen van de taken van de installatieverantwoordelijke kunnen worden gedelegeerd.
Isolerend omhulsel	NEN 3140, par. 3.5.3 NEN 3840, par. 3.5.3	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.
IV	NEN 3140, par. 3.2.2 NEN 3840, par. 3.2.2	Installatieverantwoordelijke.
Laagspanning	NEN 3140, par. 3.6.2	Laagspanning is een spanning die normaal niet hoger is dan 1000 V bij wisselspanning of 1500 V bij gelijkspanning.
Laagspanning	Arbobesluit, art. 3.1, sub f	Laagspanning is een spanning met een waarde lager dan hoogspanning.



Begrip	Bron	Toelichting
Leek	NEN 3140, par. 3.2.5 NEN 3840, par. 3.2.5	Een leek is een persoon die geen installatieverantwoordelijke, werkverantwoordelijke, vakbekwaam persoon, ploegleider (NEN 3840), voldoende onderricht persoon of bedieningsdeskundige (NEN 3840) is.
Letsel	NEN 3140, par. 3.1.6 NEN 3840, par. 3.1.6	Een letsel is een dodelijk ongeval of persoonlijk letsel veroorzaakt door een elektrische schok, verbranding, vlambogen, explosie of elektromagnetische velden
Nabijheidszone	NEN 3840, par. 3.3.3	De nabijheidszone is een beperkte ruimte rondom de gevarenszone. NB Tot het werken in de nabijheid van actieve delen behoren alle werkzaamheden waarbij een persoon óf zich in de nabijheidszone bevindt óf met delen van het lichaam of met gereedschappen, hulpmiddelen en beschermingsmiddelen waarmee wordt gewerkt in deze zone terecht kan komen, maar daarbij niet de gevarenszone bereikt.
Niet-elektrotechnische werkzaamheden	NEN 3140, par. 3.4.3 NEN 3840, par. 3.4.3	Onder niet-elektrotechnische werkzaamheden wordt verstaan activiteiten nabij een elektrische installatie, zoals bouwen, graven, schoonmaken en schilderen.
Omhulsel	NEN 3840, par. 3.5.4	Een omhulsel is een voorziening ter bescherming van materieel tegen bepaalde uitwendige invloeden en ter bescherming tegen directe aanraking naar alle richtingen.
Onder spanning werken	NEN 3140, par. 3.4.4 NEN 3840, par. 3.4.4	Met onder spanning werken wordt bedoeld alle werkzaamheden waarbij een persoon actieve delen kan aanraken of met delen van zijn lichaam, met gereedschappen, hulpmiddelen of (persoonlijke) beschermingsmiddelen terecht kan komen in de gevarenszone NB Het aanbrengen van afschermingen valt hier niet onder, mits dit zonder risico kan worden gedaan.
Ononderbroken toezicht	NEN 3140, par. 3.101.1 NEN 3840, par. 3.102.1	Met ononderbroken toezicht wordt bedoeld toezicht met als doel dat werkzaamheden veilig worden uitgevoerd en dat gedurende de werkzaamheden altijd aanwezig is.
Technisch Installatieverantwoordelijke (RWS)		De technisch installatieverantwoordelijke binnen RWS is een persoon die de operationele/technische taken van de installatieverantwoordelijke, zoals gedefinieerd in de NEN 3140/3840, vervult.
PL	NEN 3840, par. 3.2.202	Ploegleider
Ploegleider	NEN 3840, par. 3.2.202	Een ploegleider is een vakbekwaam persoon die ter plaatse met de leiding van werkzaamheden is belast.
Raamopdracht	NEN 3840, par. 3.2.201	Een raamopdracht is een generiek werkvoorschrift, een opdracht voor bepaalde tijd voor een aantal overzichtelijke en regelmatig optredende standaardhandelingen, waarbij er geen sprake mag zijn van afwijkende situaties of omstandigheden.
Regelmatig toezicht	NEN 3140, par. 3.101.2 NEN 3840, par. 3.102.2	Met regelmatig toezicht wordt bedoeld toezicht met als doel dat werkzaamheden veilig worden uitgevoerd en dat gedurende de werkzaamheden regelmatig wordt uitgevoerd
Risico	NEN 3140, par. 3.1.3 NEN 3840, par. 3.1.3	Een risico is de combinatie van de waarschijnlijkheid en de mate van mogelijk letsel of schade aan de gezondheid van een persoon.
Scheiden	NEN 3140, par. 3.4.6 NEN 3840, par. 3.4.6	Met scheiden wordt bedoeld het volledig vrijmaken van een toestel of stroomkring van andere toestellen of stroomkringen.
Scherm	NEN 3140, par. 3.5.1 NEN 3840, par. 3.5.1	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.
S-keten	NEN 3140, par. 3.6.101	Een S-keten is een 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.



Begrip	Bron	Toelichting
Spanningsloos	NEN 3140, par. 3.4.7 NEN 3840, par. 3.4.7	Met spanningsloos wordt bedoeld een spanningswaarde van (vrijwel) 0 V, dat wil zeggen zonder aanwezige spanning en/of lading.
Spanningsloos werken	NEN 3140, par. 3.4.8 NEN 3840, par. 3.4.8	Onder spanningsloos werken wordt verstaan de werkzaamheden aan een elektrische installatie die zonder spanning of lading is en die worden uitgevoerd nadat alle maatregelen ter voorkoming van elektrisch gevaar zijn genomen.
T-IV		Technisch Installatieverantwoordelijke
Vakbekwaam Persoon	NEN 3140, par. 3.2.3 NEN 3840, par. 3.2.3	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.
Voldoende Onderricht Persoon	NEN 3140, par. 3.2.4 NEN 3840, par. 3.2.4	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.
VOP	NEN 3140, par. 3.2.4 NEN 3840, par. 3.2.4	Voldoende Onderricht Persoon.
VP	NEN 3140, par. 3.2.3 NEN 3840, par. 3.2.3	Vakbekwaam Persoon.
WEB		Wet Educatie en Beroepsonderwijs.
Werken in de nabijheid van actieve delen	NEN 3840, par. 3.4.5	Onder het 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 gevarenszone.
Werkplek	NEN 3140, par. 3.3.1 NEN 3840, par. 3.3.1	De werkplek is de plaats waar werkzaamheden worden, moeten worden of zijn uitgevoerd.
Werkverantwoordelijke	NEN 3140, par. 3.2.1 NEN 3840, par. 3.2.1	De werkverantwoordelijke is een persoon die is aangewezen als direct verantwoordelijke voor de veiligheid van de werkzaamheden en het gebruik van elektrische arbeidsmiddelen. NB Delen van de taken van de werkverantwoordelijke kunnen worden gedelegeerd.
Werkzaamheden	NEN 3140, par. 3.4.1 NEN 3840, par. 3.4.1	Onder werkzaamheden wordt verstaan elke vorm van elektrotechnische of niet-elektrotechnische activiteiten waarbij elektrisch gevaar aanwezig kan zijn.
WV	NEN 3140, par. 3.2.1 NEN 3840, par. 3.2.1	Werkverantwoordelijke.



Bijlage C Taken, verantwoordelijkheden en bevoegdheden BEI

In de normen [NEN 3140] en [NEN 3840] zijn – als invulling van de verplichting uit het ARBO-besluit – taken, verantwoordelijkheden en bevoegdheden van verschillende personen beschreven. Het betreft de volgende personen die schriftelijk moeten worden aangewezen door of namens de hoogste verantwoordelijke in de organisatie voor de naleving van de Arbeidsomstandighedenwet:

- de Installatieverantwoordelijke;
- de Werkverantwoordelijke;
- de Vakbekwame persoon;
- de Voldoende onderrichte persoon;
- de Ploegleider (alleen NEN 3840);
- de Bedieningsdeskundige (alleen NEN 3840).

NB Bovengenoemde personen kunnen tot het personeel van de eigen organisatie of een andere organisatie behoren (*Bron: NEN 3140, par 3.2 en NEN 3840, par. 3.2*).

De genoemde personen moeten wel een elektrotechnische opleiding hebben zoals beschreven staat in de normen (*Bron: NEN 3140, par 2 en NEN 3840, par. 3.2*).

De installatieverantwoordelijke en werkverantwoordelijke hebben elk een eigen specifiek werkdomein. De installatieverantwoordelijke is niet boven de werkverantwoordelijke gesteld en evenmin is de werkverantwoordelijke boven de installatieverantwoordelijke gesteld. De verantwoordelijkheden zijn op elkaars werkdomeinen afgestemd. De verantwoordelijkheid voor installaties kan van de een naar de ander worden overgedragen (*Bron: NEN 3140, Bijlage F.1*).

NB De Installatieverantwoordelijkheid en werkverantwoordelijkheid kunnen in één persoon worden verenigd (*Bron: NEN 3140, par 4.3 en NEN 3840, par. 4.3*).

C.1 Installatieverantwoordelijke

Definitie

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 4.2.202 en NEN 3840, par. 4.2.202*). 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).

De punten 1, 3, 5, 6 en 8 zijn zaken die een sterke relatie hebben met besturing 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.

Opleiding

De Installatieverantwoordelijke heeft tenminste 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 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 installatieverantwoordelijke 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*).

C.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*);
- informerende 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 noodstroomstelsel aanwezig is (*Bron: NEN 3140, par. 4.2.107*).

C.3

Vakbekwaam Persoon

Definitie

Een Vakbekwaam Persoon is een persoon die is aangewezen, door of namens de hoogste verantwoordelijke voor de naleving van de ARBOWet, 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*).

C.4

Voldoende Onderricht Persoon

Definitie

Een Voldoende Onderricht Persoon is een persoon die is aangewezen, door of namens de hoogste verantwoordelijke voor de naleving van de ARBOWet, 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 lichtschaakelaars;
- 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*).

C.5 Ploegleider (hoogspanningsinstallatie)

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*).

C.6 Bedieningsdeskundige (hoogspanningsinstallatie)

Een bedieningsdeskundige is een persoon die is aangewezen, door of namens de hoogste verantwoordelijke voor de naleving van de ARBOwet, 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*).

C.7 Leek

Een leek is 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*).



Bijlage D Aanwijzingsformulieren

- D.1 Functioneel Installatiebeheerder (F-IB)
- D.2 Technisch Installatieverantwoordelijke (T-IV)
- D.3 Voldoende onderricht persoon (VOP)



Aanwijzingsbrief F-IB

in het kader van artikel 3, lid 3 van de Arbowet en artikel 3.5, lid 1 van het
Arbobesluit, conform normen NEN3140 en NEN3840

Naam:
Geboortedatum: / /
Functie:
Organisatie:
Afdeling:
wordt met ingang van: / /

door ondergetekende, of namens de hoogste verantwoordelijke voor de naleving van de
ARBOwet, aangewezen als:

FUNCTIONEEL INSTALLATIEBEHEERDER (met beperkte taken als installatieverantwoordelijke)

Deze aanwijzing is geldig tot: / / / wederopzegging¹

De aangewezen bezit voldoende kennis en ervaring van elektriciteit op niveau 4 volgens de Wet
Educatie Beroepsopleidingen of draagt zorg dat hij/zij zich laat bijstaan door adviseurs met kennis
en ervaring op dit niveau.

Gevolgdde opleidingen:

.....
.....
.....

Opgedane ervaring:

.....
.....
.....

Deze aanwijzing geldt voor de volgende locatie(s) / ruimte(n):

.....
.....
.....
.....

Deze aanwijzing geldt voor de volgende installatie(s) / delen van installatie(s):

.....
.....
.....
.....

¹ Doorhalen wat niet van toepassing is



De aangewezen(e) heeft de volgende verantwoordelijkheden / taken:

- Het goedkeuren van bedieningsprocedures;
- Het toekennen van financiële middelen ten behoeve van vervanging;
- Het toekennen van financiële middelen ten behoeve van onderhoud en inspectie;
- Het voeren van regulier overleg met de Technisch Installatieverantwoordelijke, minimaal 2 maal per jaar;
- Het toetsen van de geëiste kennis van nieuw aan te wijzen personen conform de gestelde eisen in de normen;
- Het toekennen van financiële middelen ten behoeve van opleiding/bijtscholing RWS personeel.

De volgende verantwoordelijkheden / taken van de installatieverantwoordelijkheid kunnen worden belegd bij de Technische Installatieverantwoordelijke(n):

- Het schriftelijk aanwijzen van personen in het kader van NEN 3140 en NEN 3840 (werkverantwoordelijke, vakbekwame personen, bedieningsdeskundigen, voldoende onderrichte personen) binnen de RWS-organisatie;
- Het toetsen van de geëiste kennis van nieuw aan te wijzen personen conform de gestelde eisen in de normen;
- Het geven van instructies aan de hierboven genoemde personen;
- Het goedkeuren van de uitbedrijfsname / inbedrijfsname van installatiedelen voor werkzaamheden;
- Het regelen van de toegang tot ruimten met een elektrische gevarenbron;
- Het (laten) inspecteren van de elektrische installatie;
- Het (laten) inspecteren van de elektrische arbeidsmiddelen;
- Het zorgen voor een goede registratie van de uitgevoerde inspecties;
- Het zorgen voor herstel van gevonden gebreken;
- het zorgen voor goede documentatie en tekeningen van een elektrische installatie.
- Het uit gebruik (laten) nemen van (delen van) installaties ten einde veiligheidsrisico's uit te sluiten.

De verantwoordelijkheid voor veilig beheer van de elektrische installatie kan door niemand teniet worden gedaan.

Een en ander is aan alle leidinggevers bekendgemaakt.

Plaats:

Datum: / /

Handtekening aanwijzende:

Handtekening aangewezen(e):

.....

.....



Aanwijzingsbrief T-IV

in het kader van artikel 3, lid 3 van de Arbowet en artikel 3.5, lid 1 van het
Arbobesluit, conform normen NEN3140 en NEN3840

Naam:
Geboortedatum: / /
Functie:
Organisatie:
Afdeling:

wordt met ingang van: / /

door ondergetekende, of namens de hoogste verantwoordelijke voor de naleving van de
ARBOwet, aangewezen als:

TECHNISCH INSTALLATIEVERANTWOORDELIJKE

Deze aanwijzing is geldig tot: / / / wederopzegging²

De aangewezen bezit voldoende kennis en ervaring van elektriciteit op niveau 4 volgens de Wet
Educatie Beroepsopleidingen.

Gevolgdde opleidingen:

.....
.....
.....

Opgedane ervaring:

.....
.....
.....

Deze aanwijzing geldt voor de volgende locatie(s) / ruimte(n):

.....
.....
.....
.....

Deze aanwijzing geldt voor de volgende installatie(s) / delen van installatie(s):

.....
.....
.....
.....

² Doorhalen wat niet van toepassing is



De aangewezen heeft de volgende verantwoordelijkheden / taken:

- Het voeren van regulier overleg met de Functioneel Installatiebeheerder, minimaal 2 maal per jaar;
- Het schriftelijk aanwijzen van personen in het kader van NEN 3140 en NEN 3840 (werkverantwoordelijke, vakbekwame personen, bedieningsdeskundigen, voldoende onderrichte personen) binnen de eigen RWS-organisatie;
- Het toetsen van de geëiste kennis van nieuw aan te wijzen personen conform de gestelde eisen in de normen;
- Het geven van instructies aan de hierboven genoemde personen;
- Het goedkeuren van de uitbedrijfname / inbedrijfname van installatiedelen voor werkzaamheden;
- Het regelen van de toegang tot ruimten met een elektrische gevarenbron;
- Het (laten) inspecteren van de elektrische installatie;
- Het (laten) inspecteren van de elektrische arbeidsmiddelen;
- Het zorgen voor een goede registratie van de uitgevoerde inspecties;
- Het zorgen voor herstel van gevonden gebreken;
- Het zorgen voor goede documentatie en tekeningen van een elektrische installatie.

De verantwoordelijkheid voor veilig beheer van de elektrische installatie kan door niemand teniet worden gedaan.

De aangewezen persoon

- is zich volledig bewust van zijn taak, bevoegdheid en verantwoordelijkheid in overeenstemming met zijn aanwijzing; accepteert de verantwoordelijkheden die zijn aanwijzing met zich meebrengt;
- heeft de beschikking over de voor zijn aanwijzing noodzakelijke persoonlijke beschermingsmiddelen;
- is op de hoogte van de inhoud van de bijlagen behorende bij deze aanwijzing.

Plaats:

Datum: / /

Handtekening aanwijzende:

Handtekening aangewezen:

.....

.....



Aanwijzingsbrief VOP

in het kader van artikel 3, lid 3 van de Arbowet en artikel 3.5, lid 1 van het
Arbobesluit, conform normen NEN3140 en NEN3840

Naam:
Geboortedatum: / /
Functie:
Organisatie:
Afdeling:

wordt met ingang van: / /

door ondergetekende, of namens de hoogste verantwoordelijke voor de naleving van de
ARBOwet, aangewezen als:

VOLDOENDE ONDERRICHT PERSOON

Deze aanwijzing is geldig tot: / / / wederopzegging³

Gevolgde instructie voor de volgende taken:

- Het uitschakelen van openbare verlichting
- Het uitschakelen van VRI's

.....
.....
.....

Opgedane ervaring:

.....
.....
.....

Deze aanwijzing geldt voor de volgende locatie(s) / ruimte(n) / wegen / vaarwegen:

.....
.....
.....
.....

Deze aanwijzing geldt voor de volgende installatie(s) / delen van installatie(s):

.....
.....
.....
.....

³ Doorhalen wat niet van toepassing is



De aangewezen heeft de volgende verantwoordelijkheden / taken :

- Het volgen van reguliere instructie van de Technische Installatieverantwoordelijke of Werkverantwoordelijke;
- Het uitbedrijf nemen van installatiedelen voor werkzaamheden;
- Het regelen van de toegang tot ruimten met een elektrische gevaarbron;
- Het uitvoeren van eenvoudige elektrische werkzaamheden zoals:
 - o vervangen van lampen;
 - o aan- en afkoppelen van elektromotoren *);
 - o resetten van beveiligingen;
 - o monteren van contactstoppen aan leidingen;
 - o vervangen van wandcontactdozen en lichtschakelaars *);
 - o monteren van verlichtingsarmaturen *);
 - o inspecteren van elektrische arbeidsmiddelen *);
 - o aanbrengen en verwijderen van bepaalde smeltpatronen;
 - o het gebruiken van elektrische arbeidsmiddelen in specifieke situaties.

*) Alleen voor terzake opgeleide personen, anders verwijderen.

De aangewezen persoon

- is zich volledig bewust van zijn taak, bevoegdheid en verantwoordelijkheid in overeenstemming met zijn aanwijzing;
- accepteert de verantwoordelijkheden die zijn aanwijzing met zich meebrengt;
- heeft de beschikking over de voor zijn aanwijzing noodzakelijke persoonlijke beschermingsmiddelen;
- is op de hoogte van de inhoud van de bijlagen behorende bij deze aanwijzing.

Plaats:

Datum: / /

Handtekening aanwijzende:

Handtekening aangewezen:

.....

.....



Bijlage E Toetsen van een (uitbestede) BEI

E.1 Toetsen ONB-werkplan BEI

Indien de BEI is uitbesteed, zal de opdrachtnemer een ON-werkplan-BEI (zie hiervoor Bijlage B van Veiligheidshandboek RWS 3140) maken. Deze zal door of namens de F-IB en/of de IPM-rollen voor aanvang en periodiek moeten worden getoetst. De toetsen moeten door een ter zake deskundig persoon worden uitgevoerd. Dit toetsen mag worden uitbesteed.

E.2 Aanvangstoets

De aanvangstoets zal bestaan uit:

- 1 De opdrachtnemer heeft een ON-werkplan-BEI dat voldoet aan de norm 3140/3840, waarin de taken en verantwoordelijkheden voor het uitvoeren van de werkzaamheden, periodieke inspecties en informatie zijn opgenomen. Aandachtspunten hierin zijn ook de personen van RWS die als VOP-er of door de F-IB of door de T-IV/WV worden aangewezen en hoe de instructie aan hen zal verlopen.
- 2 Beoordelen of de beoogd in te zetten personen voldoen aan het opleidingsniveau en/of de ervaring volgens de norm.
- 3 Beoordelen of er valide keuringscertificaten van meetapparatuur zijn, die gebruikt gaat worden

Indien er negatieve bevindingen zijn in deze aanvangstoets, krijgt de opdrachtnemer 2 weken de tijd om zijn ON-werkplan-BEI opnieuw in te dienen en dan volgt er een nieuwe aanvangstoets. De werkzaamheden mogen eerst worden uitgevoerd na positieve bevinding van de aanvangstoets.

E.3 Periodieke toets

De periodieke toets zal bestaan uit:

- 1 Worden de werkzaamheden uitgevoerd door de in de BEI genoemde personen.
- 2 Zijn de aanwijzingsbrieven van de in de BEI opgenomen mensen ondertekend door de juiste perso(o)n(en).
- 3 Is de einddatum in een aanwijzingsbrief niet overschreven of zal overschreven raken voor de volgende periodieke toets.
- 4 Zijn er instructies gegeven aan de medewerkers die de BEI uitvoeren en door wie en aan wie zijn deze gegeven (bijvoorbeeld verslag toolbox meetings).
- 5 Is de periodieke verplichte informatie van T-IV naar F-IB geschied en op welke datum.
- 6 Hoe is het interval voor inspecties bepaald, wordt dit nageleefd en wie voert deze uit?
- 7 Als er tekortkomingen in de verslagen van de inspecties naar voren komen, hoe wordt er gecommuniceerd en gehandeld om deze tekortkomingen op te heffen?
- 8 Beoordelen of er valide keuringscertificaten van in te zetten meetapparatuur aanwezig zijn.

E.4 Herhalingstijd

De toetsen moeten in tijd als volgt worden uitgevoerd:

- 2 weken voor in werking stellen van de BEI: de aanvangstoets.
- 4 weken na het in werking gaan van de uitbestede BEI: 1^e periodieke toets.
- Elke x maand: periodieke toets. Het interval is minimaal 3 maanden en maximaal 5 jaar, een en ander afhankelijk van de looptijd van het contract. Het aantal periodieke toetsen na de 1^e periodieke toets moet ten minste 3 zijn, tenzij het contract minder dan één jaar loopt.



E.5 Bevindingen en rapportage

Het resultaat van de toets moet worden gerapporteerd aan de beheerder van het object. Bij negatieve bevindingen in de toets die onveiligheid op elektrisch gebied van medewerkers met zich mee brengt, moet worden gerapporteerd aan het districtshoofd.

Indien er een negatieve bevinding is bij een periodieke toets, zal er 3 maanden na deze toets een extra periodieke toets moeten worden gehouden.



BIJLAGE F – Regelingenschema Kabels en Leidingen Derden

Vraagspecificatie Proces – Raamovereenkomst

Realisatie Variabel onderhoud stalen bruggen West Nederland Zuid
Project Over-Bruggen

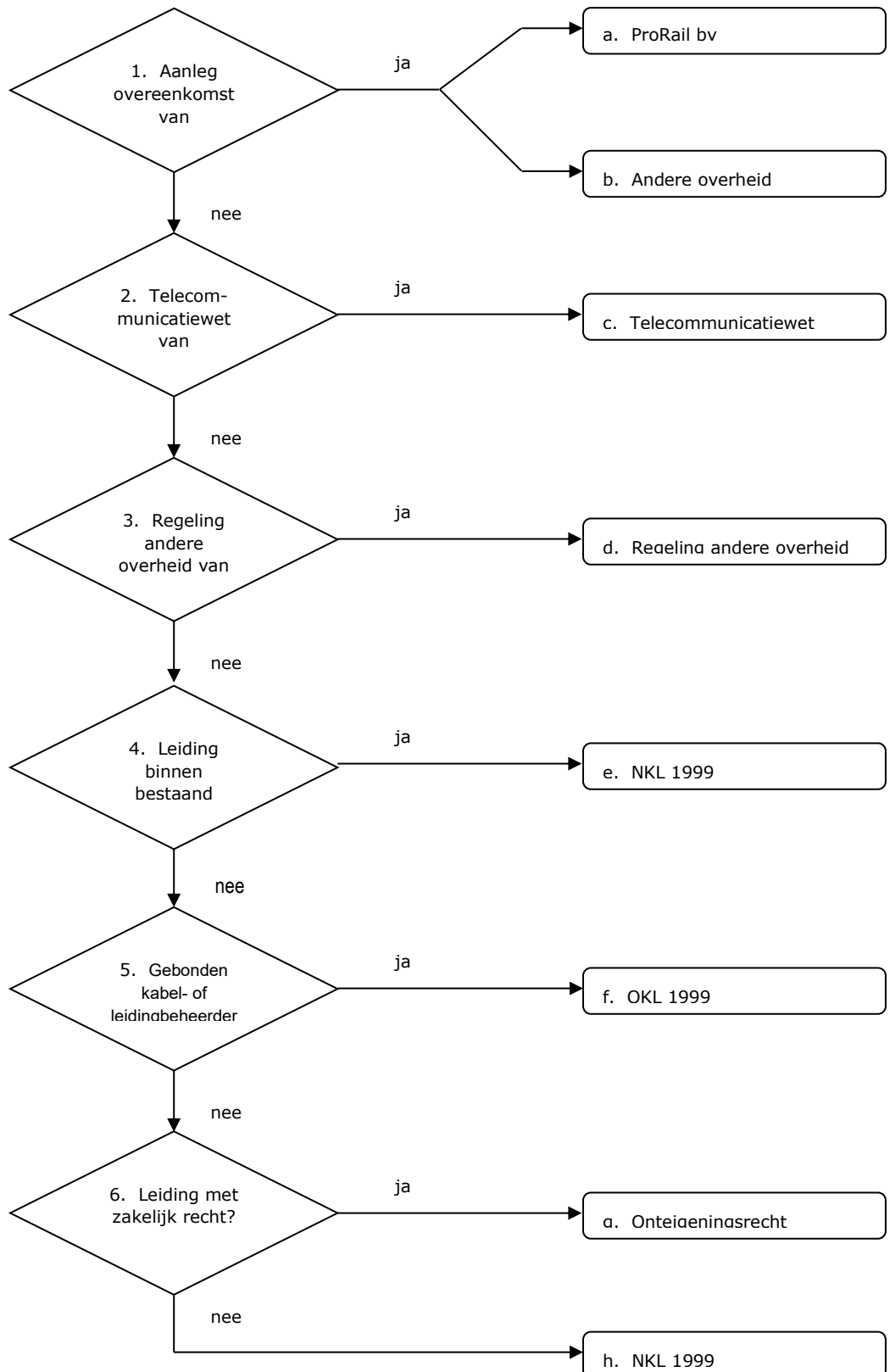


Zaaknummer: **31196743**

Datum: 14 januari 2025

Bijlage F - Regelingenschema Kabels en Leidingen Derden

Deze bijlage 'Regelingenschema Kabels en Leidingen Derden' geldt **generiek** voor alle Nadere Overeenkomsten.



TOELICHTING REGELINGENSHEMA

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 verwijdt 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 langsledingen 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

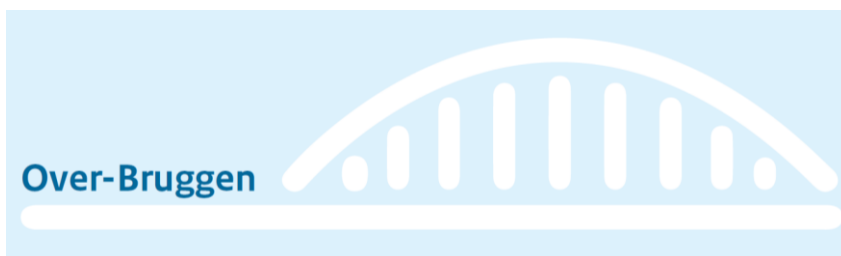
- NKL 1999 = de Nadeelcompensatieregeling verleggen kabels en leidingen in en buiten rijkswaterstaatswerken en spoorwegwerken 1999 (Staatscourant 1999, nr 97) met het daarbij behorende Uitvoeringsprotocol schadevergoeding kabels en leidingen (SKL 01-26, 14 september 2001), inclusief de model-Projectovereenstemmingen (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

Vraagspecificatie Proces – Raamovereenkomst

Realisatie Variabel onderhoud stalen bruggen West Nederland Zuid
Project Over-Bruggen



Zaaknummer: **31196743**

Datum: 14 januari 2025

Bijlage G - Verkeersmanagement voor rijkswegen

Deze bijlage 'Verkeersmanagement voor rijkswegen' geldt **generiek** voor alle Nadere Overeenkomsten.

- **Bijlage A** - Informatievoorziening ter plaatse bij verkeersmaatregelen) geldt **generiek** voor alle Nadere Overeenkomsten.
- **Bijlage B** - Werkbare Uren (WBU), Venstertijden Afsluitingen (VTA) en Werkvensters) is **specifiek** en wordt per Nadere Overeenkomst toegevoegd.
- **Bijlage C** - Slot's is **specifiek** en wordt per Nadere Overeenkomst toegevoegd.



Verkeersmanagement voor rijkswegen

Datum	30 januari 2023
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 Bommel
Datum	30 januari 2023
Status	definitief
Versienummer	1.5

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	Afkorting en begrippen	7
2	Richtlijnen, certificaten en ontheffingen voor verkeersmaatregelen (RL)	9
3	Verkeersmanagement (VM)	10
3.1	Beschrijven verkeersmanagement	10
3.2	Beschrijven fasering verkeersmaatregelen	11
3.3	Slot aanvraag	12
3.4	Beschrijving verkeersmaatregelenplan	13
3.5	Beschrijving incidentmanagement	14
3.6	Uitgangspunten voor verkeersmanagement	15
3.7	Plaatsen informatieborden	16
3.8	Plaatsen kilometerborden	16
3.9	Aanvragen van een verkeersmaatregel	17
3.10	Aanvragen van een verkeersstop	18
3.11	Annuleren van een verkeersmaatregel	18
3.12	Uitvoeren van een verkeersmaatregel	19
	Referentielijst	21

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



RWSRegiogebieden - Districten

- MN District Noord
- MN District Zuid
- NN District Oost
- NN District West
- ON District Noord
- ON District Oost
- ON District Zuid
- WNN District Noord
- WNN District Zuid
- WNZ District Noord
- WNZ District Zuid
- ZD District Noord
- ZD District Zuid
- ZN District Midden
- ZN District West
- ZN District Zuid-Oost

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	Bovenliggende eis
XX100	<i>De opdrachtnemer dient ...</i>	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 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 526 "Beleid en proces, Werk in Uitvoering 96a/96b - 2020", de CROW-publicatie 525 "Specificaties voor Materiaal en Materieel, Werk in Uitvoering 96a/96b - 2020"; 2. bij autosnelwegen: de CROW-publicatie 529 "Werken op autosnelwegen, Werk in Uitvoering 96a - 2020"; 3. bij overige (rijks)wegen: de CROW-publicatie 527 "Werken op niet-autosnelwegen, Werk in Uitvoering 96b - 2020"; 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
RL110	De opdrachtnemer, dan wel zelfstandige hulppersoon die belast is met werkzaamheden met betrekking tot verkeersmaatregelen, 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.	VM010
RL120	Indien de opdrachtnemer, dan wel zelfstandig hulppersoon, niet in het bezit is van voornoemd procescertificaat, dan dienen alle hulppersonen die belast zijn met werkzaamheden met betrekking tot verkeersmaatregelen in het bezit te zijn van 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 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.	VM010

3 Verkeersmanagement (VM)

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

3.1 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
Hinderklasse 0: Geen hinder	-				
Hinderklasse 1: Kleine hinder	Geen file: extra vertraging < 5 minuten	E	E	D	C
Hinderklasse 2: Matige hinder	5 tot 10 minuten extra vertraging door file en/of omrijden	D	D	C	C
Hinderklasse 3: Grote hinder	10 tot 30 minuten extra vertraging door file en/of omrijden	C	C	B	A
Hinderklasse 4: Zeer grote hinder	30 tot 60 minuten extra vertraging door file en/of omrijden	C	B	B	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

3.2 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
- het doel van de fase;
 - op hoofdlijnen van de toe te passen verkeersmaatregelen;
 - 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);
 - een globale risico-inventarisatie met betrekking tot:
 - verkeersveiligheid;
 - de doorstroming van het verkeer;
 - uitloop geplande duur van de activiteiten op, langs en/of in de nabijheid van de rijksweg;
 - hinderbetrouwbaarheid;
 - sociale en maatschappelijke overlast;
 - transport van gevaarlijke stoffen;
 - bijzonder transport en
 - 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;
 - een globale uitwerking van de afstemming ter zake:
 - te treffen verkeersmaatregelen;
 - in te stellen omleidingsroutes e.d. met andere Rijkswaterstaatonderdelen;
 - hulpverleningsdiensten;
 - ziekenhuizen;
 - infrabeheerders;
 - brandstofverkooppunten;
 - relevante nevenopdrachtnemers en
 - overige belanghebbenden;
 - berekeningen waaruit blijkt dat bestaande kunstwerken in de tijdelijke situatie ten minste blijven voldoen aan het bestaande constructieve veiligheidsniveau;
 - een globaal inzicht in de aanvoer-, afvoer- en omleidingsroutes (ook voor massa- en volumetransporten en transport gevaarlijke stoffen).

3.3 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 CC "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 verkeersmaatregelenplan en bij het aanvragen van de verkeersmaatregel(en).	VM330

3.4 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 fasennummer 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 (parallele) 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	13 weken
B	11 weken	10 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

3.5 Beschrijving verkeersincidentmanagement

- VM500 Indien verkeersmaatregelen of de verwachte verkeersdruk 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).

3.6 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

3.7 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

3.8 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

3.9 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, vakantieperiodes 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

3.10 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 wegininspecteur 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

3.11 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 aantoonst 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

3.12 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

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 529 "Werken op autosnelwegen, Werk in Uitvoering 96a - 2020", d.d. 1 juli 2020 ISBN 9789066286818	RL100
CROW-publicatie 525 "Specificaties voor Materiaal en Materieel, Werk in Uitvoering 96a/96b - 2020", d.d. 1 juli 2020 ISBN 9789066286788	RL100
CROW-publicatie 526 "Beleid en proces, Werk in Uitvoering 96a/96b - 2020", d.d. 1 juli 2020 ISBN 9789066286795	RL100
CROW-publicatie 527 "Werken op niet-autosnelwegen, Werk in Uitvoering 96b - 2020", d.d. 1 juli 2020 ISBN 9789066286801	RL100
CROW-publicatie 976 "Omleidingen en tijdelijke bewegwijzering", d.d. 1 november 2005 inclusief errata ISBN 90 6628 467 6	RL100

Bijlage A Informatievoorziening ter plaatse bij verkeersmaatregelen

N.B: Deze bijlage geldt **generiek** voor alle Nadere Overeenkomsten.

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

Onvoorziene omstandigheid	Standaard tekst
	
Afgevallen lading	Afgevallen lading
Afrit afgesloten	Afrit dicht volg
Olie op de weg	Olie op de weg
	
Calamiteit / ongeval <i>Icm J34 – Ongeval</i>	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 B Werkbare Uren (WBU), Venstertijden Afsluitingen (VTA) en werkvensters

N.B.: Deze bijlage is **specifiek** en wordt per Nadere Overeenkomst toegevoegd.

Bijlage C Slot's

N.B.: Deze bijlage is **specifiek** en wordt per Nadere Overeenkomst toegevoegd.



BIJLAGE H – Scheepvaartverkeersmanagement rijksvaarwegen

Vraagspecificatie Proces – Raamovereenkomst

Realisatie Variabel onderhoud stalen bruggen West Nederland Zuid
Project Over-Bruggen



Zaaknummer: **31196743**

Datum: 14 januari 2025

Bijlage H -Scheepvaartverkeersmanagement voor rijksvaarwegen

Deze bijlage 'Scheepvaartverkeersmanagement voor rijksvaarwegen' geldt **generiek** voor alle Nadere Overeenkomsten.

- **Bijlage A** - Hindertabel voor rijkswateren
geldt **generiek** voor alle Nadere Overeenkomsten.
- **Bijlage B** – Verkeersbegeleiding
geldt **generiek** voor alle Nadere Overeenkomsten.
- **Bijlage C** - Template scheepvaartverkeersmanagementplan
geldt **generiek** voor alle Nadere Overeenkomsten.
- **Bijlage D** – Stremmingmomenten
is **specifiek** en wordt per Nadere Overeenkomst toegevoegd.
- **Bijlage E** - Template verkeersmaatregelenplan
geldt **generiek** voor alle Nadere Overeenkomsten.



Rijkswaterstaat
Ministerie van Infrastructuur en Waterstaat

Scheepvaartverkeersmanagement voor rijksvaarwegen

Datum 3 maart 2022
Versie 1.1
Status definitief

Colofon

1.1

Uitgegeven door	Ministerie van Infrastructuur en Waterstaat, Rijkswaterstaat, Verkeer en Watermanagement
Informatie	J.P. Schuiten
Telefoon	0652303812
E-mail	jan-paul.schuiten@rws.nl
Uitgevoerd door	R. van Bommel
Datum	3 maart 2022
Versienummer	1.1
Status	definitief

Inhoud

1	Inleidende informatie	4
1.1	Regio-indeling Rijkswaterstaat	4
1.2	Verkeersposten en bediencentrales Rijkswaterstaat.	7
1.3	Leeswijzer	7
1.4	Wetten en reglementen	7
1.5	Verkeersmaatregelen voor evenementen.	8
1.6	Afkorting en begrippen	8
2	Richtlijnen en ontheffingen voor verkeersmaatregelen (RO)	10
3	Scheepvaartverkeersmanagement (SV)	11
3.1	Beschrijven verkeersmanagement	11
3.2	Aanvraag vaarwegmarkering	12
3.3	Aanvraag stremming	12
3.4	Beschrijven verkeersmaatregelen	13
3.5	Plaatsen informatieborden	14
3.6	Aanvragen van een verkeersmaatregel	15
3.7	Annuleren van een verkeersmaatregel	15
3.8	Uitvoeren van een verkeersmaatregel	16
	Referentielijst	17

1 Inleidende informatie

Dit document geeft een nadere duiding van de eisen die Rijkswaterstaat stelt aan verkeersmanagement bij activiteiten in, op, over of langs de wateren in beheer van Rijkswaterstaat en die verkeershinder kunnen veroorzaken. Een activiteit kan onder andere uit te voeren werkzaamheden betreffen, stremmingen op andere vaarwegen, of evenementen die veel bezoekers aantrekken.

Rijkswaterstaat kan in bovengenoemde situaties vanuit haar Scheepvaartverkeersmanagementtaak, hierna te noemen verkeersmanagement, aanvullende eisen stellen. Het verkeersmanagement zit standaard in de DBFM en UAV-GC contracten van de Aanleg en Onderhoudsorganisaties van Rijkswaterstaat (GPO en PPO).

Bij evenementen die scheepvaarthinder kunnen veroorzaken en waarvoor het treffen van verkeersmaatregelen een vergunningsvoorwaarde of voorwaarde aan de toestemming is, is dit document eveneens van toepassing.

De inhoud van dit document bestaat in belangrijke mate uit een bundeling van reeds bestaande werkwijzen en procedures van de Verkeer- en Watermanagementorganisatie (VWM) van Rijkswaterstaat waar de verkeersmanagementtaak is belegd. Denk hierbij aan Vaarwegmarkeringsmaatregelen, de inzet van vaartuigen en de formulering van hinder categorieën en bijbehorende procedures.

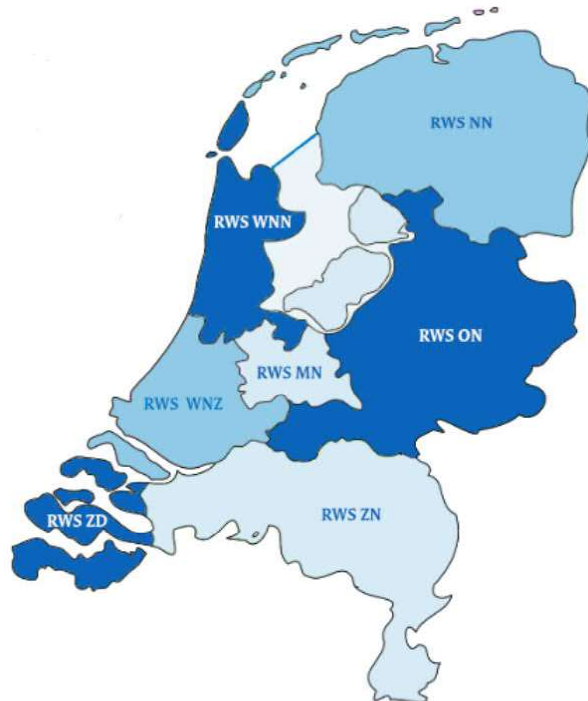
Doel

Het doel van dit document is om in bovengenoemde situaties vroegtijdig duidelijk te maken hoe uitvoering te geven aan het bijkomende verkeersmanagement. Dit zowel om onveilige of anderszins ongewenste situaties op de vaarwegen te voorkomen als om misverstanden hierover in een (te) laat stadium te voorkomen.

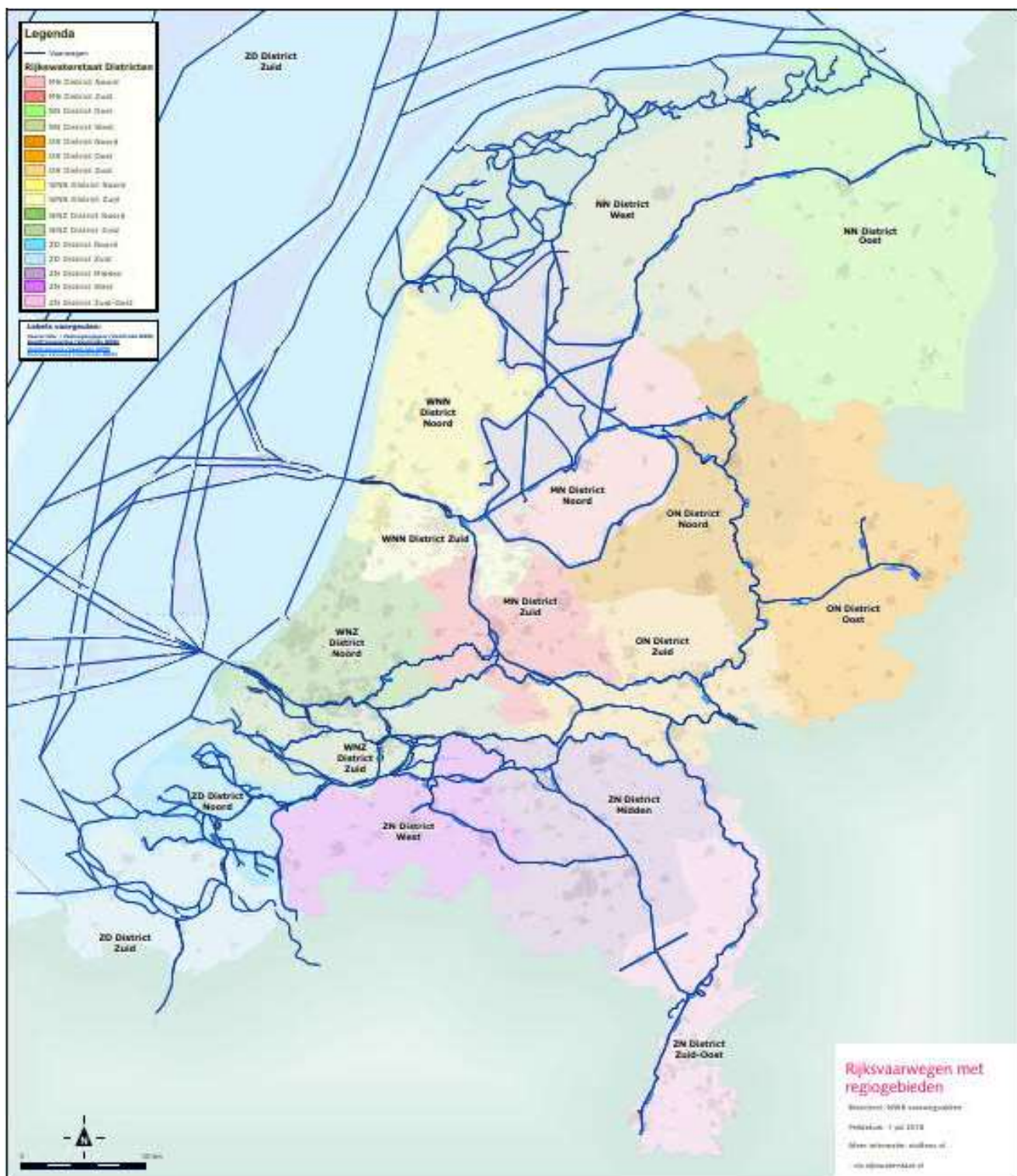
De terminologie in dit document is op zichzelf staand.

1.1 Regio-indeling Rijkswaterstaat

Rijkswaterstaat is een landelijke organisatie en is in 7 regio's onderverdeeld. Daarbinnen is er nog een verdeling in districten. In figuur 1 staat de onderverdeling van de regio's met de regionaam. In figuur 2 staat de onderverdeling van de districten. De verkeersmaatregelen in bovengenoemde situaties gelden landelijk, dus alle regio's en districten van Rijkswaterstaat hanteren hiervoor dezelfde eisen (dit document). Dit document laat daarbij nog voldoende ruimte voor lokaal maatwerk op detailniveau.



Figuur 1 RWS Regio-indeling



Figuur 2 Rijkswaterstaat districtenindeling

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

1.2 Verkeersposten en bediencentrales Rijkswaterstaat.

Opsomming van de verkeersposten en bediencentrales van Rijkswaterstaat

- Verkeerspost Schellingwoude;
- Verkeerspost Hansweert
- Verkeerspost Wemeldinge
- Verkeerspost Tiel
- Verkeerspost Nijmegen
- Verkeerspost Terneuzen
- Verkeerspost Wijk bij Duurstede
- Verkeerspost Dordrecht
- Brandaris zeeverkeerscentrale
- Zeeverkeerspost Schiermonnikoog
- Schelde Coördinatiecentrum Vlissingen
- Centrale Meldpost IJsselmeergebied
- Bediencentrale Rhon
- Bediencentrale Maasbracht
- Bediencentrale Tilburg

De adressen 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	Bovenliggende eis
XX100	<i>De opdrachtnemer dient ...</i>	XX010

Naast de eisen zijn er 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".

De eisen kennen een volgorde in tijd en een afweging. In een schematisch overzicht worden de keuzes en de volgorde in tijd aangegeven.

Een schematisch overzicht van de volgorde van de eisen staat in het stappenplan wat volgt na de referentielijst.

1.4 Wetten en reglementen

In dit document zullen geen wettelijke verplichtingen of verplichtingen die voortvloeien uit reglementen worden opgenomen die voor iedereen van toepassing zijn. Meer informatie is te vinden via:

<https://www.rijkswaterstaat.nl/water/wetten-regels-en-vergunningen/scheepvaart/scheepvaartverkeerswet/index.aspx>

1.5 Verkeersmaatregelen voor evenementen.

Dit document is van toepassing wanneer een evenement kan leiden tot scheepvaarthinder op de rijkswateren en het treffen van verkeersmaatregelen een vergunningsvoorwaarde of voorwaarde aan de toestemming is.

Ook wanneer de aanvrager van het evenement organisatie een derde partij voor de verkeersmaatregelen in de hand neemt, blijft de verantwoordelijkheid hiervoor bij de aanvrager van de vergunning of de toestemming. De partij die namens de organisatie verantwoordelijk is voor de verkeersmaatregelen, staat gelijk aan opdrachtnemer. Overigens zal in dit document onder "opdrachtnemer" ook verstaan worden de aanvrager van een vergunning of toestemming. Afkortingen en begrippen
In dit document worden de onderstaande afkortingen gebruikt.

1.6 Afkortingen en begrippen

Afking	Betekenis
CEMT	Conférence Européenne des Ministres de Transport
DRIP	Dynamisch Route Informatie Paneel
RST	Richtlijnen ScheepvaartTekens
RWS	RijksWaterStaat

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 verkeersmaatregelaanvragen voor de activiteiten
Bouwcommunicatie	Het afstemmen van de verkeersmaatregelen met belanghebbenden (vaarweggebruikers, hulpdiensten omwonenden e.d.) en het informeren van het verkeer tijdens de verkeersmaatregelen
Evenementen	Een georganiseerde gebeurtenis (te waterlating) die veel bezoekers aantrekt
Go / no go criteria	Beslisriteria of de te plaatsen verkeersmaatregelen op het geplande tijdstip kunnen worden geplaatst
Hinderklassen	De mate van verkeershinder ingedeeld in klassen
Informatieborden	Het informeren van het vaarweggebruiker via borden langs de vaarweg
Informatiewagen	Het informeren van de vaarweggebruiker m.b.v. verrijdbare digitale informatiedragers (bijvoorbeeld tekstwagens)
Nautisch beheerder	Instantie die op grond van wettelijke regelingen als bevoegd gezag is aangewezen, met de zorg voor veilige en vlotte afwikkeling van het verkeer op de vaarwegen
Opdrachtgever	De natuurlijke of rechtspersoon die de opdrachtnemer opdraagt activiteiten te verrichten
Opdrachtnemer	De natuurlijke of rechtspersoon, de aannemer, aan wie voor dit document het verkeersmanagement is opgedragen

Begrippen	Betekenis
Rijkswaterstaat	Rijkswaterstaat is een rijksorganisatie die vertegenwoordigd wordt door de vaarwegbeheerder, nautische beheerder en de bediencentrale/verkeerspost e.d. Bij werken van Rijkswaterstaat is ook de opdrachtgever een vertegenwoordiger van Rijkswaterstaat
Stremmingsmomenten	Een projectspecifieke periode waarbinnen Rijkswaterstaat het acceptabel acht dat capaciteit aan een specifiek gedeelte van de rijkswateren wordt onttrokken, waardoor de verkeershinder in een hinderklasse 4 of 5 valt. Dit geldt ook voor de zogenaamde "reserve" stremmingstermijnen
Vaarwegbeheerder	Ook wel watersysteembeheerder draagt zorg om waterkwaliteitsbeheer, waterkwantiteitsbeheer, voorkoming overstromingen, wateroverlast en verkeer mogelijk te maken en te houden, overeenkomstig de aan de betreffende vaarweg toegekende vaarwegfunctie
Verkeershinder	Het hinderen van verkeer wat leidt tot langere reistijd
Verkeersmanagement	Het proces en de organisatie van de opdrachtnemer hoe belanghebbenden worden geïnformeerd, hoe te komen tot verkeersmaatregelen om de activiteiten in, op, over en/of langs de rijkswateren door de verkeersmaatregelen op een veilige manier worden afgeschermd en de veiligheid van het verkeer wordt geborgd

2 Richtlijnen en ontheffingen voor verkeersmaatregelen (RO)

Dit hoofdstuk gaat over welke richtlijnen voor de verkeersmaatregelen van toepassing zijn en ontheffingen die de opdrachtnemer daarvoor nodig heeft.

RO010	De opdrachtnemer dient bij het plannen en toepassen (waaronder ontwerpen, plaatsen, in stand houden, verwijderen) van de verkeersmaatregelen te voldoen aan: 1. Hindertabel voor rijkswateren van bijlage A; 2. Indien scheepvaarttekens nodig zijn, dan geldt de Richtlijnen Scheepvaarttekens (RST 2008);	
RO020	Indien de opdrachtnemer voor activiteiten in, op, over en/of langs de rijkswateren scheepvaartbegeleiding nodig heeft, dan dient de opdrachtnemer de scheepvaartbegeleiding uit te voeren conform Scheepvaartbegeleiding beschreven in bijlage B.	RO010 SV010
RO030	De opdrachtnemer dient er zorg voor te dragen dat (zelfstandige) hulppersonen en materieel, die betrokken zijn bij de verkeersmaatregelen in, op, over en/of langs de rijkswateren, in het bezit zijn van een geldige, door Rijkswaterstaat te verstrekken verklaring. Met deze verklaring wordt ontheffing verleend van artikelen volgens de Scheepvaartverkeerswet, voor zover noodzakelijk voor de verkeersmaatregelen.	SV010

3 Scheepvaartverkeersmanagement (SV)

In dit hoofdstuk worden in chronologische volgorde de eisen en bepalingen beschreven om te komen tot geaccepteerde verkeersmaatregelen voor de scheepvaart. Wanneer de verkeersmaatregelen hinder veroorzaken voor de gebruikers van de rijkswateren, wil Rijkswaterstaat weten hoe de opdrachtnemer managet dat aan de eisen van dit document wordt voldaan.

SV010 De opdrachtnemer dient de werkzaamheden met betrekking tot verkeersmanagement voor vaarwegen te verrichten, zodanig dat veiligheid en minimale verkeershinder zijn gewaarborgd.

3.1 Beschrijven verkeersmanagement

SV100 Indien de verkeersmaatregelen voor activiteiten in, op, over en/of langs de rijkswateren zullen leiden tot verkeershinder die vallen op basis van Bijlage A "Hindertabel voor rijkswateren" binnen hinderklasse 1 of hoger, dan dient de opdrachtnemer een verkeersmanagementplan voor vaarwegen, waarmee de opdrachtnemer bewerkstelligt dat veiligheid en minimale verkeershinder zijn gewaarborgd gedurende de looptijd van de overeenkomst, ter acceptatie voor te leggen aan Rijkswaterstaat. SV010

SV110 De opdrachtnemer dient in het verkeersmanagementplan ten minste te beschrijven: SV100

1. het proces verkeersmanagement voor vaarwegen;
2. een uitwerking van de projectorganisatie met betrekking tot verkeersmanagement voor vaarwegen;
3. de relatie met de planning en de ontheffingen;
4. de wijze waarop de verkeersmaatregelen, die voortvloeien uit de activiteiten in, op, over en/of langs de rijkswateren, worden ingedeeld in hinderklassen op basis van Bijlage A "Hindertabel voor rijkswateren";
5. de verkeersmaatregelen, op hoofdlijnen, vallend binnen de hinderklassen 1 tot en met 4;
6. bij hinderklasse 1B en 1C, op hoofdlijnen, de benodigde werkruimte tot ten hoogste 1/3 deel van de breedte op de vaarweg en de afstemming over de vaarwegmarkering met Rijkswaterstaat Verkeer en Watermanagement afdeling Operationele Taken;
7. de communicatie met Rijkswaterstaat en de nautisch beheerder, gebaseerd op de minimale communicatietermijnen volgens Bijlage A "Hindertabel voor rijkswateren";
8. de communicatie met de doelgroepen voor bouwcommunicatie volgens Bijlage A "Hindertabel voor rijkswateren".

Voor het verkeersmanagementplan kan gebruik gemaakt worden van bijlage C "Template Scheepvaartverkeersmanagementplan".

SV120 Indien de opdrachtnemer een mogelijkheid ziet de aan het contract ten grondslag liggende uitgangspunten ten aanzien van SV110

verkeersmanagement voor vaarwegen te verbeteren, dan dient de opdrachtnemer gemotiveerde voorstellen tot wijziging welke strekken tot een vermindering van de totale verkeershinder (waaronder hinderbeleving) ter acceptatie voor te leggen aan Rijkswaterstaat. Het afwijzen van voorstellen tot wijziging geeft de opdrachtnemer geen recht op bijbetaling of schadevergoeding.

3.2 Aanvraag vaarwegmarkering

SV200	Indien de opdrachtnemer voor zijn activiteiten in, op, over en/of langs de rijkswateren een versmalde vaarweg met (aangepaste) markering/betonning nodig heeft, dan dient de opdrachtnemer, na acceptatie van het verkeersmanagementplan conform SV100, af te stemmen met Rijkswaterstaat Verkeer en Watermanagement afdeling Operationele Taken.	SV100
B-SV210	Het ontwerp van de vaarwegmarkering voor een versmalde vaarweg zal worden uitgevoerd door Rijkswaterstaat Verkeer en Watermanagement afdeling Operationele Taken.	SV200
B-SV220	Het aanbrengen, verleggen, in stand houden en het verwijderen van de vaarwegmarkering zal worden uitgevoerd door de Rijksrederij, in opdracht van Rijkswaterstaat Verkeer en Watermanagement afdeling Operationele Taken.	B-SV210
SV240	De Opdrachtnemer dient uiterlijk 8 weken voor de aanvangsdatum van de benodigde vaarwegmarkering voor een versmalde vaarweg deze datum te melden aan Rijkswaterstaat Verkeer en Watermanagement afdeling Operationele Taken.	SV200,
SV250	Indien de vaarwegmarkering voor een versmalde vaarweg tussentijds moet worden aangepast, dan dient de opdrachtnemer uiterlijk 15 werkdagen voor de datum van uitvoering een verzoek tot aanpassing vaarwegmarkering in te dienen bij Rijkswaterstaat Verkeer en Watermanagement afdeling Operationele Taken.	SV200

3.3 Aanvraag stremming

SV300	Indien de opdrachtnemer één of meerdere stremmingsaanvragen, al dan niet door Rijkswaterstaat gereserveerd in bijlage D "Stremmingsmomenten", nodig heeft voor zijn activiteiten in, op, over en/of langs de rijkswateren, 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 de stremmingsmomenten tijdig kan opnemen in de landelijke planning.	SV100
B-SV310	Indien Rijkswaterstaat stremmingsmomenten heeft gereserveerd, dan zijn deze opgenomen in bijlage D "Stremmingsmomenten".	SV300

SV320	De opdrachtnemer dient, rekening houdende met de communicatietermijnen van Bijlage A "Hindertabel voor rijkswateren", een stremming tijdig aan te vragen bij Rijkswaterstaat.	SV300 SV110
SV330	De opdrachtnemer dient in zijn stremmingsaanvraag ten minste te beschrijven: een afweging tussen verkeershinder en de activiteiten in, op, over en/of langs de rijkswateren waarom een stremming noodzakelijk wordt geacht; 1. de indeling van de stremmingsmomenten in hinderklassen op basis van Bijlage A "Hindertabel voor rijkswateren"; 2. de begintijd / -datum en de eindtijd / -datum per aangevraagd stremmingsmoment; 3. de onderbouwde berekeningen van de extra reistijden en mogelijke vertragingen voor het om te leiden verkeer, waarbij rekening is gehouden met vaarwegcapaciteit en -intensiteit en de CEMT-klassering; 4. een risico-inventarisatie met betrekking tot: a. veiligheid en doorstroming van het verkeer; b. uitloop van de activiteiten in, op, over en/of langs de rijkswateren; c. hinderbetrouwbaarheid; d. sociale en maatschappelijke overlast; e. transport van gevaarlijke stoffen; f. bijzonder transport en g. de bereikbaarheid voor hulpverleningsdiensten rond afgesloten trajecten of objecten; Eén en ander inclusief de bijbehorende maatregelen om de risico's weg te nemen, te beperken of te beheersen; 5. een uitwerking van de afstemming van de te treffen maatregelen met Rijkswaterstaatonderdelen, hulpverleningsdiensten, overige vaarwegbeheerders, bunkerstations en overige stakeholders.	SV300
SV340	De opdrachtnemer mag ten aanzien van de door Rijkswaterstaat in bijlage D "Stremmingsmomenten" gereserveerde stremmingmomenten vroegtijdig een voorstel tot wijziging indienen als daardoor verkeershinder geminimaliseerd kan worden. Het afwijzen van voorstellen tot wijziging geeft de opdrachtnemer geen recht op bijbetaling of schadevergoeding.	SV300

3.4 Beschrijven verkeersmaatregelen

SV400	De opdrachtnemer dient binnen de termijnen genoemd in bijlage A, een verkeersmaatregelenplan conform de template van bijlage E "Template verkeersmaatregelenplan", waarmee de opdrachtnemer bewerkstelligt dat met de te plaatsen verkeersmaatregel voor activiteiten in, op, over en/of langs de rijkswateren de veiligheid en minimale verkeershinder zijn gewaarborgd, ter acceptatie voor te leggen aan Rijkswaterstaat.	SV100
SV410	De opdrachtnemer dient in zijn verkeersmaatregelenplan ten minste in detail te beschrijven:	SV400

1. de toe te passen verkeersmaatregel;
2. de afweging tussen de benodigde ruimte voor de activiteiten in, op, over en/of langs de rijkswateren en de resterende verkeersruimte
3. de beschrijving van de activiteiten binnen de verkeersmaatregel;
4. een duidelijke situatietekening in kleur, inclusief alle relevante te plaatsen, aan te passen en/of te verwijderen bebording en bewegwijzering ten behoeve van het aanduiden van stremmingen of omleidingsroutes in verband met afsluitingen;
5. de tekst op de informatiewagens, omleidingsborden, DRIP's en vooraankondigingsborden;
6. de telefoonnummers van betrokken/relevante contactpersonen;
7. de begintijd / -datum en de eindtijd / -datum per aangevraagde verkeersmaatregel en omleiding;
8. de "go / no go"-criteria voor de start van de verkeersmaatregelen;
9. de schriftelijke goedkeuringen of akkoordverklaringen van de betrokken vaarwegbeheerders voor verkeersbegeleiding, toepassen van afsluitingen en omleidingsroutes;
10. de onderbouwde berekeningen van de extra reistijden en mogelijke vertragingen voor het om te leiden verkeer, waarbij rekening is gehouden met vaarwegcapaciteit en -intensiteit en de CEMT-klassering en een verklaring van geen bezwaar van de hulpverleningsdiensten.

SV430	Indien de verkeersmaatregelen verkeershinder kunnen veroorzaken die volgens Bijlage A "Hindertabel voor rijkswateren" vallen in hinderklasse 2, 3, of 4, dan dient de opdrachtnemer te bewerkstelligen dat het verkeersmaatregelenplan volgens Bijlage A "Hindertabel voor rijkswateren" aangegeven termijnen door Rijkswaterstaat is geaccepteerd.	SV420

B-SV440	Indien een verkeersmaatregelenplan is geaccepteerd, dan behoudt Rijkswaterstaat zich het recht voor, in geval van uitlopende en noodzakelijke activiteiten op het (parallele) netwerk in hinderklasse 2 of hoger, de acceptatie daarvan in te trekken tot twee derde van de in Bijlage A "Hindertabel voor rijkswateren" genoemde minimale communicatietermijn voor de stakeholders en verkeer voorafgaande aan de aanvang van de verkeersmaatregelen. Dit geeft de opdrachtnemer geen recht op bijbetaling of schadevergoeding. Rijkswaterstaat neemt in dat geval het initiatief tot het voorstellen van een nieuwe uitvoeringsperiode.	SV430

3.5 Plaatsen informatieborden

SV500	De opdrachtnemer dient, voor de verkeersmaatregelen die hinder veroorzaken vallend in volgens Bijlage A "Hindertabel voor rijkswateren" hinderklasse 2, 3 en 4, voorafgaande aan het treffen van de betreffende verkeersmaatregelen, vooraankondigingsborden te plaatsen en deze gelijktijdig met de verkeersmaatregelen te verwijderen.	SV010

SV510	De opdrachtnemer dient, voor de verkeersmaatregelen die hinder veroorzaken die volgens Bijlage A "Hindertabel voor rijkswateren"	SV010

vallen in hinderklasse 2, 3 en 4, voorafgaande aan de betreffende verkeersmaatregelen, ter plaatse van elke verkeersmaatregel, mobiele DRIP's en/of informatieborden te plaatsen en deze gelijktijdig met de verkeersmaatregelen te verwijderen.

3.6 Aanvragen van een verkeersmaatregel

SV600	De opdrachtnemer dient de te treffen verkeersmaatregelen volgens bijlage E "Template verkeersmaatregelenplan" aan te vragen bij de desbetreffende vaarwegbeheerder van Rijkswaterstaat.	SV400
SV610	De opdrachtnemer dient de verkeersmaatregelen uiterlijk de in Bijlage A "Hindertabel voor rijkswateren" vermelde termijn te hebben aangevraagd.	SV600
B-SV620	De opdrachtnemer ontvangt uiterlijk de tweede vrijdag vóór de week van uitvoering verkeersmaatregel bericht of toestemming wordt verleend voor de te treffen verkeersmaatregelen van hinderklasse 1B of zwaarder.	SV610
B-SV630	De opdrachtnemer ontvangt uiterlijk de vrijdag vóór de week van uitvoering verkeersmaatregel bericht of toestemming wordt verleend voor de te treffen verkeersmaatregelen van hinderklasse A1.	SV610
B-SV640	Een aanvraag voor een verkeersmaatregel wordt binnen de totale verkeersmaatregelenplanning voor de rijkswateren beoordeeld op te verwachten hinder voor het verkeer.	B-SV620 B-SV630
SV650	Indien er sprake is van niet voorziene onveilige omstandigheden voor het verkeer, dan kan de opdrachtnemer, in aanvulling op en in afwijking van hetgeen is bepaald, direct een aanvraag indienen voor het plaatsen van een urgente verkeersmaatregel. De opdrachtnemer dient voor het plaatsen daarvan toestemming te vragen bij de voor de regio verantwoordelijke verkeerspost / bediening / nautisch centrum van Rijkswaterstaat (zie §1.2). Het niet instemmen met een aangevraagde urgente verkeersmaatregel geeft de opdrachtnemer geen recht op bijbetaling of schadevergoeding.	SV010
SV660	Indien de opdrachtnemer een urgente verkeersmaatregel treft, dan dient hij deze aan Rijkswaterstaat te melden.	SV650

3.7 Annuleren van een verkeersmaatregel

SV700	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 twee werkdagen voorafgaand aan het begintijdstip van de geplande verkeersmaatregelen voor te leggen aan de vaarwegbeheerder.	SV400

B-SV710	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 op de opdrachtnemer, tenzij de opdrachtnemer aantoont dat er sprake is van niet aan hem verwijtbare oorzaken die ten grondslag liggen aan het verzoek tot annulering.	SV700
SV720	Indien de activiteiten waarvoor de verkeersmaatregelen zijn aangevraagd worden afgelast/uitgesteld, dan dient de opdrachtnemer de afgelasting/het uitstel onmiddellijk te melden aan de stakeholders en het verkeer.	SV700

3.8 Uitvoeren van een verkeersmaatregel

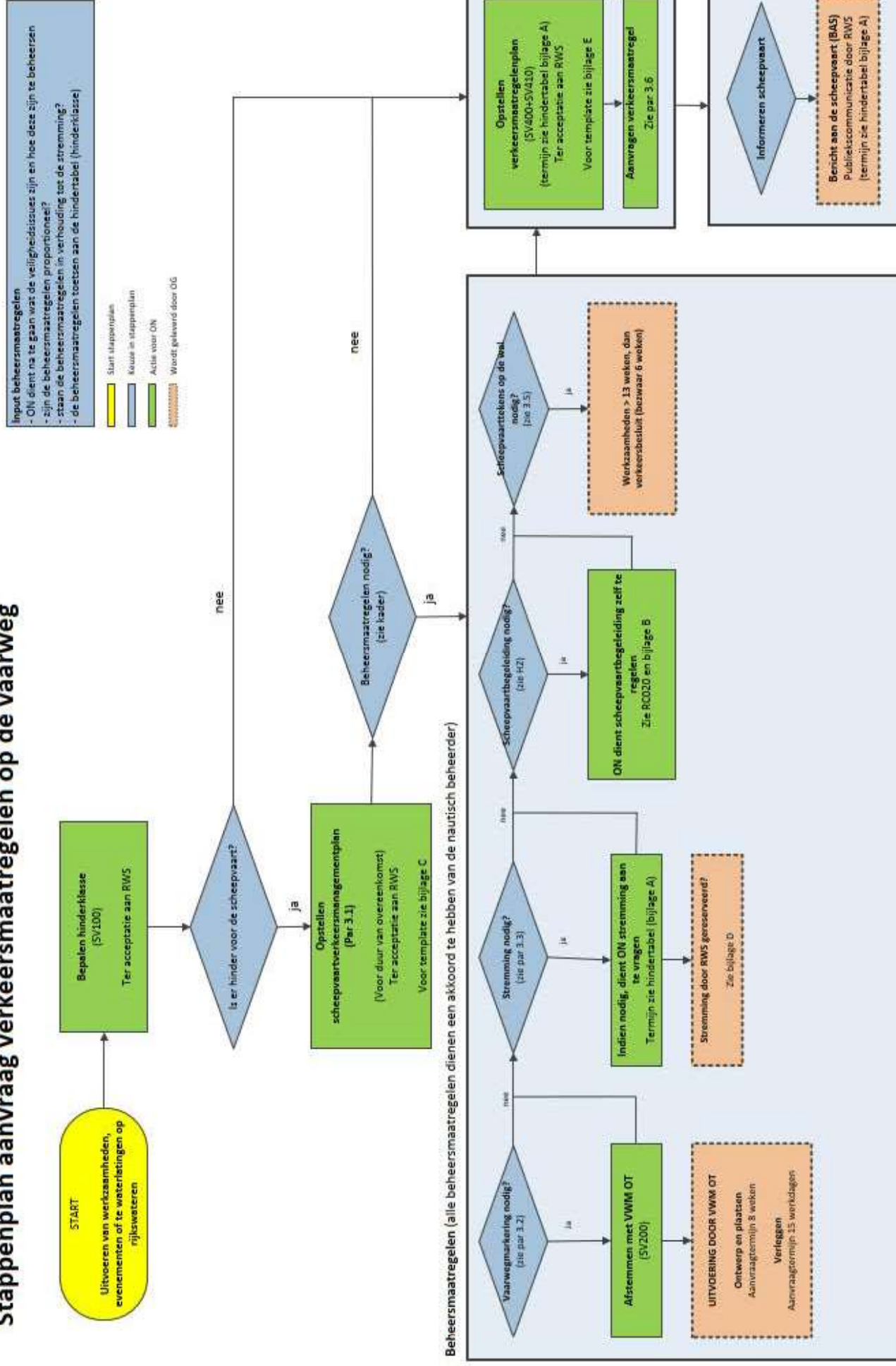
SV800	De opdrachtnemer dient ten aanzien van elke te plaatsen verkeersmaatregel direct voor aanvang de begintijd en direct na beëindiging de eindtijd telefonisch te melden aan de voor de regio verantwoordelijke verkeerspost / bediencentrale / nautisch centrum van Rijkswaterstaat (zie §1.2).	SV400
B-SV810	Als begintijd voor de verkeersmaatregel wordt het tijdstip van aanvang van het plaatsen van de verkeersmaatregel op en/of langs de vaarweg genomen en als eindtijd het tijdstip waarop de volledige verkeersmaatregel is verwijderd en de vaarweg volledig beschikbaar is voor het verkeer.	SV800
SV820	De opdrachtnemer dient tijdens het aan- en/of afmelden van een verkeersmaatregel de nummerherkenning van de telefoon van de opdrachtnemer aan te hebben staan.	SV800
SV830	De opdrachtnemer mag geen capaciteit aan de rijkswateren onttrekken buiten de vastgestelde stremmingmomenten. Het opbouwen of afbreken van een verkeersmaatregel wordt ook gezien als het onttrekken van capaciteit.	SV010 SV300

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
Richtlijnen Vaarwegen - RVW 2020 d.d. 31 juli 2020 ISBN 9789090334233 Gepubliceerd op: http://www.rws.nl/zakelijk/werken-aan-infrastructuur/bouwrichtlijnen-infrastructuur/vaarwegen.aspx	RO010
Richtlijnen Scheepvaarttekens (RST 2008) d.d. december 2008 ISBN 978 90 369 3638 5 Gepubliceerd op: http://www.rws.nl/zakelijk/werken-aan-infrastructuur/bouwrichtlijnen-infrastructuur/vaarwegen.aspx	RO010

Stappenplan aanvraag verkeersmaatregelen op de vaarweg



Bijlage A Hindertabel voor rijkswateren

N.B.: Deze bijlage geldt **generiek** voor alle Nadere Overeenkomsten.

Hinderklasse 0: Geen hinder voor de scheepvaart				
Hinderklasse 1: Hinder voor scheepvaart, bijv. snelheidsbeperking of voorkomen hinderlijke golfslag.				
	Duur van hinder op de vaarweg	Minimale communicatietermijn stakeholder	Minimale Communicatietermijn vaarwegverkeer	Minimale termijn definitieve verkeersmaatregelenplan
A	≤ 1 dag hinder	5 werkdagen voor week van uitvoering	5 werkdagen voor week van uitvoering	5 werkdagen voor week van uitvoering
B	> 1 dag, ≤ 4 weken hinder	6 weken voor uitvoering		
C	> 4 weken hinder	8 weken voor uitvoering		
Hinderklasse 2: Wachtijd voor scheepvaart maximaal 2 uur				
	Duur van hinder op de vaarweg	Minimale communicatietermijn stakeholder	Minimale Communicatietermijn vaarwegverkeer	Minimale termijn definitieve verkeersmaatregelenplan
A	≤ 1 dag hinder	8 weken voor uitvoering	6 weken voor uitvoering	6 weken voor uitvoering
B	> 1 dag, ≤ 1 week hinder	8 weken voor uitvoering		
C	> 1 week hinder	8 weken voor uitvoering		
Hinderklasse 3: Beperking met één gestremde sluiskolk van een sluizencomplex. Doorvaart mogelijk, oplopende wachtijden.				
	Duur van hinder	Minimale communicatietermijn stakeholder	Minimale Communicatietermijn vaarwegverkeer	Minimale termijn definitieve verkeersmaatregelenplan
A	> 2 uur ≤ 4 uur hinder	8 weken voor uitvoering	4 weken voor uitvoering	6 weken voor uitvoering
B	> 4 uur, ≤ 1 dag hinder	10 weken voor uitvoering	6 weken voor uitvoering	
C	> 1 dag, ≤ 2 dagen hinder	12 weken voor uitvoering	8 weken voor uitvoering	
D	> 2 dagen hinder	26 weken voor uitvoering	12 weken voor uitvoering	6 weken voor uitvoering
Hinderklasse 4: Beperking met gestremde vaarweg. Geen doorvaart, totale stremming van de vaarweg. Omvaren indien mogelijk.				
	Duur van hinder	Minimale communicatietermijn stakeholder	Minimale Communicatietermijn vaarwegverkeer	Minimale termijn definitieve verkeersmaatregelenplan
A	> 2 ≤ 4 uur hinder	10 weken voor uitvoering	6 weken voor uitvoering	6 weken voor uitvoering
B	> 4 uur, ≤ 1 dag hinder	12 weken voor uitvoering	10 weken voor uitvoering	
C	> 1 dag, ≤ 2 dagen hinder	26 weken voor uitvoering	12 weken voor uitvoering	6 weken voor uitvoering
D	> 2 dagen hinder	52 weken voor uitvoering	26 weken voor uitvoering	
Afwijken van genoemde termijnen is mogelijk bij calamiteiten, storingen of indien de belangen van Rijkswaterstaat dit vereisen.				

Bijlage B Verkeersbegeleiding

N.B.: Deze bijlage geldt **generiek** voor alle Nadere Overeenkomsten.

Omschrijving document
Afweging inzet vaartuigen marktpartijen voor verkeersbegeleiding De afweging eigen vaartuigen of vaartuigen van de markt komt met name aan de orde bij de afhandeling van incidenten, contractverlening voor werkzaamheden, bij het formuleren van vergunnings-/toestemmingsvoorwaarden bij evenementen, bijzondere transporten, ontheffingen voor bovenmaatse schepen of andere activiteiten in, op, aan of over de vaarweg waarbij risico's kunnen ontstaan en waarbij scheepvaartbegeleiding met een vaartuig nodig is. De gebezigde terminologie in dit document is op zichzelf staand. Eisen aan marktpartijen voor verkeersbegeleiding met vaartuigen Dit document is van toepassing waar Rijkswaterstaat (RWS) voor de uitvoering van haar publiekrechtelijke taak verkeersbegeleiding, gebruik maakt van private marktpartijen. Onder publiekrechtelijke taken verstaan we in deze nota: taken die door of in opdracht van een (semi)overheid worden uitgevoerd. De overheid blijft aansprakelijk en verantwoordelijk voor de publiekrechtelijke taak. Dat valt niet over te dragen. Daarom stelt RWS voorwaarden aan de uitvoering van deze taken door private marktpartijen. Dit kader beschrijft deze voorwaarden. De voorwaarden vallen uiteen in enkele minimale technische eisen aan het vaartuig en enkele voorwaarden aan de bemanning en in het bijzonder ook aan de verkeers-begeleidende taak vanaf dit vaartuig. Deze taak van nautisch verkeersregelaar gaat niet verder dan het verstrekken van verkeersinformatie c.q. verkeersaanwijzingen welke door de vaarweggebruikers gerubriceerd kunnen worden als een door RWS uitgegeven instructie. De Nautisch verkeersregelaar is onder geen enkel beding bevoegd tot het toepassen van ambts- of politiedwang of de schijn daarvan opwekken. De nautisch verkeersregelaar kan verkeersaanwijzingen geven aan het scheepvaartverkeer maar kan niet handhavend optreden bij het niet opvolgen van een aanwijzing. Hiervan kan wel aangifte gedaan worden bij een bevoegd opsporingsambtenaar.

Bijlage C Template scheepvaartverkeersmanagementplan

N.B: Deze bijlage geldt **generiek** voor alle Nadere Overeenkomsten.

[voorblad met projectnaam, opdrachtnemer, datum, versiebeheer]

1. Inleiding

[geef hier een korte introductie van het werk. Optioneel kan een situatietekening worden bijgevoegd]

2. Verkeersmanagement vaarwegen

2.1. Proces verkeersmanagement voor vaarwegen

[beschrijf hier het proces om te komen tot benodigde vaarwegmaatregelen. Dit kan in de vorm van een schema]

2.2. Een uitwerking van de projectorganisatie met betrekking tot verkeersmanagement voor vaarwegen

- Wie plant de werkzaamheden in?;
- Wie ontwerp de verkeersmaatregel?;
- Hoe vindt planning werkzaamheden en afstemming verkeersmaatregel plaats?;
- Wie is verantwoordelijk voor plaatsing en verwijdering van de verkeersmaatregel?;
- Wie doet de scheepvaartbegeleiding op het water?
- Wie controleert de verkeersmaatregel?
- Wie is oproepbaar bij aanvullende maatregelen of herstel maatregelen?
-

2.3. Relatie met Planning en de ontheffingen

- [geef hier op hoofdlijnen de planning aan en de benodigde doorlooptijden]
- [Geef aan van welke kades / ligplaatsen gebruik gemaakt gaat worden voor aan- en afvoer van materiaal en voor overnachten]

2.4. Beschrijving Hinderklassen:

de wijze waarop de verkeersmaatregelen, die voortvloeien uit de activiteiten in, op, over en/of langs de rijkswateren, worden ingedeeld in hinderklassen op basis van Bijlage A "Hindertabel voor rijkswateren"

[Omschrijf hier de verwachte hinder en stremmingen en hoe de hinder geminimaliseerd kan worden.

- Welke hinderklassen zijn in de tijd gezien van toepassing
- Welke objecten worden gestremd en wanneer

2.5. Beschrijving van de verkeersmaatregelen, op hoofdlijnen, vallend binnen de hinderklassen 1 tot en met 4

- benodigde vaarwegmarkering waar en op welk moment
- benodigde scheepvaartbegeleiding waar en op welk moment
- benodigde scheepvaartekens op de wal
- is er extra bediening nodig op een brug/sluis? Houd rekening met aanvraagtermijn van 8 weken
- bij hinderklasse 1B en 1C, op hoofdlijnen, de benodigde werkruimte tot ten hoogste 1/3 deel van de breedte op de vaarweg en de afstemming over de vaarwegmarkering met Rijkswaterstaat Verkeer en Watermanagement afdeling Operationele Taken;

2.6. Communicatie:

2.6.1. de communicatie met Rijkswaterstaat en de nautisch beheerder, gebaseerd op de minimale communicatietermijnen volgens Bijlage A "Hindertabel voor rijkswateren"

[Een voorbeeldtabel of schema met daarin alle contactpersonen kan helpen]

Project:	
Opdrachtnemer	
(onder)aannemer	
Projectleider	Naam + bereikbaarheidsgegevens
Uitvoerder	Naam + bereikbaarheidsgegevens
Contactpersonen RWS	Naam + bereikbaarheidsgegevens
Nautisch beheerder	Naam + bereikbaarheidsgegevens
Gegevens betrokken objecten	
Verkeerspost	Naam + bereikbaarheidsgegevens
Sluis	Naam + bereikbaarheidsgegevens
Brug	Naam + bereikbaarheidsgegevens

2.6.2. de communicatie met de doelgroepen voor bouwcommunicatie volgens Bijlage A "Hindertabel voor rijkswateren"

[beschrijf hier hoe de communicatie volgens termijnen van bijlage A (hindertabel) verloopt bij:

- Schuttevaaier;
- Omgeving;
- hulpdiensten;
- passerende scheepvaart]

Bijlage D Stremmingmomenten

N.B.: Deze bijlage is **specifiek** en wordt per Nadere Overeenkomst toegevoegd.

Bijlage E Template verkeersmaatregelenplan

N.B.: Deze bijlage geldt **generiek** voor alle Nadere Overeenkomsten.

[voorblad met projectnaam, opdrachtnemer, datum, versiebeheer]

1. Algemene gegevens
 - a. Locatie van de werkzaamheden;
 - b. de begintijd / –datum en de eindtijd / –datum per aangevraagde verkeersmaatregel en omleiding
 - c. de telefoonnummers van betrokken/relevante contactpersonen;
 - d. naam van de contactpersoon van Rijkswaterstaat inzake de uitvoering van het werk;
 - e. de “go / no go”-criteria voor de start van de verkeersmaatregelen;
2. De verkeersmaatregel
 - a. Beschrijf de afweging tussen de benodigde ruimte voor de activiteiten in, op, over en/of langs de rijkswateren en de resterende verkeersruimte
 - b. Beschrijf de activiteiten;
 - c. een duidelijke situatietekening in kleur, inclusief alle relevante te plaatsen, aan te passen en/of te verwijderen bebording en bewegwijzering ten behoeve van het aanduiden van stremmingen of omleidingsroutes in verband met afsluitingen;
 - d. de schriftelijke goedkeuringen of akkoordverklaringen van de betrokken vaarwegbeheerders voor verkeersbegeleiding, toepassen van afsluitingen en omleidingsroutes;
 - e. de onderbouwde berekeningen van de extra reistijden en mogelijke vertragingen voor het om te leiden verkeer, waarbij rekening is gehouden met vaarwegcapaciteit en -intensiteit en de CEMT-klassering en een verklaring van geen bezwaar van de hulpverleningsdiensten.
 - 2.1. Vaarwegmarkering (betonning)
 - a. Indien vaarwegmarkering nodig is, dienen de gegevens te worden verstrekt die zijn overeengekomen volgens eis SV200 met Rijkswaterstaat Verkeer en Watermanagement afdeling Operationele Taken
 - b. Uitzondering hierop kan de werkbetonning zijn
 - 2.2. Scheepvaartbegeleiding

Indien nodig, beschrijf waar en wanneer begeleiding nodig is. Denk hierbij aan voorschriften uit duikprotocollen en veiligheidsprotocollen van de betrokken regio.
 - 2.3. Verkeerstekens
 - a. Welke borden moeten er komen?
 - b. Waar moeten de borden worden geplaatst?
 - c. Is er verlichting aangebracht?
 - d. Extra aandachtspunt: Indien de borden langer dan 13 weken blijven staan, dan dient er een verkeersbesluit te worden genomen
 - 2.4. DRIP's en informatieborden
 - a. Welke informatiedrager wordt ingezet;
 - b. Welke informatie komt op de informatiedrager?

Operationeel draaiboek (voor de bediening)

Waar en wat gaat er gebeuren in 1 korte zin

Situatieschets / Foto

Datum en tijd begin en gepland einde:

Wie is de coördinator die ter plaatse en aanspreekbaar is, naam en tel nr:

Gewenste waterstand (binnen- of buitenzijde, naam vaarwater) in de kolk bij aanvang:

Gewenste stand van de deur(en) bij aanvang:

Gewenste stand van de brug(gen) bij aanvang:

Gewenste stand van de slagbomen (op of neer) bij aanvang:

Welke werkvaartuigen zijn er bij betrokken en hoe laat en aan welke zijde willen ze invaren:

En aan welke zijde willen ze eruit na afloop:

Is de kolk gedurende de stremming beschikbaar voor spuien:

Wie wordt geïnformeerd Bediencentrale / Verkeerscentrale voor verdere communicatie:

Is er extra bediening nodig / welke tijden / extra collega's:

Is er plaatselijke bediening nodig:

Opmerkingen:

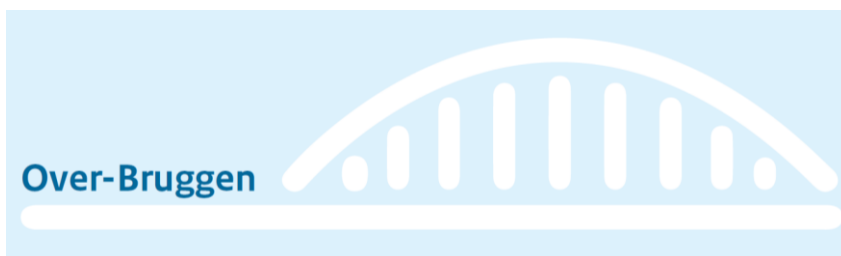
Zijn er nog extra bijzonderheden/aanvullende informatie?:



BIJLAGE I – Rijkswaterstaat Brede Afspraak Archeologie

Vraagspecificatie Proces – Raamovereenkomst

Realisatie Variabel onderhoud stalen bruggen West Nederland Zuid
Project Over-Bruggen



Zaaknummer: **31196743**

Datum: 14 januari 2025

Bijlage I - Rijkswaterstaat Brede Afspraak Archeologie

Deze bijlage 'Rijkswaterstaat Brede Afspraak Archeologie' geldt **generiek** voor alle Nadere Overeenkomsten.



Rijkswaterstaat Brede Afspraak Archeologie

Datum	3 december 2024
Versie	
Status	definitief

Colofon

Uitgegeven door	Rijkswaterstaat ICG
Auteur	Eli Gehasse, Madelene van den Berg, Paul Feitz
Informatie	Contractenbuffet Rijkswaterstaat
E-mail	contractenbuffet@rws.nl
Datum	3 december 2024
Versie	2.3
Status	definitief

Inhoud

1	INLEIDENDE INFORMATIE	4
2	EISEN	6
2.1.	WETTELIJK EN BELEIDSKADER	6
2.2.	TOEVALSVONDSTEN MET VOORONDERZOEK	8
2.3.	BEGELEIDENDE DOCUMENTEN	8

1 Inleidende informatie

In 1992 werd te Valletta, de hoofdstad van Malta, het Europees Verdrag inzake de bescherming van het Archeologisch Erfgoed ondertekend door de Ministers van Cultuur van de bij de Raad van Europa aangesloten landen. Het Verdrag staat ook bekend als de Conventie van Valletta en als het Verdrag van Malta.

Het doel van het Verdrag is het beschermen van het archeologisch erfgoed als bron van het Europese gemeenschappelijke geheugen en als middel voor geschiedkundige en wetenschappelijke studie. Om dit te bereiken dient elke betrokken Staat op zijn eigen wijze een archeologisch rechtsstelsel in te stellen. Het Verdrag verplicht dat archeologische belangen al in een vroeg stadium worden betrokken in de besluitvorming rond de ruimtelijke ordening. Het uitgangspunt hierbij is de archeologische waarden zoveel mogelijk in de bodem te bewaren (behoud in situ). Indien dat niet mogelijk is, dient de archeologische informatie middels opgraven veilig gesteld te worden (behoud ex situ). Verder verplicht het Verdrag dat de financiering van archeologisch onderzoek geregeld wordt. Door Nederland is dit punt vertaald als: de initiatiefnemer tot de bodemverstoring dient het archeologische onderzoek te bekostigen.

Het Verdrag is in 2007 via de Wet op de archeologische monumentenzorg geïmplementeerd in de Nederlandse wetgeving, dat wil zeggen in de gewijzigde Monumentenwet 1988 (in werking getreden op 1 september 2007). De Monumentenwet 1988 is per 1 juli 2016 opgegaan in de Erfgoedwet 2016; de regels over de omgang met cultureel erfgoed uit de Erfgoedwet 2016 zijn per 1 januari 2024 overgegaan naar de Omgevingswet 2024.

Bij alle Rijkswaterstaat projecten waarin de bodem op enigerlei wijze verstoord wordt, dient zodoende (verkenkend) archeologisch onderzoek te worden uitgevoerd. Bij bodemverstoringen moet niet alleen gedacht worden aan de direct met de aanleg of het beheer en onderhoud van infrastructuur samenhangende grondingrepen (ontgraving, baggeren), maar ook aan het aanbrengen van ophogingen en (tijdelijke) gronddepots (vanwege zetting), het verleggen van kabels en leidingen, het rooien van bomen, het slopen van opstallen en werkzaamheden in het kader van natuurcompensatie.

Voor het al dan niet moeten uitvoeren van archeologisch onderzoek is verder van belang of de versturende werkzaamheden plaatsvinden in ongeroerde of in reeds eerder geroerde grond.

Binnen het project dient het aspect archeologie te worden bekeken in samenhang met de:

- andere cultuurhistorische aspecten (historische (steden)bouwkunde en historische landschappen); en
- aspecten natuur, landschap, bodem, lucht, geluid en ruimtelijke kwaliteit. Landschappelijke inpassing, natuurcompensatie, ecoducten, geluidschermen, e.d. kunnen immers van invloed zijn op archeologische / cultuurhistorische waarden.

Het archeologisch vooronderzoek (bureauonderzoek en inventariserend veldonderzoek) dient steeds zo vroeg als mogelijk in de planprocedure te worden uitgevoerd zodat de informatie over het al dan niet aanwezig zijn van archeologische waarden in het plangebied zo vroeg mogelijk bekend wordt.

In de "[Overeenkomst betreffende de samenwerking tussen de Rijksdienst voor het Cultureel Erfgoed en Rijkswaterstaat inzake cultureel erfgoed](#)", hierna "samenwerkingsovereenkomst" (d.d. 11 november 2019), is vastgelegd dat de samenwerking in het bijzonder betrekking heeft op de planstudiefase en de uitvoeringsfase van een werk en op het beheer en onderhoud van archeologische monumenten na afloop van een werk.

De Rijksdienst voor het Cultureel Erfgoed treedt hierbij op als adviseur van Rijkswaterstaat over de omgang met Cultureel Erfgoed (waaronder archeologie) binnen een werk van Rijkswaterstaat.

In de verkennings- en planstudiefase treedt Rijkswaterstaat op als opdrachtgever van het archeologisch vooronderzoek (bureauonderzoek, gevolgd door een inventariserend veldonderzoek). Ten aanzien van het vooronderzoek is Rijkswaterstaat verantwoordelijk voor het (laten) opstellen van een Archeologisch Plan van Aanpak (bij bureau- en booronderzoek) of een Archeologisch Programma van Eisen voor uitvoerend onderzoek (bij proefsleuvenonderzoek) (samenwerkingsovereenkomst art. 4).

In de tot de [samenwerkingsovereenkomst](#) behorende bijlage 1 is de samenwerking tussen de Rijksdienst voor het Cultureel Erfgoed en Rijkswaterstaat uitgewerkt voor de fase van de intake (met een start zo vroeg mogelijk in de planvormingsfase), met de bijbehorende werkwijze. Na afronding van het archeologisch bureauonderzoek besluit de Rijksdienst voor het Cultureel Erfgoed – in samenspraak met Rijkswaterstaat - of vervolgonderzoek in de vorm van inventariserend veldonderzoek noodzakelijk is, en zo ja, of zij hierbij betrokken wil blijven dan wel Rijkswaterstaat verwijst naar het bevoegde gezag voor archeologie (zijnde de gemeente of provincie).

Na afronding van het archeologisch vooronderzoek (bureauonderzoek en inventariserend veldonderzoek) en op basis van het Archeologisch Selectiebesluit van het bevoegd gezag besluit Rijkswaterstaat:

- over de noodzaak van archeologisch vervolgonderzoek (opgraving, begeleiding en/of fysieke bescherming); en
- of en in welke mate (geheel of gedeeltelijk) het archeologisch vervolgonderzoek deel uitmaakt van een geïntegreerd contract met de opdrachtnemer.

Na afronding van het archeologisch vooronderzoek besluit Rijkswaterstaat of en in welke mate (geheel of gedeeltelijk) het archeologisch vervolgonderzoek deel uitmaakt van een geïntegreerd contract met de opdrachtnemer.

In het onderhavige project zijn behoudenswaardige archeologische resten aanwezig, zoals aangetoond in het reeds uitgevoerde archeologisch vooronderzoek (bureauonderzoek en inventariserend veldonderzoek). Het is de verplichting van de opdrachtnemer om overeenkomstig deze "Rijkswaterstaat Brede Afspraak Archeologie" te zorgen voor het op juiste wijze verlopen van het verder benodigde archeologisch onderzoek (opgraving, begeleiding en/of fysieke bescherming).

2 Eisen

2.1. Wettelijk en beleidskader

Ten aanzien van archeologische werkzaamheden dient de opdrachtnemer zich te houden aan de vigerende wettelijke en beleidsbepalingen inzake archeologische waarden, met name aan:

- het genoemde Verdrag van Valletta (Malta 1992);
- de Erfgoedwet 2016;
- de Omgevingswet 2024;
- de "[Overeenkomst betreffende de samenwerking tussen de Rijksdienst voor het Cultureel Erfgoed en Rijkswaterstaat inzake cultureel erfgoed](#)" (11 november 2019); en
- de binnen de archeologische beroepsgroep geldende voorschriften en inzichten (weergegeven in de Kwaliteitsnorm Nederlandse Archeologie (KNA)). Zie voor meer informatie over de certificeringsplicht en de KNA: www.sikb.nl.

Projectspecifieke eisen aangaande de genoemde werkzaamheden (opgraving, begeleiding en/of fysieke bescherming) vloeien voort uit het voor het project opgestelde Wetenschappelijke Archeologisch Kader (indien van toepassing), het Archeologische Projectconvenant (indien van toepassing) en zijn opgenomen in het "Archeologisch Programma van Eisen voor uitvoerend onderzoek" (conform format van de SIKB).

Indien contractueel bepaald, dan dient de opdrachtnemer de volgende werkzaamheden te verrichten:

1. Het opstellen van een archeologieplan.
2. Het verrichten van archeologische graafwerkzaamheden.
3. Het verrichten van archeologische begeleiding.
4. Het treffen van fysieke beschermingsmaatregelen.

Ad 1. Archeologieplan

De opdrachtnemer dient - uitgaande van het "Programma van Eisen voor uitvoerend archeologisch onderzoek" - een archeologieplan op te stellen waarin aantoonbaar aangegeven wordt hoe, binnen de wettelijke - en beleidskaders, rekening gehouden gaat worden met en uitvoering gegeven gaat worden aan alle archeologische werkzaamheden. Dit archeologieplan behoeft de goedkeuring van de opdrachtgever en wordt door opdrachtgever ter advisering voorgelegd aan de Rijksdienst voor het Cultureel Erfgoed indien zij eerder heeft aangegeven hierbij betrokken te willen zijn (zie Samenwerkingsovereenkomst bijlage 1) en aan het betreffende bevoegd gezag voor archeologie.

Ad 2. Archeologische graafwerkzaamheden

Archeologische graafwerkzaamheden (boringen en opgravingen) mogen alleen uitgevoerd worden door bureaus die daarvoor gecertificeerd zijn, dan wel werken onder de bevoegdheid van een certificaathouder (Erfgoedwet art. 5.1). De certificaten worden door certificerende instellingen verleend en geauditeerd op basis van de Beoordelingsrichtlijn Archeologie (BRL SIKB 4000 Archeologie) voor KNA-protocol 4003 (inventariserend veldonderzoek) en/of KNA-protocol 4004 (opgraven).

Daarnaast dienen de bij de archeologische graafwerkzaamheden betrokken KNA-actoren te zijn ingeschreven in het actorenregister. Het in te zetten bureau heeft goedkeuring van de opdrachtgever.

Een desgewenst door de opdrachtgever aangestelde Archeologische Directievoerder houdt toezicht op de uitvoering van de archeologische graafwerkzaamheden conform het Archeologisch Programma van Eisen voor uitvoerend onderzoek.

Archeologische monumenten

In het geval dat een werk een relatie heeft met een wettelijk beschermd archeologisch rijksmonument dan dient de opdrachtnemer voor zijn werkzaamheden een omgevingsvergunning aan te vragen bij de betreffende gemeente (soms de provincie), waarbij de Rijksdienst voor het Cultureel erfgoed advies- en instemmingsrecht heeft (artikel 4.32 lid 1 onder a en lid 2 Omgevingsbesluit). In geval van een beschermd archeologisch provinciaal of gemeentelijk monument dient de opdrachtnemer een omgevingsvergunning aan te vragen bij de provincie, respectievelijk de gemeente.

Ad. 3 Archeologische begeleiding

Archeologische begeleiding van civiele graafwerkzaamheden mag alleen worden uitgevoerd door bureaus die daarvoor gecertificeerd zijn, dan wel werken onder de bevoegdheid van een certificaathouder (Erfgoedwet art. 5.1). De certificaten worden door certificerende instellingen verleend en geauditeerd op basis van de Beoordelingsrichtlijn Archeologie (BRL SIKB 4000 Archeologie) voor KNA-protocol 4003 (inventariserend veldonderzoek) en/of KNA-protocol 4004 (opgraven). Daarnaast dienen de bij de archeologische begeleiding betrokken KNA-actoren te zijn ingeschreven in het actorenregister.

Het in te zetten bureau heeft goedkeuring van de opdrachtgever. De opdrachtnemer en het bureau dat de archeologische begeleiding uitvoert dienen de uitvoering en planning van de werkzaamheden en de archeologische begeleiding van de werkzaamheden in overleg op elkaar af te stemmen.

Een desgewenst door de opdrachtgever aangestelde Archeologische Directievoerder houdt toezicht op de uitvoering van de archeologische begeleiding conform het Archeologisch Programma van Eisen voor uitvoerende werkzaamheden.

Ad. 4. Fysieke bescherming

Voor het uitvoeren van fysieke beschermingsmaatregelen inzake archeologische waarden is door de Rijksdienst voor het Cultureel Erfgoed een Archeologische Visie voor Beheer en Inrichting opgesteld. Daarnaast is door de opdrachtgever het document Archeologische Richtlijnen voor Beheer en Inrichting opgesteld dat door de Rijksdienst voor het Cultureel Erfgoed is getoetst.

De opdrachtgever, de Rijksdienst voor het Cultureel Erfgoed, de opdrachtnemer en het uitvoerend (archeologisch) bureau bepalen gezamenlijk of en hoe de fysieke beschermingsmaatregelen (omschreven in de Archeologische Richtlijnen voor Beheer en Inrichting) geïmplementeerd (kunnen) worden. Een desgewenst door de opdrachtgever aangestelde Archeologische Directievoerder houdt toezicht op de uitvoering van de fysieke beschermingsmaatregelen conform de Archeologische Richtlijnen voor Beheer en Inrichting.

Eventuele fysieke beschermingsmaatregelen dienen uitgevoerd te worden door een bureau dat werkt volgens de binnen de archeologische beroepsgroep geldende inzichten en voorschriften (KNA). Voor het uitvoeren van fysieke beschermingswerkzaamheden in archeologische monumenten is een

opgravingscertificaat verplicht. Het in te zetten bureau heeft de goedkeuring van de opdrachtgever.

2.2. Toevalsvondsten met vooronderzoek

Ondanks zorgvuldige inventarisatie van het plangebied door bureauonderzoek en inventariserend veldonderzoek, kan het voorkomen dat er tijdens de uitvoeringswerkzaamheden toch nog onverwachte archeologische vondsten worden aangetroffen. Er zijn drie typen toevalsvondsten met vooronderzoek:

1. De toevalsvondst wordt aangetroffen in een terrein waar tijdens het vooronderzoek (bureauonderzoek, eventueel gevolg door inventariserend veldonderzoek) geen archeologische waarden zijn vastgesteld, op grond daarvan is aan het terrein geen archeologische waarde toegekend.
2. De toevalsvondst wordt aangetroffen in een terrein waar wel archeologische waarden zijn vastgesteld of verwacht, maar het terrein is niet geselecteerd voor verder archeologisch onderzoek (opgraving of begeleiding).
3. De toevalsvondst wordt aangetroffen bij archeologische begeleiding, waar in het kader van die begeleiding geen rekening mee is gehouden.

In alle drie de gevallen dient de opdrachtnemer de toevalsvondst direct te melden bij de opdrachtgever, de Rijksdienst voor het Cultureel Erfgoed en het bevoegd gezag. De opdrachtnemer dient de betreffende uitvoeringswerkzaamheden onmiddellijk te verleggen en maatregelen te nemen ter voorkoming van verdere versterking van de vondstlocatie. Binnen 48 uur na de melding van de toevalsvondst brengt de Rijksdienst voor het Cultureel Erfgoed een advies uit aan de opdrachtgever over de te nemen vervolgstappen.

2.3. Begeleidende documenten

Samenhangend met deze Rijkswaterstaat Brede Afspraak Archeologie worden - indien aanwezig en relevant - de documenten hieronder, die specifiek voor het project zijn opgesteld, als bijlagen bij de overeenkomst tot uitvoering van de werkzaamheden gevoegd.

- Rapport Archeologisch Bureauonderzoek
- Wetenschappelijk Archeologisch Kader
- Archeologisch Projectconvenant
- Programma van Eisen Inventariserend Veldonderzoek
- Rapport Inventariserend Veldonderzoek
- Archeologisch Selectieadvies
- Archeologisch Selectiebesluit van het bevoegd gezag
- Programma van Eisen Opgraven
- Programma van Eisen Archeologische begeleiding
- Archeologische Visie voor Beheer en Inrichting
- Archeologische Richtlijnen voor Beheer- en Inrichting



BIJLAGE J – Rijkswaterstaat Brede Afspraak Maatschappelijk Verantwoord Inkopen

Vraagspecificatie Proces – Raamovereenkomst

Realisatie Variabel onderhoud stalen bruggen West Nederland Zuid
Project Over-Bruggen



Zaaknummer: **31196743**

Datum: 14 januari 2025

Bijlage J - Rijkswaterstaat Brede Afspraak Maatschappelijk Verantwoord Inkopen

Deze bijlage 'Rijkswaterstaat Brede Afspraak Maatschappelijk Verantwoord Inkopen' geldt **generiek** voor alle Nadere Overeenkomsten



Rijkswaterstaat Brede Afspraak Maatschappelijk Verantwoord Inkopen (RBA MVI)

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

Datum 1 maart 2022
Status Definitief

Colofon

Uitgegeven door	Rijkswaterstaat, Grote Projecten en Onderhoud
Informatie	Gerrit Knoeff
Telefoon	0610948577
E-mail	Gerrit.Knoeff@rws.nl
Vastgesteld door	"Programma Duurzaam Aanleg & Onderhoud" en Redactieraad GPO Inkoopcentrum GWW (ICG)
Datum	Maart 2022
Status	Definitief
Versienummer	2.1

Inhoud

1	Inleiding	5
2	Verplichtingen van de opdrachtnemer	6
3	MVI-eisen GWW	7
3.1	Civiele constructies	8
3.1.1	Duurzaam ontwerp houten constructie	8
3.1.2	Duurzaam ontwerp staalconstructie	8
3.1.3	Duurzaam hout	8
3.1.4	Milieuvriendelijke smeermiddelen voor bewegingswerken	9
3.2	Conserveringswerken	9
3.2.1	Oplosmiddelarme conserveringssysteem	9
3.2.2	Producten met lood- of chromaathoudende pigmenten	10
3.2.3	Leveren beheer- en onderhoudsplan	11
3.2.4	Milieumanagementsysteem	11
3.3	Openbare verlichting (OVL)	11
3.3.1	Ledverlichting	11
3.3.2	Levensduur ledsysteem	12
3.3.3	Dimbare OVL-installatie	12
3.3.4	Lichthinder wordt beperkt	12
3.4	Straatmeubilair	12
3.4.1	Straatmeubilair (m.u.v. Speeltoestellen): meer dan 5% kunststof	12
3.4.2	Inkoop en reparatie van Speeltoestellen – kunststof onderdelen voorzien van markering	13
3.4.3	Straatmeubilair (incl. Speeltoestellen): verven	13
3.4.4	Duurzaam hout	14
3.4.5	Speeltoestellen – kunststof	14
3.5	Gemalen	14
3.5.1	Energierendement van systeem	14
3.5.2	Energierendement van systeemdelen	15
3.5.3	Smeeroliën en hydraulische vloeistoffen	15
3.6	Waterzuiveringsinstallaties en slibbehandeling	16
3.6.1	Ecotoxiciteit chemicaliën	16
3.7	Mobiele werktuigen uitbesteding	16
3.7.1	Emissie-eisen mobiele dieselwerktuigen met variabel toerental	16
3.7.2	Milieumanagementsysteem	17
3.7.3	Training in het nieuwe draaien	17
3.7.4	Onderhoud gebruikte mobiele werktuigen	18
3.8	Verkeersregelininstallaties	18
3.8.1	Diminrichting in regeltoestel	18
3.8.2	Energiezuinige lichtbronnen	18
3.8.3	Energiezuinige lampen voor scheepvaartseinen	19
3.8.4	Levenscycluskosten	19

3.8.5	Minimale levensduur en garantie	19
3.9	Groenvoorzieningen	20
3.9.1	Vakbekwaam ontwerper en beheerder groenvoorziening	20
3.9.2	Verwerven van bloembollen	20
3.9.3	Boomkwekerijproducten van een genetische kwaliteit (buitenstedelijk)	21
3.9.4	Meststoffen en bodemverbeteraars bij aanleg en onderhoud van openbaar groen (incl. sport- en speelvelden)	21
3.9.5	Ongewenste kruiden, ziekten en plagen (excl. sport- en speelvelden)	22
3.9.6	Duurzaam ontwerp groenvoorziening	22
3.9.7	Plan en rapportage bemesting, bodemverbetering en bestrijding	22
3.9.8	Eisen aan compost	23
3.9.9	Geen invasieve exoten	23
3.10	Reiniging openbare ruimte	23
3.10.1	Verwijderen van graffiti met hogedrukwaterreiniger	23
3.10.2	Ervaring met integraal plaagdiermanagement (IPM)	24
3.10.3	Milieumanagementsysteem	24
3.10.4	Milieu-impact onkruidbestrijding op verhardingen	24
3.10.5	Plan van aanpak Plaagdierbeheersing	25
3.10.6	Vermindering van PM10 straatstof	25
3.10.7	Milieukeur voor buitenschoonmaakmiddelen	26

1 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 minimeisen 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-criteriatool² 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 werk³ 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 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 wegzout Rijkswaterstaat".

¹ Rijkswaterstaat heeft een verdergaande ambitie dan het opnemen van de minimeisen 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.

2 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.

3 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. Straatmeubilair
5. Gemalen
6. Waterzuiveringsinstallaties en slibbehandeling
7. Mobiele werktuigen uitbesteding
8. Verkeersregelininstallaties
9. Groenvoorzieningen
10. Reiniging openbare ruimte

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.

3.1 Civiele constructies

3.1.1 Duurzaam ontwerp houten constructie

- **Ambitieniveau:** 1
- **Criteriumtype:** EIS;
- **Criteriumcode:** 029.01

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.

3.1.2 Duurzaam ontwerp staalconstructie

- **Ambitieniveau:** 1
- **Criteriumtype:** EIS
- **Criteriumcode:** 029.02

Deze eis uit de RBA is opgenomen in de Vraagspecificatie.

3.1.3 Duurzaam hout

- **Ambitieniveau:** 1
- **Criteriumtype:** EIS
- **Criteriumcode:** 029.07

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 certificeringssysteem 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.

3.1.4 Milieuvriendelijke smeermiddelen voor bewegingswerken

- **Ambitieniveau:** 1
- **Criteriumtype:** EIS
- **Criteriumcode:** 029.12

Eisen

1. Bij onderhoud dienen motorsmeeroliën met een lage viscositeit te worden gebruikt of geregenereerde smeeriën met ten minste 25% geregenereerde basisoliën. Smeeriën met een lage viscositeit zijn die in de categorie SAE 0W30, SAE-5W30 of gelijkwaardig.
2. Hydraulische vloeistoffen en vetten mogen niet voorzien zijn van een gevarenaanduiding voor milieu of gezondheid of een waarschuwingszin (R-zinnen) ten tijde van de toepassing (laagste classificatielimiet in Verordening (EG) nr. 1272/2008.
3. Er wordt geen afwijking toegestaan van het verbod in artikel 6, lid 6, van Verordening (EG) nr. 66/2010 voor stoffen die beschouwd worden als zeer zorgwekkend en die zijn opgenomen in de lijst zoals bedoeld in artikel 59 van Verordening (EG) nr. 1907/2006, voor zover die aanwezig zijn in concentraties van meer dan 0,010 gewichtsprocent in mengsels.
4. Het koolstofgehalte uit hernieuwbare grondstoffen moet groter dan of gelijk aan 45% zijn.
5. De cumulatieve massaconcentratie van aanwezige stoffen die zowel niet biologisch afbreekbaar als bio-accumulatief zijn, mag niet meer dan 0,1 gewichtsprocent bedragen.

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 5. Op de website van RVO is een lijst beschikbaar van oliën en vetten die voldoen aan de eisen van het Europese Ecolabel;
- Rapport, of andere documentatie van een onafhankelijk deskundige, waaruit blijkt dat aan dit criterium is voldaan;
- Of gelijkwaardig.

3.2 Conserveringswerken

3.2.1 Oplosmiddelarme conserveringssystemen

- **Ambitieniveau:** 1
- **Criteriumtype:** EIS
- **Criteriumcode:** 030.01

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 $\leq 25^\circ$ -60°)	WG	30
	SG	30
*b- Glanzende coatings voor wanden en plafonds (glans $> 25^\circ$ -60°)	WG	100
	SG	100
*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.

3.2.2 Producten met lood- of chromaathoudende pigmenten

- **Ambitieniveau:** 1
- **Criteriumtype:** EIS
- **Criteriumcode:** 030.02

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.

3.2.3 Leveren beheer- en onderhoudsplan

- **Ambitieniveau:** 1
- **Criteriumtype:** CB
- **Criteriumcode:** 030.04

De eis uit de RBA is opgenomen in de Vraagspecificatie.

3.2.4 Milieumanagementsysteem

- **Ambitieniveau:** 1
- **Criteriumtype:** GE
- **Criteriumcode:** 030.07

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.

3.3 Openbare verlichting (OVL)

3.3.1 Ledverlichting

- **Ambitieniveau:** 1
- **Criteriumtype:** EIS
- **Criteriumcode:** 033.01

Deze eis uit de RBA is opgenomen in de Vraagspecificatie.

3.3.2 Levensduur ledsysteem

- **Ambitieniveau:** 1
- **Criteriumtype:** EIS
- **Criteriumcode:** 033.02

Deze eis uit de RBA is opgenomen in de Vraagspecificatie.

3.3.3 Dimbare OVL-installatie

- **Ambitieniveau:** 1
- **Criteriumtype:** EIS
- **Criteriumcode:** 033.03

Deze eis uit de RBA is opgenomen in de Vraagspecificatie.

3.3.4 Lichthinder wordt beperkt

- **Ambitieniveau:** 1
- **Criteriumtype:** EIS
- **Criteriumcode:** 033.04

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.

3.4 Straatmeubilair

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

- **Ambitieniveau:** 1
- **Criteriumtype:** EIS
- **Criteriumcode:** 035.01

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.

Post-consumer wil zeggen dat het de fabriek waar het kunststof wordt geproduceerd heeft verlaten. Bij pre-consumer is dit niet het geval (bijv. snijafval bij de productie).

Deze eis geldt niet:

- Indien de opdrachtnemer hergebruikte* of refurbished producten levert;
- Voor de toepassing van:
 - kunststoffen in touw en vezelversterkte kunststoffen;
 - transparante of gekleurde overkappingen (vanwege vertroebeling).

*** Definitie hergebruikte of refurbished producten:**

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.

3.4.2 Inkoop en reparatie van Speeltoestellen – kunststof onderdelen voorzien van markering

- **Ambitieniveau:** 1
- **Criteriumtype:** GC
- **Criteriumcode:** 035.11

Eis

Indien kunststof onderdelen met een gewicht groter dan of gelijk aan 50 gram en een voor markering beschikbaar oppervlak van minstens 5 cm² zichtbaar worden gemarkeerd met een symbool of afkorting zoals beschreven in ISO 11469 of ISO 1043, wordt de inschrijving hoger gewaardeerd. Uitgezonderd zijn onderdelen waarvan de inschrijver kan onderbouwen dat de markering vanwege technische redenen niet mogelijk is.

3.4.3 Straatmeubilair (incl. Speeltoestellen): verven

- **Ambitieniveau:** 1
- **Criteriumtype:** EIS
- **Criteriumcode:** 035.03

Eis

Het vluchtige organische verbinding (VOS) gehalte (excl. water) voor verven met een spreidend vermogen van ten minste 15 m²/l en voor vernissen die worden toegepast op hout, dient maximaal 250 g/l (met een dekkraft 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.

3.4.4 Duurzaam hout

- **Ambitieniveau:** 1
- **Criteriumtype:** EIS
- **Criteriumcode:** 035.05

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 certificeringssysteem 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.

3.4.5 Speeltoestellen – kunststof

- **Ambitieniveau:** 1
- **Criteriumtype:** EIS
- **Criteriumcode:** 035.10

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% (gewichtspcenten binnen een product) gerecycled materiaal te zijn. Naast post-consumer materiaal mag ook pre-consumer materiaal gebruikt worden.

Post-consumer wil zeggen dat het de fabriek waar het kunststof wordt geproduceerd heeft verlaten. Bij pre-consumer is dit niet het geval (bijv. snijafval bij de productie).

Deze eis geldt niet voor de toepassing van kunststoffen in:

- touw en vezelversterkte kunststoffen;
- transparante of gekleurde overkappingen, vanwege vertroebeling.

3.5 Gemalen

3.5.1 Energierendement van systeem

- **Ambitieniveau:** 1
- **Criteriumtype:** EIS
- **Criteriumcode:** 037.01

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] .

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 aanbidding is opgegeven, dan betaalt de leverende partij over elke procent lager rendement een boete [x].

3.5.2 Energierendement van systeemdelen

- **Ambitieniveau:** 1
- **Criteriumtype:** EIS
- **Criteriumcode:** 037.03

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 aanbidding is opgegeven, dan betaalt de leverende partij over elke procent lager rendement een boete [x].

3.5.3 Smeeroliën en hydraulische vloeistoffen

- **Ambitieniveau:** 1
- **Criteriumtype:** EIS
- **Criteriumcode:** 037.04

Eisen

1. Bij onderhoud dienen smeeroliën met een lage viscositeit te worden gebruikt of geregenereerde smeeroliën met ten minste 25% geregenereerde basisoliën. Smeeroliën met een lage viscositeit zijn die in de categorie SAE 0W30, SAE-5W30 of gelijkwaardig.
2. Hydraulische vloeistoffen en vetten mogen niet voorzien zijn van een gevarenaanduiding voor milieu of gezondheid of een waarschuwingszin (R-zinnen) ten tijde van de toepassing (laagste classificatielimiet in Verordening (EG) nr. 1272/2008 of Richtlijn 99/45/EG van de Raad).

3. Er wordt geen afwijking toegestaan van het verbod in artikel 6, lid 6, van Verordening (EG) nr. 66/2010 voor stoffen die beschouwd worden als zeer zorgwekkend en die zijn opgenomen in de lijst zoals bedoeld in artikel 59 van Verordening (EG) nr. 1907/2006, voor zover die aanwezig zijn in concentraties van meer dan 0,010 gewichtsprocent in mengsels.
4. Het koolstofgehalte uit hernieuwbare grondstoffen moet groter dan of gelijk aan 45% zijn.
5. De cumulatieve massaconcentratie van aanwezige stoffen die zowel niet biologisch afbreekbaar als bio-accumulatief zijn, mag niet meer dan 0,1 gewichtsprocent bedragen.

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 5. Op de website van RVO is een lijst beschikbaar van oliën en vetten die voldoen aan de eisen van het Europese Ecolabel;
- Rapport, of andere documentatie van een onafhankelijk deskundige, waaruit blijkt dat aan dit criterium is voldaan;
- Of gelijkwaardig

3.6 Waterzuiveringsinstallaties en slibbehandeling

3.6.1 Ecotoxiciteit chemicaliën

- **Ambitieniveau:** 1
- **Criteriumtype:** EIS
- **Criteriumcode:** 038.01

Eis

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

3.7 Mobiele werktuigen uitbesteding

3.7.1 Emissie-eisen mobiele dieselwerktuigen met variabel toerental

- **Ambitieniveau:** 1
- **Criteriumtype:** EIS
- **Criteriumcode:** 040.01

Eis

De in te zetten mobiele dieselwerktuigen met motoren met een variabel toerental dienen ten minste te voldoen aan de volgende Fasenormen (vgl. richtlijn 2004/26/EG):

- 19 kW tot 37 kW vermogen: Fasenorm III-A;
- 37 kW tot 56 kW vermogen: Fasenorm III-B;
- 56 kW tot 560 kW vermogen: Fasenorm IV.

De in te zetten mobiele dieselwerktuigen met motoren met een constant toerental dienen ten minste te voldoen aan Fasenorm II (vgl. verordening (EU) 2016/1628).

Verificatie

De opdrachtnemer kan worden gevraagd om een afschrift van de conformiteitsverklaring van de voor de uitvoering van de opdracht in te zetten mobiele dieselwerktuigen. Hieruit is onder andere af te leiden welke emissie(s) aan het type/de typen werktuigen is/zijn toegekend.

3.7.2 Milieumanagementsysteem

- **Ambitieniveau:** 1
- **Criteriumtype:** GE
- **Criteriumcode:** 040.03

Eis

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

- de concrete maatregelen die zijn of worden getroffen om de milieubelasting van de bedrijfsprocessen die verband houden met de uitvoering van de opdracht, zoals het gebruik van biologische smeermiddelen, bandenspanning controle en beheer, het gebruik van load sensing technologie en hydraulische olie en de wijze waarop met koelmiddelen wordt omgegaan, te verminderen;
- dat naleving van de desbetreffende milieuwetgeving is geborgd;
- dat aandacht wordt besteed aan de bewustwording en de competentie van medewerker(s) ten aanzien van het omgaan met de voor deze opdracht relevante milieuaspecten;
- hoe de voor deze opdracht relevante milieuaspecten worden gemonitord als basis voor kwaliteitsgarantie.

Op de website van [EMAS] (http://ec.europa.eu/environment/emas/index_en.htm) is meer informatie te vinden.

Verificatie

De opdrachtnemer kan worden gevraagd om documentatie te overleggen waaruit blijkt dat aan bovenstaande eisen wordt voldaan. Een milieuzorgsysteem zoals ISO 14001 of EMAS toont aan dat een bedrijf of organisatie een systematisch milieumanagementsysteem hanteert voor het behandelen van relevante milieukwesties tijdens dagelijkse activiteiten. Het certificaat dient de in de eis gestelde onderwerpen te betreffen (concrete maatregelen, borging van naleving milieuwetten, bewustwording personeel, monitoring).

Op de website van Stichting Coördinatie en Certificatie Milieu- en Arbo-managementsystemen (SCCM) is een database te vinden waarin alle ISO 14001-certificaten zijn opgenomen van in Nederland door de RvA geaccrediteerde certificatie-instellingen. Wanneer een certificaat er onverhoopt niet op mocht staan, dan kan contact worden gezocht met de betreffende certificatie-instelling. Op www.sccm.nl zijn de contactgegevens te vinden.

3.7.3 Training in het nieuwe draaien

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

Eis

Het aandeel van de machinisten en/of uitvoerders, voormannen en planners welke bij de uitvoering van de opdracht is betrokken en de erkende training Het Nieuwe Draaien heeft gevolgd is minimaal 25%.

Daarnaast hebben alle projectmedewerkers bij de start van het project een projectspecifieke introductie ontvangen met aandacht voor Het Nieuwe Draaien.

Verificatie

De opdrachtnemer kan worden gevraagd een lijst van actieve werknemers op het project en certificatie van erkende instelling/trainer te overleggen. De opdrachtnemer dient een overzicht van de projectspecifieke introductie en presentielijsten in na de start van het project.

3.7.4 Onderhoud gebruikte mobiele werktuigen

- **Ambitieniveau:** 1
- **Criteriumtype:** EIS
- **Criteriumcode:** 040.07

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 de gebruiker waaruit blijkt dat de machine bij aflevering correct is ingesteld (afleveringsbeurt door leverancier voldoet ook), de machine volgens een periodiek keuringssysteem wordt gekeurd (kopie keuringsformulier of keuringssticker voldoet ook) en regulier onderhouden wordt middels een onderhoudsprogramma (kopie onderhouds-/servicecontract voldoet ook).

3.8 Verkeersregelinstallaties

3.8.1 Diminrichting in regeltoestel

- **Ambitieniveau:** 1
- **Criteriumtype:** EIS
- **Criteriumcode:** 041.01

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.

3.8.2 Energiezuinige lichtbronnen

- **Ambitieniveau:** 1
- **Criteriumtype:** EIS
- **Criteriumcode:** 041.02

Eis

Energiezuinige lichtbronnen volgens Klasse II lichtbronnen.

3.8.3 Energiezuinige lampen voor scheepvaartseinen

- **Ambitieniveau:** 1
- **Criteriumtype:** EIS
- **Criteriumcode:** 041.04

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.

3.8.4 Levenscycluskosten

- **Ambitieniveau:** 1
- **Criteriumtype:** EIS
- **Criteriumcode:** 041.12

Deze eis uit de RBA is opgenomen in de Vraagspecificatie.

3.8.5 Minimale levensduur en garantie

- **Ambitieniveau:** 1
- **Criteriumtype:** EIS
- **Criteriumcode:** 041.14

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 inkoopende 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.

3.9 Groenvoorzieningen

3.9.1 Vakbekwaam ontwerper en beheerder groenvoorziening

- **Ambitieniveau:** 1
- **Criteriumtype:** GE
- **Criteriumcode:** 043.01

Deze eis uit de RBA is opgenomen in de Vraagspecificatie.

3.9.2 Verwerven van bloembollen

- **Ambitieniveau:** 1
- **Criteriumtype:** EIS
- **Criteriumcode:** 043.02

Eisen

Ten minste 90% (berekend op basis van de aankoopsom) van de te gebruiken bloembollen voldoet aan de volgende eisen:

1. Bij de teelt van bloembollen zijn bepalingen ten aanzien van het gebruik van gewasbeschermingsmiddelen van toepassing van de meest recente versie van het On the way to PlanetProof schema 'plantaardige producten':
 - a. Gewasbeschermingsmiddelen uit bijlage 2c, lijst I zijn niet toegestaan.
 - b. Er zijn aantoonbaar compenserende maatregelen genomen voor gewasbeschermingsmiddelen uit bijlage 2c, lijst II.
 - c. Overige wettelijk toegelaten gewasbeschermingsmiddelen die niet zijn genoemd in lijst I en lijst II van bijlage 2c., zoals de 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).
 - d. 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.
2. Bij de teelt van bloembollen zijn voor de bemesting de wettelijke gebruiksnormen gehanteerd en is de organische stofbalans op bedrijfsniveau berekend. Hierbij moet inzichtelijk worden gemaakt dat het bedrijf streeft naar een positieve organische stofbalans (jaarlijkse aanvoer van effectieve organische stof (EOS) is minimaal gelijk aan afbraak).
3. Bij levering zit een lijst van de geleverde bloembollen 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 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;
 - gelijkwaardig certificaat.
- Registratie van de bij de teelt van de geleverde 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 geacordeerd door een onafhankelijke deskundige derde (zoals een geaccrediteerde certificerende instelling). Het document kan per boomkwekerijproduct of partij bloembollen zijn opgesteld, of de geaggregeerde gegevens van meerdere producten bevatten.
- Of gelijkwaardig.

3.9.3 Boomkwekerijproducten van een genetische kwaliteit (buitenstedelijk)

- **Ambitieniveau:** 1
- **Criteriumtype:** EIS
- **Criteriumcode:** 043.04

Deze eis uit de RBA is opgenomen in de Vraagspecificatie.

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

- **Ambitieniveau:** 1
- **Criteriumtype:** EIS
- **Criteriumcode:** 043.06

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.

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

- **Ambitieniveau:** 1
- **Criteriumtype:** EIS
- **Criteriumcode:** 043.07

Eis

Bij de uitvoering van de werkzaamheden worden geen gewasbeschermingsmiddelen gebruikt, tenzij in de volgende gevallen en na toestemming of opdracht van de opdrachtgever:

1. Bestrijding van invasieve soorten noodzakelijk is i.v.m. (verwachte) overlast en risico voor de volksgezondheid';
en
2. Er kan worden aangetoond dat mechanische bestrijding niet voldoende werkt.

Verificatie

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

3.9.6 Duurzaam ontwerp groenvoorziening

- **Ambitieniveau:** 1
- **Criteriumtype:** EIS
- **Criteriumcode:** 043.09

Deze eis uit de RBA is opgenomen in de Vraagspecificatie.

3.9.7 Plan en rapportage bemesting, bodemverbetering en bestrijding

- **Ambitieniveau:** 1
- **Criteriumtype:** CB
- **Criteriumcode:** 043.11

Eis

De opdrachtnemer dient voorafgaande aan de beplantings- en onderhoudswerkzaamheden te overhandigen:

- bodemanalyse;
- advies aangaande bemesting en bodemverbetering;
- werkplan waarin vermeld staat hoe en wanneer het onderhoud wordt uitgevoerd conform het advies uit het criterium Toepassen meststoffen en bodemverbeteraars bij aanleg en onderhoud van openbaar groen (incl. sport- en speelvelden) en de eisen uit Bestrijden van ongewenste kruiden, ziekten en plagen (excl. sport- en speelvelden).
- Uitgangspunt is dat de juiste beplanting op de juiste plek komt en dus zo min mogelijk bijbemesting etc. nodig is.

De opdrachtnemer dient periodiek over de uitgevoerde werkzaamheden te rapporteren.

3.9.8 Eisen aan compost

- **Ambitieniveau:** 1
- **Criteriumtype:** EIS
- **Criteriumcode:** 043.17

Eisen:

- 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 groeimateriaal, 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

3.9.9 Geen invasieve exoten

- **Ambitieniveau:** 1
- **Criteriumtype:** EIS
- **Criteriumcode:** 043.18

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.

3.10 Reiniging openbare ruimte

3.10.1 Verwijderen van graffiti met hogedrukwaterreiniger

- **Ambitieniveau:** 1
- **Criteriumtype:** EIS

- **Criteriumcode:** 044.01

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.

3.10.2 Ervaring met integraal plaagdiermanagement (IPM)

- **Ambitieniveau:** 1
- **Criteriumtype:** GE
- **Criteriumcode:** 044.03

Deze eis uit de RBA is opgenomen in de Vraagspecificatie.

3.10.3 Milieumanagementsysteem

- **Ambitieniveau:** 1
- **Criteriumtype:** GE
- **Criteriumcode:** 044.04

Eis

De opdrachtnemer dient voor dat deel/die delen van de organisatie dat/die betrokken is/zijn bij de uitvoering van de aanbestede opdracht te beschikken 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.

3.10.4 Milieu-impact onkruidbestrijding op verhardingen

- **Ambitieniveau:** 1
- **Criteriumtype:** EIS
- **Criteriumcode:** 044.06

Eis

Dit criterium is van toepassing indien volgens het Besluit gewasbeschermingsmiddelen en biociden, chemische onkruidbestrijding niet toelaatbaar is. Gedurende de contractperiode moet het aantal werkronde mechanische onkruidbestrijding beperkt blijven tot:

- voor de heteluchtmethode maximaal 6 werkronde per jaar;
- voor de overige mechanische methoden maximaal 4 werkronde per jaar; Of de opdrachtnemer 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 werkronde 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.

3.10.5 Plan van aanpak Plaagdierbeheersing

- **Ambitieniveau:** 1
- **Criteriumtype:** CB
- **Criteriumcode:** 044.08

Eis

De opdrachtnemer stelt binnen een half jaar na opdracht, in samenspraak met de opdrachtgever, een plan van aanpak op waarin wordt vastgelegd hoe, gedurende de contractperiode en binnen de kaders van het contract, de principes van integrated pest management (IPM) in praktijk worden gebracht.

In het plan van aanpak worden ten minste de volgende onderwerpen meegenomen:

- Schoonmaakwerkzaamheden;
- Afval en afvalscheiding (wegnemen van voedsel);
- Energie- en watergebruik (voor thermische bestrijding);
- Gebruik van biociden;
- Monitoring plaagdieren;
- Communicatie met gebruikers.

Voor deze onderwerpen worden doelstellingen vastgesteld en worden maatregelen geformuleerd (zowel voor de eigenaar/opdrachtgever als voor de uitvoerder/opdrachtnemer) om de doelstellingen te realiseren.

3.10.6 Vermindering van PM10 straatstof

- **Ambitieniveau:** 1
- **Criteriumtype:** EIS
- **Criteriumcode:** 044.13

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.

3.10.7 Milieukeur voor buitenschoonmaakmiddelen

- **Ambitieniveau:** 1
- **Criteriumtype:** EIS
- **Criteriumcode:** 044.14

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.

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	029.01
Civiele constructies	Duurzaam ontwerp staalconstructie	029.02
Civiele constructies	Duurzaam hout	029.07
Civiele constructies	Milieuvriendelijke smeermiddelen voor bewegingswerken	029.12
Conserveringswerken	Oplosmiddelarme conserveringssystemen	030.01
Conserveringswerken	Producten met lood- of chromaathoudende pigmenten	030.02
Conserveringswerken	Leveren beheer- en onderhoudsplan	030.04
Conserveringswerken	Milieumanagementsysteem	030.07
Openbare verlichting	Toepassen ledverlichting	033.01
Openbare verlichting	Levensduur ledsysteem	033.02
Openbare verlichting	Dimbare OVL-installatie	033.03
Openbare verlichting	Lichthinder wordt beperkt	033.04

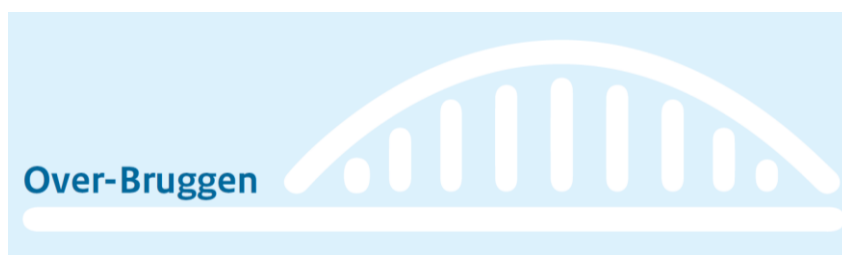
Straatmeubilair	Straatmeubilair (m.u.v. Speeltoestellen): meer dan 5% kunststof	035.01
Straatmeubilair	Inkoop en reparatie van Speeltoestellen – kunststof onderdelen voorzien van markering	035.11
Straatmeubilair	Straatmeubilair (incl. Speeltoestellen): verven	035.03
Straatmeubilair	Duurzaam hout	035.05
Straatmeubilair	Speeltoestellen - kunststof	035.10
Gemalen	Energierendement van systeem	037.01
Gemalen	Energierendement van systeemdelen	037.03
Gemalen	Smeeroliën en hydraulische vloeistoffen	037.04
Waterzuiveringsinstallaties en slibbehandeling	Ecotoxiciteit chemicaliën	038.01
Mobiele werktuigen uitbesteding	Emissie-eisen mobiele dieselwerktuigen met variabel toerental	040.01
Mobiele werktuigen uitbesteding	Milieumanagementsysteem	040.03
Mobiele werktuigen uitbesteding	Training in het nieuwe draaien	040.04
Mobiele werktuigen uitbesteding	Onderhoud gebruikte mobiele werktuigen	040.07
Verkeersregelinstallaties	Diminrichting in regeltoestel	041.01
Verkeersregelinstallaties	Energiezuinige lichtbronnen	041.02
Verkeersregelinstallaties	Energiezuinige lampen voor scheepvaartseinen	041.04
Verkeersregelinstallaties	Levenscycluskosten	041.12
Verkeersregelinstallaties	Minimale levensduur en garantie	041.14
Groenvoorzieningen	Vakbekwaam ontwerper en beheerder groenvoorziening	043.01
Groenvoorzieningen	Verwerven van bloembollen	043.02
Groenvoorzieningen	Boomkwekerijproducten van een genetische kwaliteit (buitenstedelijk)	043.04
Groenvoorzieningen	Meststoffen en bodemverbeteraars bij aanleg en onderhoud van openbaar groen (incl. sport- en speelvelden)	043.06
Groenvoorzieningen	Ongewenste kruiden, ziekten en plagen (excl. sport- en speelvelden)	043.07
Groenvoorzieningen	Duurzaam ontwerp groenvoorziening	043.09
Groenvoorzieningen	Plan en rapportage bemesting, bodemverbetering en bestrijding	043.11
Groenvoorzieningen	Eisen aan compost	043.17
Groenvoorzieningen	Geen invasieve exoten	043.18
Reiniging openbare ruimte	Verwijderen van graffiti met hogedrukwaterreiniger	044.01
Reiniging openbare ruimte	Ervaring met integraal plaagdiermanagement (IPM)	044.03
Reiniging openbare ruimte	Milieumanagementsysteem	044.04
Reiniging openbare ruimte	Minder milieu-impact onkruidbestrijding op verhardingen	044.06
Reiniging openbare ruimte	Plan van aanpak Plaagdierbeheersing	044.08
Reiniging openbare ruimte	Verminderen van PM10 straatstof	044.13
Reiniging openbare ruimte	Milieukeur voor buitenschoonmaakmiddelen	044.14



BIJLAGE K – Minimum eisen emissienormen materieel en energiedragers

Vraagspecificatie Proces – Raamovereenkomst

Realisatie Variabel onderhoud stalen bruggen West Nederland Zuid
Project Over-Bruggen



Zaaknummer: **31196743**

Datum: 14 januari 2025

Bijlage K - Minimum eisen emissienormen materieel en energiedragers

Deze bijlage 'Eisen duurzaam materieel' geldt **generiek** voor alle Nadere Overeenkomsten

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

Voertuigen				
N1 – Bestelbusjes en M1 – Personenvervoer	Euro 5	Euro 6	100% ZE	100% ZE
N2 – Lichte vrachtwagens	Euro V	Euro VI	Euro VI	100% ZE
N3 – Zware vrachtwagens en M2/M3 – Bussen	Euro V	Euro VI	Euro VI	Euro VI
Vaartuigen				
Motoren voor zeegaande vaartuigen		Emissies conform Tier I eisen	Emissies conform Tier II eisen	Emissies conform Tier III eisen
Energiedragers voor Zeegaande vaartuigen	10% duurzame Energiedragers ²	20% duurzame energiedragers ²	40% duurzame energiedragers ²	60% duurzame energiedragers ²
Motoren voor binnenlandse vaartuigen	Geen eis	Geen eis	Emissies conform CCR II	Emissies conform CCR II of stage V (IWP-IWA)
Energiedragers voor binnenlandse vaartuigen	20% duurzame energiedragers ²	35% duurzame energiedragers ²	60% duurzame energiedragers ²	75% duurzame energiedragers ²

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 L – Levering Areaalgegevens

Vraagspecificatie Proces – Raamovereenkomst

Realisatie Variabel onderhoud stalen bruggen West Nederland Zuid
Project Over-Bruggen



Zaaknummer: **31196743**

Datum: 14 januari 2025

Bijlage L - Levering Areaalgegevens

Niet van toepassing op niveau Raamovereenkomst.

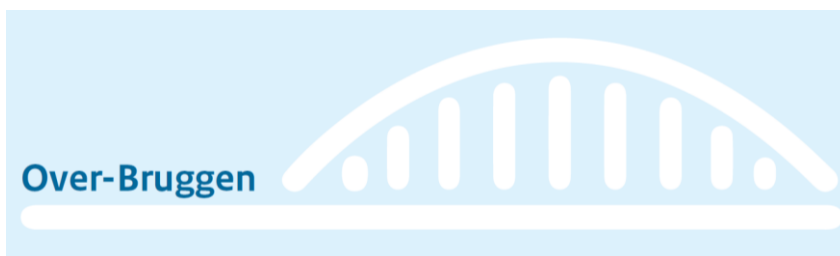
Per Nadere Overeenkomst wordt een bijlage L 'Levering Areaalgegevens' toegevoegd.



BIJLAGE M - Cybersecurity Implementatie- richtlijn Objecten v2.4

Vraagspecificatie Proces – Raamovereenkomst

Realisatie Variabel onderhoud stalen bruggen West Nederland Zuid
Project Over-Bruggen



Zaaknummer: **31196743**

Datum: 14 januari 2025

Bijlage M - Cybersecurity Implementatierichtlijn Objecten v2.4

Deze bijlage 'Cybersecurity Implementatierichtlijn Objecten' geldt **generiek** voor alle Nadere Overeenkomsten.



RWS INFORMATIE

Cybersecurity Implementatierichtlijn Objecten



Datum 23 april 2021
Versie 2.4
Status Definitief

Colofon

Uitgegeven door	CIV/IRN/Security Centre/Security by Design
Auteurs	Turabi Yildirim Mark van Leeuwen Michael Theuerzeit Mieke van Nierop
Datum	23 april 2021
Versie	2.4
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

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	11
2	VERDIEPENDE MAATREGELEPAKKETTEN	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	119
BIJLAGE CSR 18	BACK-UP EN RECOVERY	120
BIJLAGE CSR 19	INTELLECTUEEL EIGENDOM	121
BIJLAGE CSR 20	CAMERA'S EN ONGANG MET CAMERABEELDEN VAN DE VERKEERSREGISTRATIESYSTEMEN	128
BIJLAGE CSR 21	UNIFORM AANLEVEREN VAN INCIDENTRAPPORTAGES	129
BIJLAGE CSR 22	VIRTUALISATIE	131
BIJLAGE CSR 23	VERWIJDERING EN Vernietiging van informatie en apparatuur	132
BIJLAGE A	BEGRIPPENLIJST	133
BIJLAGE B	CYBERSECURITY DOSSIER / CYBERSECURITY BEVEILIGINGSPLAN	135
BIJLAGE C	BEST PRACTICE VOOR RISICO INSCHATTING BIJ CSIR AFWIJKINGEN	136

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 RAMSSHEEP¹ 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

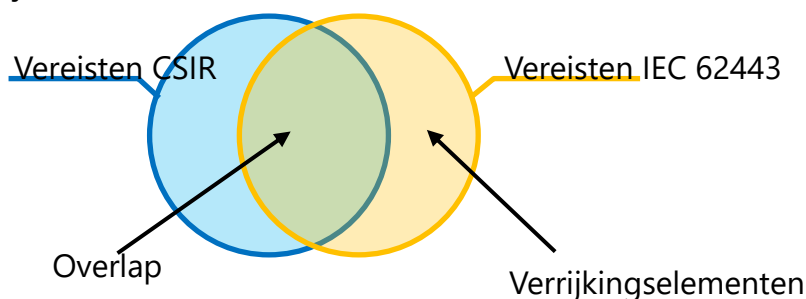
Cybersecurity Implementatierichtlijn Objecten (CSIR)

Beschrijving CSIR

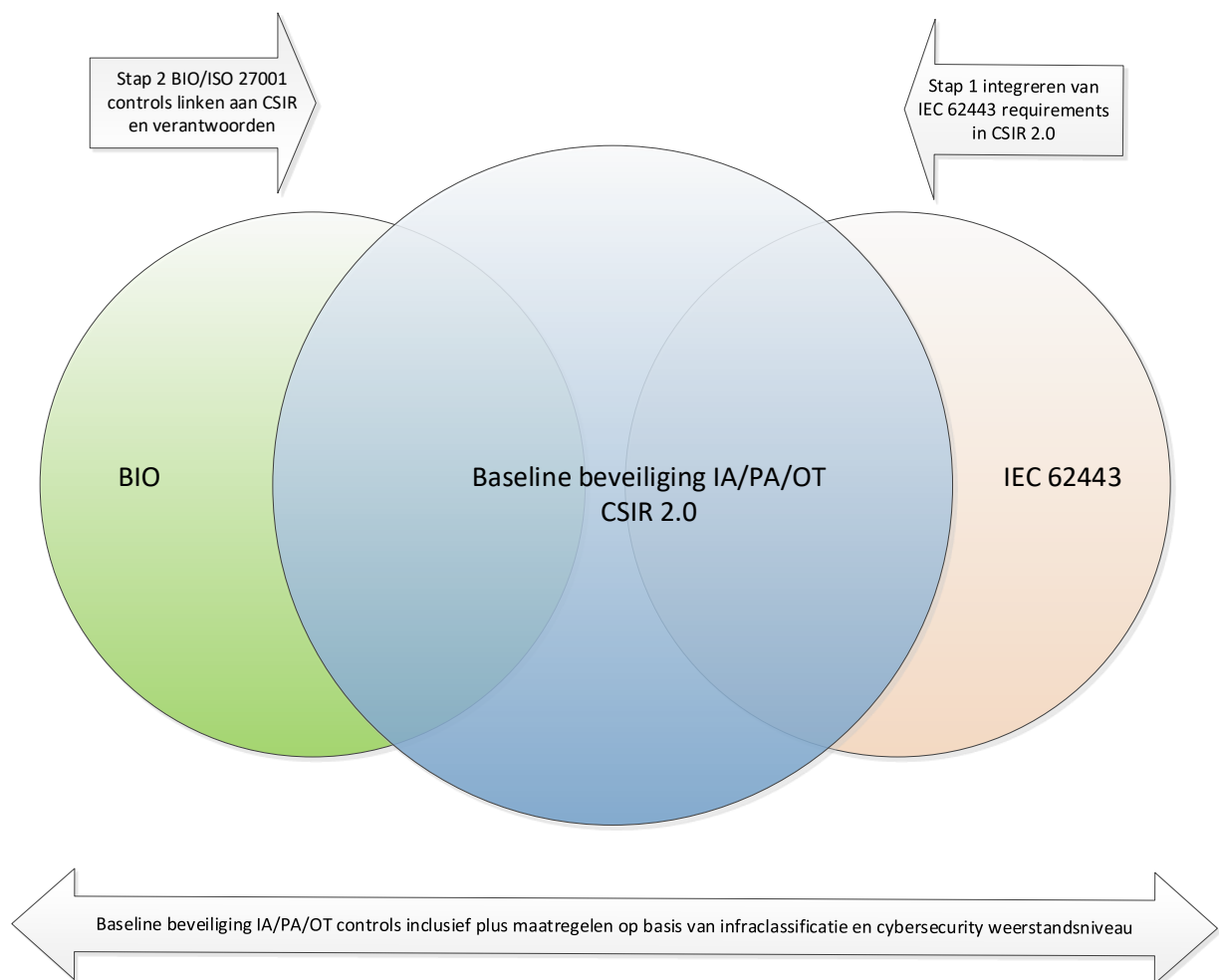
De eerste versie van de Cybersecurity Implementatierichtlijn Objecten is een vertaalslag van de relevante controls/beheersdoelen uit de BIO en de NCSC Checklist beveiliging ICS/SCADA systemen met controls en requirements aanvullingen uit de relevante delen van de IEC 62443 voor de beveiliging van Industriële 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 geormerkt 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

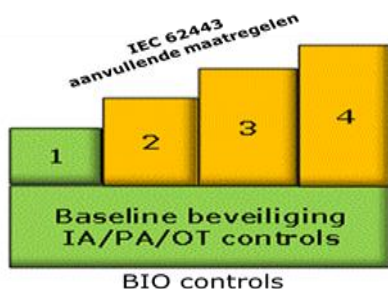
De Cybersecurity Implementatierichtlijn Objecten 2.0 is een doorontwikkeling van de eerste versie van de Cybersecurity Implementatie Richtlijn Objecten RWS. In versie 1.0 van de Cybersecurity Implementatie Richtlijn Objecten waren al de nodige en beschikbare requirements uit de voorlopers van de IEC 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 kwetsbaarheden 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.

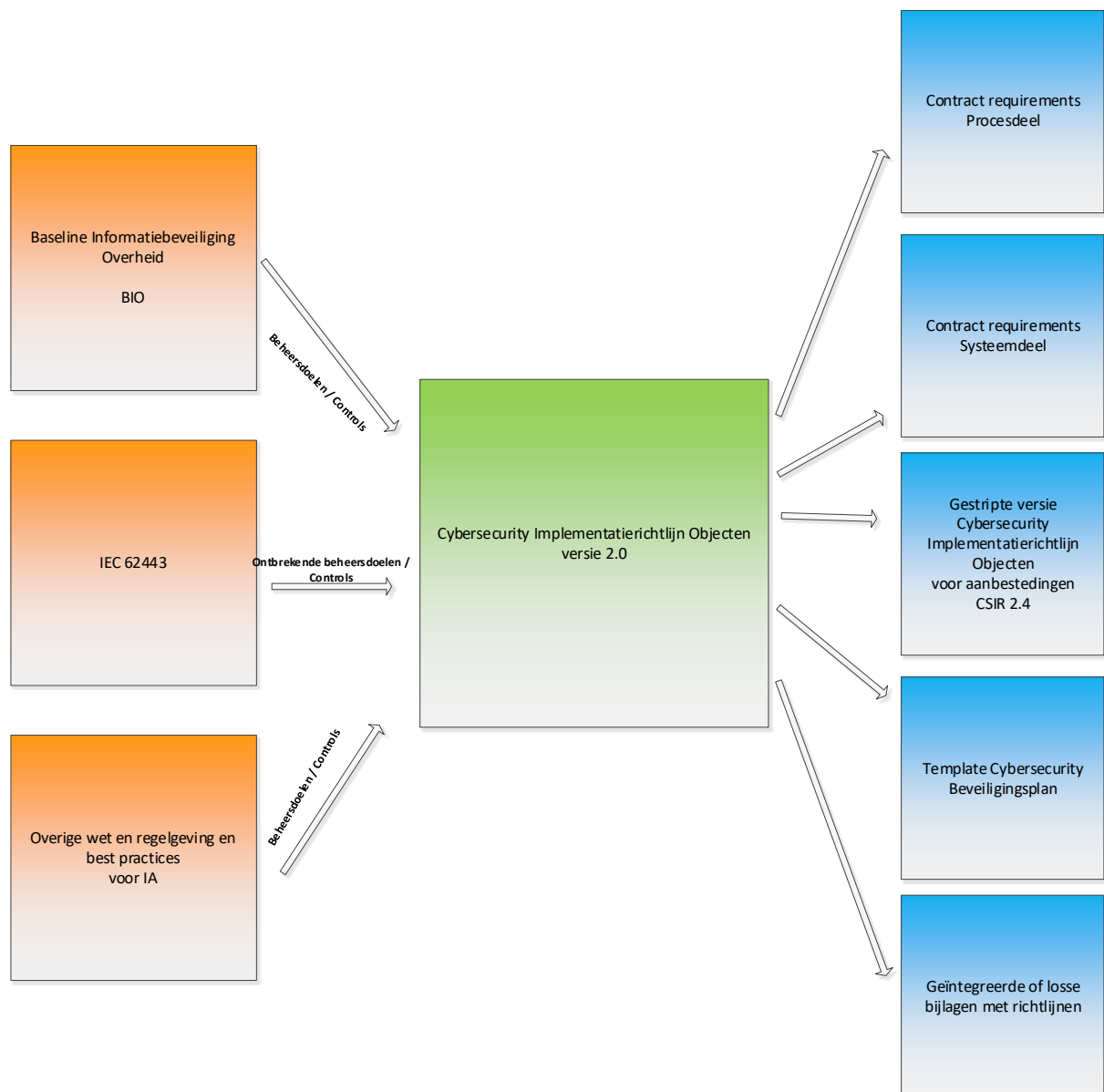
De door de controls aangeroepen verdiepende uitwerkingen uit hoofdstuk 2 van de CSIR zijn maatregel pakketten om de meest voorkomende kwetsbaarheden en risico's binnen de Industriële Automatiseringsomgeving te mitigeren. Bij de keuze voor deze verdiepende set van maatregelen is gebruik gemaakt van internationale 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 weerstandsniveau 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.

Hoofdstuk 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 requirements 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		Weerstandsniveau			
No.	Vereiste	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		Weerstandsniveau			
No.	Vereiste	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		Weerstandsniveau			
No.	Vereiste	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		Weerstandsniveau			
No.	Vereiste	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		Weerstandsniveau			
No.	Vereiste	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 gegeven 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		Weerstandsniveau			
No.	Vereiste	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		Weerstandsniveau			
No.	Vereiste	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		Weerstandsniveau			
No.	Vereiste	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		Weerstandsniveau			
No.	Vereiste	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		Weerstandsniveau			
No.	Vereiste	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		Weerstandsniveau			
No.	Vereiste	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		Weerstandsniveau			
No.	Vereiste	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, beheerder dient aan te kunnen tonen dat de antimalware software correct is geïnstalleerd en geconfigureerd. De juiste werking dient hierbij te kunnen worden aangetoond.	X	X	X	X
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 netwerkkapparatuur 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 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.	X	X		
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		Weerstandsniveau			
No.	Vereiste	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		Weerstandsniveau			
No.	Vereiste	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 zijn van alle recente beveiligingsupdates en patches. Patches mogen het niveau van systeem hardening niet aantasten.	X	X	X	X
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		Weerstandsniveau			
No.	Vereiste	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		Weerstandsniveau			
No.	Vereiste	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	X	X	X	X

	netwerkverkeer (bijvoorbeeld de SCADA en PLC systemen) 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		Weerstandsniveau			
No.	Vereiste	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 modules 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

	I. 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		Weerstandsniveau			
No.	Vereiste	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 risicomangement 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		Weerstandsniveau			
No.	Vereiste	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		Weerstandsniveau			
No.	Vereiste	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		Weerstandsniveau			
No.	Vereiste	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		Weerstandsniveau			
No.	Vereiste	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		Weerstandsniveau			
No.	Vereiste	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	X	X	X	X

	(waaronder fysieke en logische netwerktekeningen, verbindingen 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		Weerstandsniveau			
No.	Vereiste	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		Weerstandsniveau			
No.	Vereiste	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: - 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; - 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; - Back-ups worden bewaard tot het moment van uitdienstname van het betreffend systeem; - 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		Weerstandsniveau			
No.	Vereiste	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. Configuratie documentatie 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 Wettransfer (of vergelijkbare service) mag uitsluitend versleuteld worden uitgewisseld tussen Rijkswaterstaat en Opdrachtnemer, waarbij bestanden worden versleuteld 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 Wettransfer (of vergelijkbare service) mag uitsluitend versleuteld worden uitgewisseld tussen Rijkswaterstaat en BAW partners, waarbij bestanden worden versleuteld 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

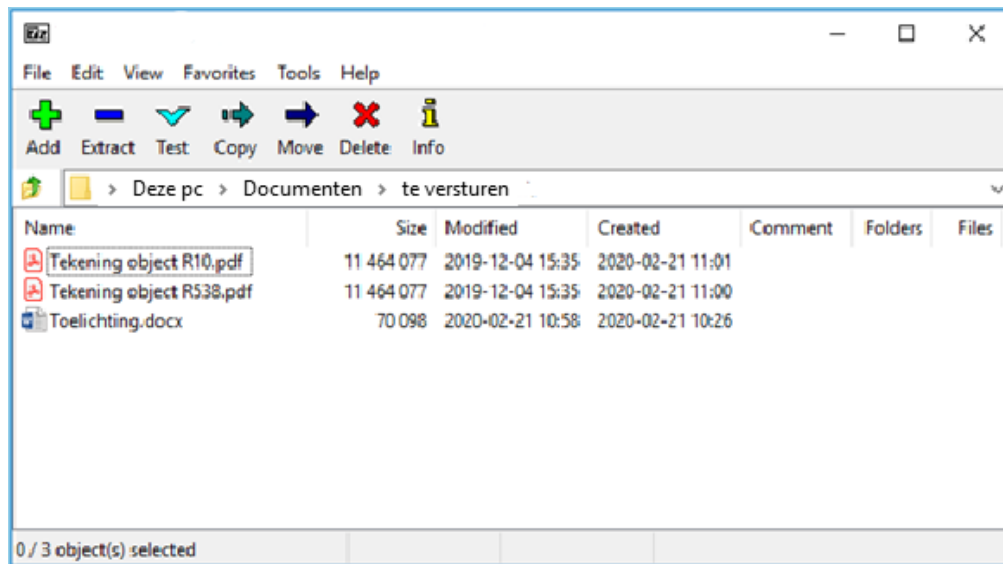
Informatie met de classificatie RWS Bedrijfsvertrouwelijk of TLP AMBER mag onversleuteld via servers van opdrachtgever, opdrachtnemer of BAW partner worden uitgewisseld, mits er een voldoende authenticatie van de gebruiker en zijn bevoegdheden plaatsvindt.

CSR 1.2.2 Versleutelen van gegevens

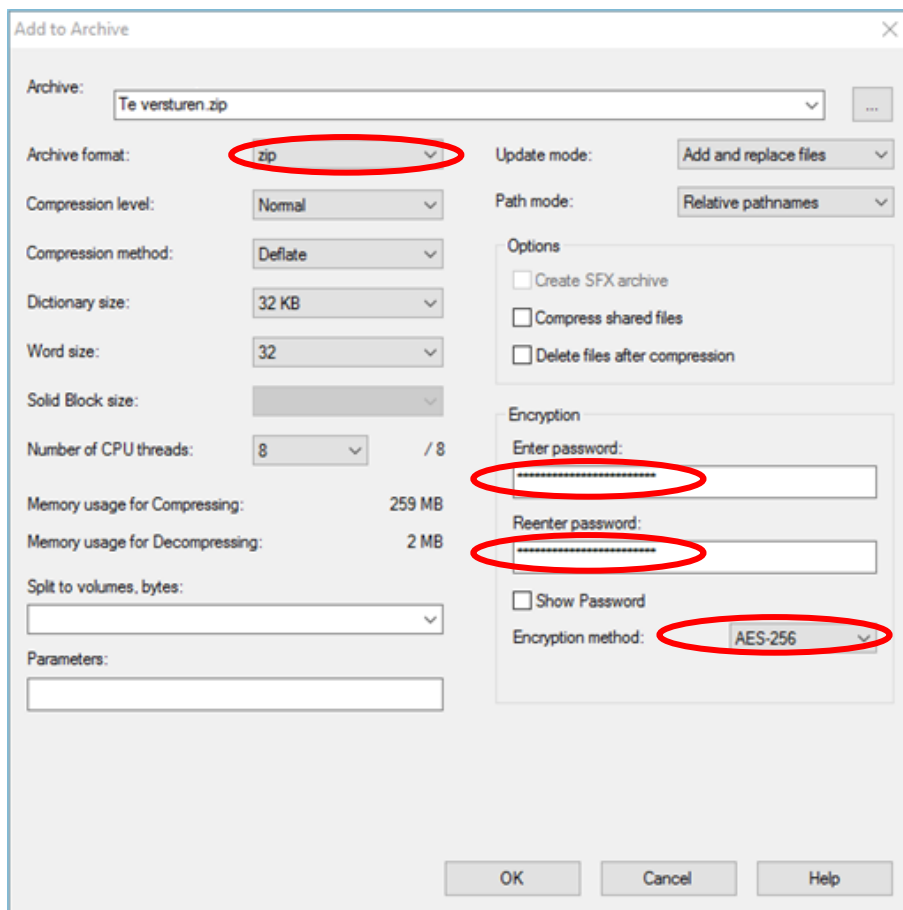
Wanneer versleuteling van informatie nodig is, dient dit te gebeuren met ten minste AES 256 encryptie en een sterk wachtwoord dat voldoet aan de vereisten voor wachtwoorden. Voor versleuteling maakt RWS gebruik van 7-Zip. Dit is een eenvoudig te gebruiken computerprogramma, waarmee bestanden versleuteld 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 zoneringsmodel voor het IV netwerk is gebaseerd op het zoneringsmodel van de NORA².

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:

- Netwerksegmenten zijn fysiek of logisch van elkaar, gescheiden (er kan geen verkeer vrij tussen verschillende segmenten worden uitgewisseld);
- Voor de netwerksegmenten is bepaald aan welke zones deze gekoppeld kunnen zijn;
- 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 routing 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.

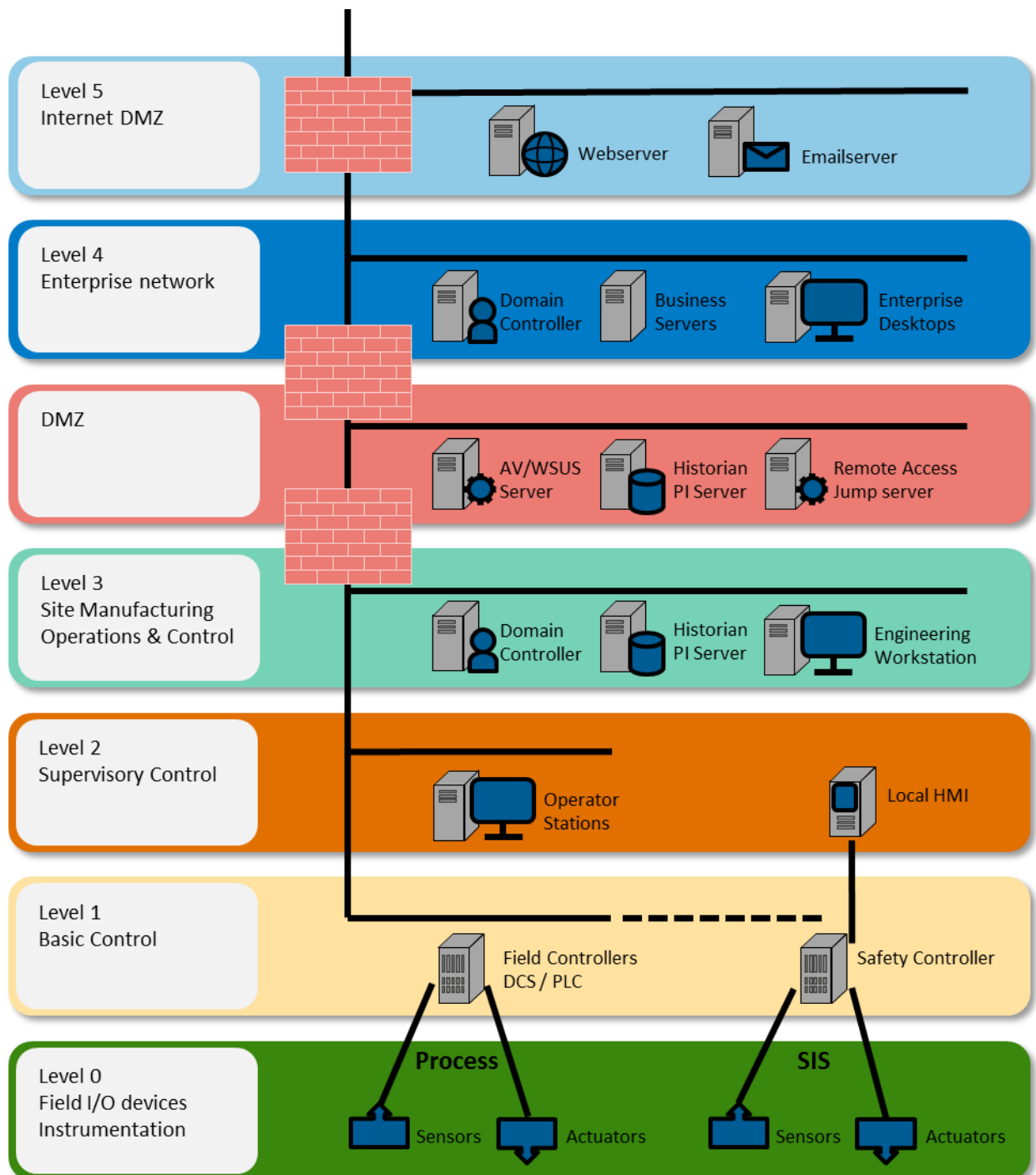
CSR 3.2.4 Gelaagde opbouw van het netwerk

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 kwetsbaarheidsscans uitgevoerd te worden voor de gebruikte IoT apparatuur. Hierbij is aandacht voor kwetsbaarheidsscans, 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 algemeenschap 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:

- 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).
- 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 leettertekens (Bijvoorbeeld: 3KleineKleutertjesdiezatenopeen###).
- 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 gecijferd.
- 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:

- Inventariseer voor het object welke software en firmware er op elk apparaat draait en neem dit op in het (bij voorkeur centrale) CMDB;
- 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);
- 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;
- 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;
- 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 $t > 5 \text{ jaar}$	De kans en daarmee het falen of misbruik van de functie van het object wordt niet binnen 5 jaar verwacht.
2	Klein $(3 \text{ jaar} < t \leq 5 \text{ jaar})$	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 $(2 \text{ jaar} < t \leq 3 \text{ jaar})$	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 $(1 \text{ jaar} < t \leq 2 \text{ jaar})$	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 $(t \leq 1 \text{ jaar})$	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 betreffend 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 moeilijker 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.

	Impact			
	Verwaarloosbaar (1)	Beperkt (2)	Groot (3)	Ernstig (4)
S	Het niet patchen leidt tot een niet compliancy registratie en rapportage en heeft een verwaarloosbare invloed op gebruiksveiligheid van het object, maar dit blijft binnen geaccepteerde grenzen.	Het niet patchen leidt tot een niet compliancy registratie en rapportage en 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.	Het niet patchen 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 ernstige toename van het aantal ongelukken met blijvend letsel of met blijvende gezondheidsschade.	Het niet patchen 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.
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 betreffende 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	Uitstel patch geeft > 1000 k Euro aan

	Impact			
	Verwaarloosbaar (1)	Beperkt (2)	Groot (3)	Ernstig (4)
			extra onderhoudskosten.	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 bepaald 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 een 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) versie³;
 - Installeer de laatste (mogelijke) patches¹;
 - Schakel niet-gebruikte system services uit of verwijder deze⁴;
 - ii. Virtualization layer;
 - Gebruik de nieuwste (mogelijke) versie¹; Deze versie dient wel te worden ondersteund door de softwareleverancier;
 - Installeer de laatste (mogelijke) patches¹;
 - Schakel niet-gebruikte functionaliteit uit of verwijder deze;
 - iii. Applicaties
 - Verwijder alle niet noodzakelijke applicaties;
 - Installeer de nieuwste versie van applicaties¹; Deze versie dient wel te worden ondersteund door de softwareleverancier;
 - Installeer de laatste (mogelijke) patches¹;
 - Zorg voor secure coding tijdens ontwikkeling van eigen software⁵;
 - iv. Firmware
 - Installeer de laatste (mogelijke) firmware¹;
- 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:

- Het verzamelen, analyseren en reageren op status info van de ICT en ISC/SCADA deelsystemen binnen de IA;
- Het ontdekken van menselijke fouten of systeem fouten, zoals fouten bij de bediening, maar ook het ontdekken van indringers in systemen;
- Het ontdekken van corruptie van data of programmatuur;
- 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:

- Een syslog server inrichten die de syslog events vanuit de gelaagd opgebouwde objectnetwerk verzamelt en toegankelijk maakt voor analysedoeleinden en automatische waarschuwingen;
- De syslogserver wordt voorzien van malware protectie, hardening en logging van de activiteiten op de server zelf (toegang, config/systeemaanpassingen en kopieer acties);
- De syslogserver en syslog database is alleen toegankelijk voor geautoriseerden;
- De syslog database kan niet gewijzigd of vernietigd worden door beheerders;
- Het openen van een nieuw logbestand maar ook het verwijderen ervan dient te worden gelogd;
- De bewaartermijn van de syslog database moet instelbaar zijn met een minimum van een maand;
- Op aangeven van Opdrachtgever wordt de syslog database langer bewaard;
- De syslog database dient zodanig ingericht te worden dat deze via het RWS netwerk toegankelijk is voor het Security Operations Centre van RWS;
- 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;
- 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;
- 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;
- 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;
- 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

Event:	Omschrijving:
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
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

- Gebruik **bij voorkeur een nieuwe USB stick** waar de malwarescan software op geïnstalleerd gaat worden;
- 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;
- Scan de USB stick **voor elk gebruik** op een computer buiten het object met een actuele malwarescan software;
- 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".

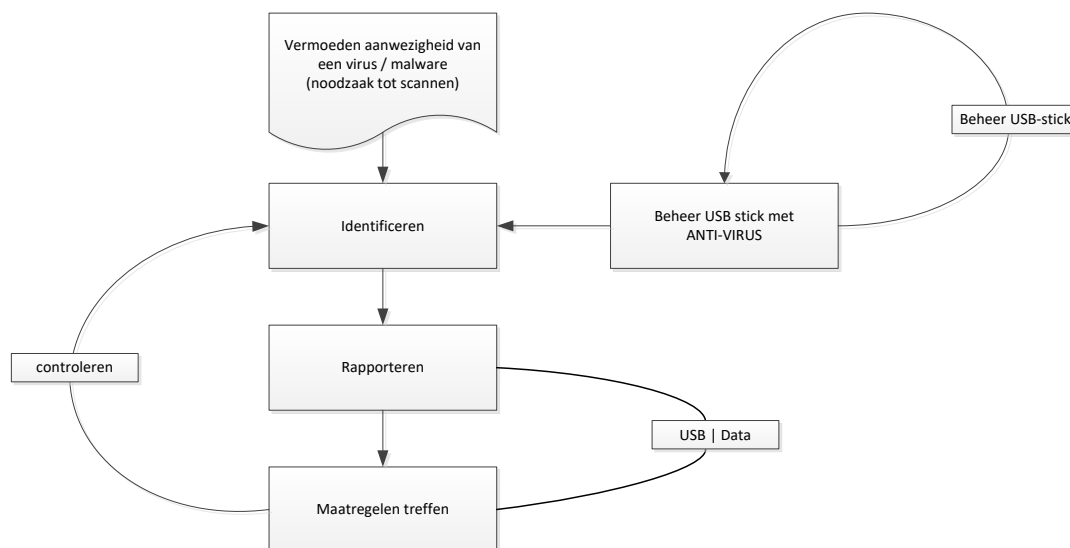
CSR 11.2.3 Voorbereiden op malwarescanning

Handel volgens onderstaande werkwijze:

- Update de USB stick met de laatste antimalware software en laatst beschikbare malwaredefinities;
- Scan de USB stick met antimalware software **voor elk gebruik** op een computer buiten het object met een actuele malwarescan software;
- Zet op deze USB stick een malwarescan tool/software die **uitsluitend een rapportage** geeft over de besmetting zonder automatische handelingen;
- Gebruik een malwarescanner welke **geen verbinding met internet** nodig heeft om op te kunnen starten (bijvoorbeeld i.v.m. licentie controle);
- Gebruik een USB stick waar de antimalware software als een **portable applicatie** op kan worden geïnstalleerd;
- 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;
- 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 systeemdokumentatie;
- 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 systeemdokumentatie

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

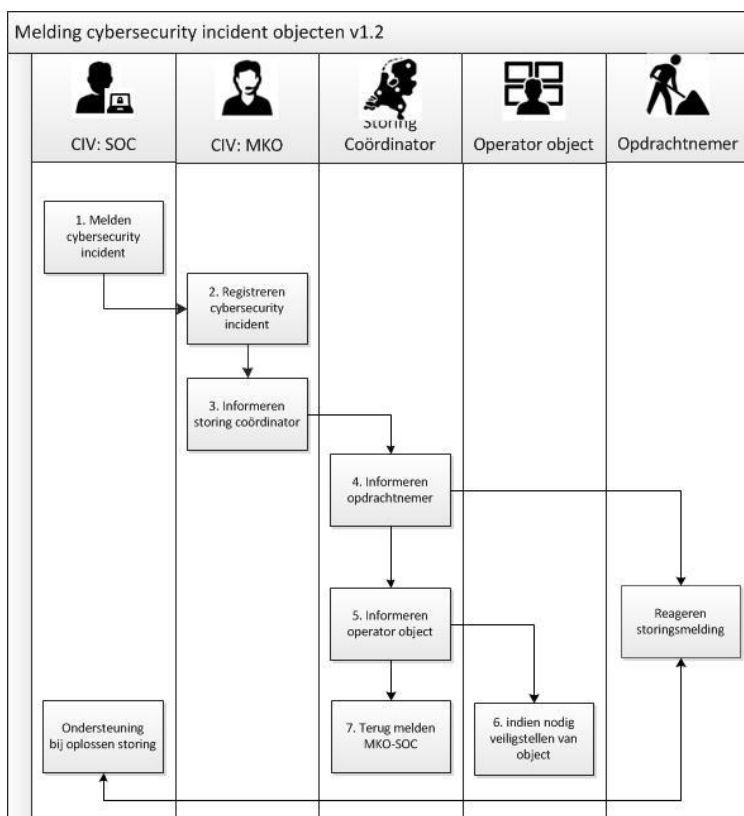
Het Security Operations Centre (hierna SOC) van Rijkswaterstaat ontwikkelt als één van haar diensten het monitoren van (loggings van) systemen en netwerkomgevingen van Rijkswaterstaat. Technische maatregelen worden ingevoerd om het ontsluiten en monitoren van (loggings op) regionale systemen en netwerkomgevingen 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 storingsmeldingen 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 (netwerknnaam) 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 informeren 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 informeren 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 informeren 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 treedt 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 voortvloeien 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 optreedt 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 bedeeft 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

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.

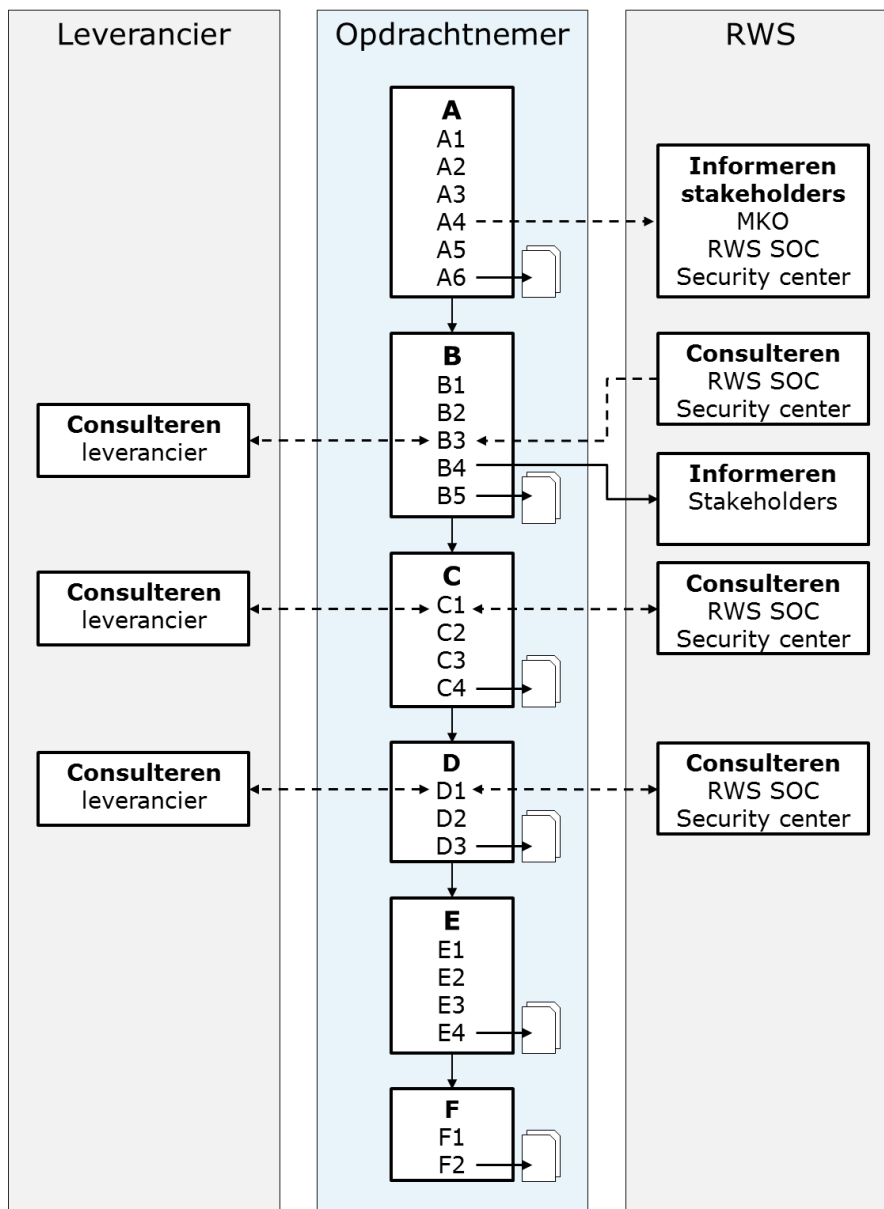
CSR 14.2.5.6 Rapporteren

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 bedeed krijgen. Werknemers van zowel Opdrachtnemer als RWS kunnen deelnemer zijn in de recovery organisatie.

Met betrekking tot het recoveryteam geldt het volgende:

- Het recoveryteam bestaat uit belangrijke stakeholders binnen de organisatie;
- De stakeholders kennen en steunen het recoveryplan;
- 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;
- Het recoveryplan kan alleen door daartoe bevoegde personen uit de recovery organisatie worden geactiveerd;
- Communicatie binnen het team vindt plaats via (waar relevant) Atex-proof portofoons en waar nodig voor gegevensuitwisseling, via email;
- Elke deelnemer in het recoveryteam heeft een kaart met essentiële contactinformatie van het team en draagt deze bij zich;
- Elke deelnemer in het recoveryteam bewaart een papieren kopie van het recoveryplan thuis op een veilige plaats;
- 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:

- Geïnstalleerde hardware, inclusief firmware en configuraties;
- Geïnstalleerde Operating Systems en software, inclusief configuraties;
- Actuele back-ups van de systemen;
- Netwerk configuratie, inclusief gebruikte communicatiemiddelen;
- Documentatie (online en offline);
- Recoveryorganisatie en communicatieplan;
- Recoverymiddelen en werkprocedures;
- Testprocedures;
- 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. netwerkkaparaatuur;
- 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 netwerkkaparaatuur

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.

Nr.	Activiteit	Omschrijving
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 een *Data model CMDB Cybersecurity Industriële Automatisering* is het vastleggen van heldere en eenduidige afspraken over de gegevensvastlegging en de uitwisseling ervan. In een (conceptueel/logisch) datamodel wordt vastgelegd over welke dingen we een administratie bijhouden: de entiteitentypes/Asset-types. Daarbij beschrijft dit model wat we hierover vastleggen: attribuuttypes en relatietypes.

Aanvullend op dit model wordt het *CMDB Cybersecurity Industriële Automatisering Excel Format* beschikbaar gesteld. Deze bevat aanwijzingen en templates om de gegevens in het voor u liggende model aan te leveren.

CSR 16.1.1 Scope

Het Data model CMDB Cybersecurity Industriële Automatisering kan worden gezien als een gedetailleerde beschrijving van de informatiebehoefte van de objecteigenaren in het kader van assetmanagement en het Security Operation Center (SOC). Het model stelt wel eisen aan de database(s) waarin de betreffende Asset-types worden vastgelegd maar bepaalt niet in welke database(s) dit zou moeten gebeuren.

In dit model worden per Asset-type de verplicht in te vullen velden beschreven. Waar de velden optioneel zijn, wordt dit expliciet aangegeven. Voor ieder veld geldt, dat deze verplicht moet worden ingevuld tenzij wordt vermeld dat het veld optioneel is.

CSR 16.1.2 Disclaimer

Het opslaan en beheren van documenten, behoort niet tot de scope van het *Data model CMDB Cybersecurity Industriële Automatisering*. Echter, voor vier Asset-types beschreven in dit model (Beheer en onderhoudsdocumentatie, Data- communicatienetwerkontwerp, Programmatuurbeschrijving en Wijzigingendocument) geldt wel dat deze naar documentatie verwijzen. De attribuuttypes betreffen dus specifieke metadata bij deze documentatie die voor Cybersecurity van belang is.

Voldoen aan de eisen van dit model betekent nog niet dat voor de betreffende documentatie aan alle wettelijke eisen m.b.t. de metadata voor documentatie is voldaan.

Dit model maakt waar mogelijk gebruik van standaarden zoals de Rijkswaterstaat Objecttypenbibliotheek (OTL), DISK en de NEN.

CSR 16.1.3 Beheer en Eigenaarschap

Het model wordt beheerd door het IV Configuratie Management Overleg (ICMO). Wijzigingen die betrekking hebben op de datamodelering 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 16.1.4 Wijzigingsverzoeken

Het Data model CMDB Cybersecurity Industriële Automatisering bevat een overzicht van nu bij Rijkswaterstaat bekende, voor Cybersecurity relevante, Asset-types en attribuuttypes. 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.

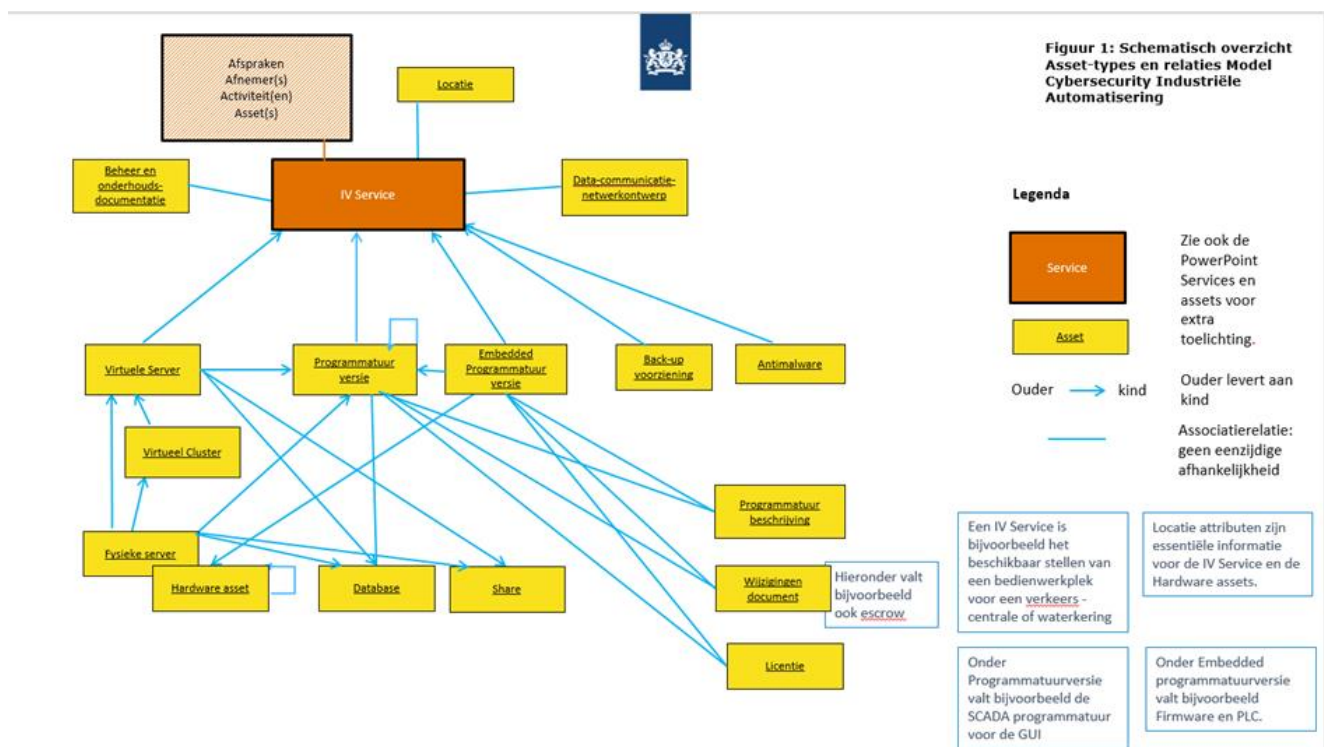
Wanneer er een wijzigingen van het datamodel nodig is (bijvoorbeeld de toevoeging of verwijdering van een Asset-type), wordt deze wijziging voorgelegd aan de contactpersoon bij RWS en pas na schriftelijke goedkeuring door de aangewezen contactpersoon bij RWS doorgevoerd in de templates. Daarbij levert de opdrachtnemer een beschrijving van de betreffende wijziging zodat deze ook kan worden doorgevoerd in het Data model CMDB Cybersecurity Industriële Automatisering. Indien de wijziging toch vragen oproept bij relevante RWS medewerkers, wordt de wijziging toegelicht en zo nodig aangepast totdat deze door de betreffende RWS als begrijpelijk wordt ervaren.

CSR 16.1.5 Toekomst

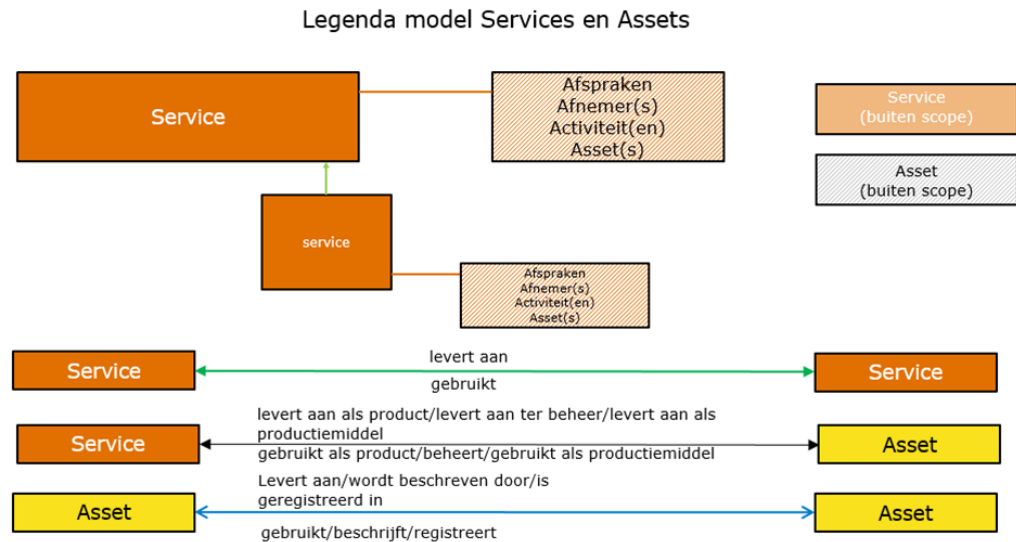
Dit model is een éérste stap en zal met nieuwe kennis worden bijgewerkt.

CSR 16.1.6 Leeswijzer

Paragraaf CSR 16.2 geeft een overzicht van de Asset-types en Relatietypes van het *Data model CMDB Cybersecurity Industriële Automatisering*. Paragraaf CSR 16.2.1 start met het schematisch overzicht. Begrippen uit dit overzicht worden daaropvolgend toegelicht in de paragraaf 16.2.2 *Samenvatting Metamodel Services, Assets en Relaties*. In paragraaf 16.2.3 volgt een beschrijving van de Asset-types en Relatietypes. Deze start met overzichten van de Assettypes (paragraaf 16.2.3.1) en de Relatietypes (paragraaf 16.2.3.2). Tot slot is voor alle Asset-types is een korte definitie opgesteld en worden de attribuuttypes beschreven. Dit is beschreven in de paragraaf Asset-types uitgelicht (deel 16.2.3.3).

CSR 16.2 Overzicht Asset-types en Relatietypes**CSR 16.2.1 Schematisch overzicht**

CSR 16.2.2 Samenvatting Metamodel Services, Assets en Relaties



Service: een afgebakende prestatie van een persoon of organisatie, die voorziet in een behoefte van haar afnemers.

- Een service levert meestal één of meerdere assets als producten of beheert één of meerdere assets als beheerde objecten.
- Een service kan samengesteld zijn.
- Als een service een product levert, is het gespecificeerd welk product of producten het zijn en onder welke condities ze geleverd worden.
- Als een service een asset beheert, is het gespecificeerd welk asset of assets het zijn en onder welke condities ze worden beheerd. Denk bijvoorbeeld aan service levels.

Voorbeeld: beschikbaar stellen Bedienwerkplek

Voorbeeld: beschikbaar stellen transformatie door Noodsluit startautomaat

Asset: iets wat waarde vertegenwoordigd

- Een asset kan verschillende rollen vervullen afhankelijk van het gezichtspunt:
- Een asset kan een product zijn. Deze wordt dan geleverd aan derden voor gebruik of afgeleverd, om te behouden (verbruik).
- Een asset kan een productiemiddel zijn en wordt dan gebruikt door de dienstverlener.
- Een asset kan een beheerd object zijn.

In het *Data model CMDB Cybersecurity Industriële Automatisering* worden twee soorten relaties beschreven:

1. Relaties waarbij geen eenzijdige afhankelijkheid geldt: **Associatierelaties**.

2. Relaties met een **levert aan-gebruikt/Ouder-Kind relatie**

In de huidige CMDB van RWS vastgelegd als een levert aan/Ouder-Kind relatie waarbij de Ouder levert aan het Kind. Deze relatie kent 1 richting: van Ouder naar Kind.

Waarbij de pijl van de Ouder richting het Kind gaat.

Indien van toepassing, moeten de relaties worden vastgelegd als levert aan-gebruikt/Ouder-Kind relaties. Dit omdat juist het in beeld krijgen van de afhankelijkheden tussen assets en services één van de belangrijkste doelen is van dit model.

Aanvullende opmerkingen:

De in een Service Management Database en/of CMDB geregistreerde service, betreft altijd een instantie van de service:

een specifieke service die aan een specifieke afnemer/klant wordt geleverd. De omschrijving van de Service, die vele instanties kan hebben, word vastgelegd in de Servicecatalogus.

Het in de CMDB geregistreerde asset, betreft altijd een instantie van het entiteitstype/assettype die een rol heeft in de instantie van één of meerdere service(s).

De omschrijving van het assettype, dat dus vele instanties kan hebben, wordt vastgelegd in het Conceptueel Datamodel Configuratie management waarvan het *Data model CMDB Cybersecurity Industriële Automatisering* een deelmodel is.

CSR 16.2.3 Beschrijving Asset-types en Relatietypes

CSR 16.2.3.1 Overzicht Asset-types

Model	Asset-type
<i>Data model CMDB Cybersecurity Industriële Automatisering</i>	Antimalware
<i>Data model CMDB Cybersecurity Industriële Automatisering</i>	Back-up voorziening
<i>Data model CMDB Cybersecurity Industriële Automatisering</i>	Beheer en onderhouds-documentatie
<i>Data model CMDB Cybersecurity Industriële Automatisering</i>	Data-communicatie-netwerkontwerp
<i>Model Infra en Hardware KA</i>	Database
<i>Model Infra en Hardware KA</i>	Embedded
<i>Model Infra en Hardware KA</i>	Programmatuurversie
<i>Model Infra en Hardware KA</i>	Fysieke Server
<i>Model Infra en Hardware KA</i>	Hardware asset
<i>Model Generieke Entiteitstypes</i>	IV Service
<i>Model Infra en Hardware KA</i>	Share
<i>Model Generieke Entiteitstypes</i>	Locatie
<i>Model Programmatuur</i>	Licentie
<i>Data model CMDB Cybersecurity Industriële Automatisering</i>	Programmatuur beschrijving
<i>Model Programmatuur</i>	Programmatuurversie
<i>Model Infra en Hardware KA</i>	Virtueel Cluster
<i>Model Infra en Hardware KA</i>	Virtuele server
<i>Data model CMDB Cybersecurity Industriële Automatisering</i>	Wijzigingen document (Escrow)

CSR 16.2.3.2 Overzicht Relatie types

Relatietype	Assettype/Service-type-1	Is ouder van/levert aan	Assettype/service-type-2
Ouder-Kind (Parent-Child) relatie	Virtuele Server		IV Service
	Virtuele Server		Programmatuur versie
	Virtuele Server		Database
	Virtuele Server		Share
	Programmatuur versie		IV Service
	Embedded Programmatuur versie		IV Service
	Back-up voorziening		IV Service
	Antimalware		IV Service
	Programmatuurversie		Programmatuurversie
	Fysieke server (Hardware asset)		Programmatuurversie
	Fysieke server (Hardware asset)		Database
	Fysieke server (Hardware asset)		Share
	Fysieke server (Hardware asset)		Virtueel Cluster
	Fysieke server (Hardware asset)		Virtuele Server
	Virtueel Cluster		Virtuele Server
	Embedded Programmatuur versie		Programmatuur versie
	Embedded Programmatuur versie		Hardware asset
	Hardware asset		Connection Type
	Netwerkkomponent (Hardware asset)		Connection Type
	Connection Type		Hardware assets (Fysieke serverpoort)
	Hardware asset		Hardware asset
	Zie voor de verdere mogelijke relaties van Hardware assets het model Infra & Hardware KA		

Assettypes met associatiere relaties

Relatietype	Assettype/Service-type 1	Is verbonden met	Assettype/Service-type 2
Associatiere relatie	Beheer en onderhoudsdocumentatie		IV Service
	Data-communicatie-netwerkontwerp		IV Service
	Locatie		IV Service
	Let op: locatiegegevens worden voorlopig als attribuuttypes bij IV Service geregistreerd		
	Programmatuurversie		Database
	Locatie		Hardware asset
	Let op: locatiegegevens worden voorlopig als attribuuttypes bij assets geregistreerd		
	Programmatuur beschrijving		Programmatuur versie
	Programmatuur beschrijving		Embedded Programmatuur versie

Assettypes met associatierelaties			
	Wijzigingen document (Escrow)		Programmatuur versie
	Wijzigingen document (Escrow)		Embedded Programmatuur versie
	Licentie		Programmatuur versie
	Licentie		Embedded Programmatuur versie

CSR 16.2.3.3 Asset-types uitgewerkt

Hieronder volgt een gedetailleerde uitwerking van de in paragraaf 1.2 beschreven Asset-types.

Antimalware Asset-type

Product met functionaliteit voor bescherming tegen alle vormen van Malicious software.

Bron: RWS CSIR

Attribuut	Definitie	Schrijfwijze
Object ID		Invullen door RWS
Bron ID		Unieke ID (Uniek ID zoals geregistreerd bij opdrachtnemer)
Status Programmatuur versie		Keuzeveld: Ge-Deïnstalleerd Geïnstalleerd Niet geïnstalleerd Ontwikkelen
Versie	Een specifieke variatie of verdere ontwikkeling van een origineel product	Zonder voorloop-V, nummers gescheiden door punten.
Merk	Uit het Model Infra & Hardware KA: De handelsnaam, waaronder een producent een productrange op de markt plaatst.	
Producent	Overkoepelende naam, waaronder de 'Producent' zijn producten verkoopt.	
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.	Naam van de programmatuur zoals uitgegeven door de producent
Ordernummer vendor		
Taal	Taalcode van de software conform ISO-693-3	Taalcode van de software conform ISO-693-3
Maatwerktype	In hoeverre er hier sprake is van maatwerk en welk type maatwerk het betreft.	keuzelijst: COTS, MOTS (modified of the shelf), maatwerk

A/B/C klassificatie	[A] Applicaties die standaard worden geleverd op de standaard Werkstation. [B] Applicaties die optioneel door iedere Werkplekgebruiker kunnen worden aangevraagd. [C] Overig. Vastgesteld door RWS-bestuur.	[A] Applicaties die standaard worden geleverd op de standaard Werkstation. [B] Applicaties die optioneel door iedere Werkplekgebruiker kunnen worden aangevraagd. [C] Overig.
Vestiging		Vestigingen opzoeken in dropdownlijst in Topdesk Indien van toepassing Let op: vaak niet beschikbaar voor opdrachtnemer dan als alternatief de adresgegevens invullen. Zie Excel
Overige plaatsbepaling zoals kamernummer		
GPS Location Latitude		
GPS Location Longitude		
RD X- coördinaat		
RD Y- coördinaat		

Back-up voorziening Asset-type

Product dat de functionaliteit biedt om een kopie te maken van de programmatuur. Het betreft hier twee eisen:

1. Er moet periodiek een back-up worden gemaakt.
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 ook worden vastgelegd.

Bron: RWS CSIR

Attribuut	Definitie	Schrijfwijze
Object ID		Invullen door RWS
Bron ID		Unieke ID (Uniek ID zoals geregistreerd bij opdrachtnemer)
Locatie laatste Back-up	Fysiek adres	
Datum laatste Back-up		d-m-jyyy (let op: streepjes noodzakelijk)
Datum laatste recovery test		d-m-jyyy (let op: streepjes noodzakelijk)
Recovery succesvol?		Ja/nee
Producent	Overkoepelende naam, waaronder de 'Producent' zijn producten verkoopt.	
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.	Naam van de programmatuur zoals uitgegeven door de producent

Beheer en onderhoudsdocumentatie Asset-type

Documentatie waarin met betrekking tot het betreffende Asset het volgende wordt vastgelegd :

- beheer en onderhoudsinstructies;
- vervangingsinstructies;
- handleiding CS R16 Configuratie item/Asset;
- verantwoordelijken voor het onderhoud;
- status onderhoud.
- Patch procedure

Bron: RWS CSIR

Gedocumenteerde informatie: informatie die een organisatie (2.57) moet beheren en onderhouden en het medium waarop deze informatie is vastgelegd.

Bron: NEN-ISO/IEC 27001 (nl) Informatietechnologie - Beveiligingstechnieken - Managementsystemen voor informatiebeveiliging - Eisen (ISO/IEC 27001:2017 en, IDT)

Attribuut	Definitie	Schrijfwijze
Object ID		Invullen door RWS
Bron ID		(Uniek ID zoals geregistreerd bij opdrachtnemer)
Plaats	Waar kan de beheerdocumentatie worden gevonden?	Dit kan zowel een digitaal als fysiek adres zijn. Zo specifiek mogelijk dus indien van toepassing ook kamernummer en kast vermelden.
Datum laatst gewijzigd		d-m-jjjj (let op: streepjes noodzakelijk)
Verantwoordelijk		Naam, organisatie en contactgegevens van de persoon die verantwoordelijk is voor de beheer en onderhoudsdocumentatie.
Beheer en onderhouds-documentatie Gewijzigd door?		Naam, organisatie en contactgegevens van de persoon die de laatste wijziging van de beheer en onderhoudsdocumentatie heeft doorgevoerd.
beheer en onderhouds-instructies aanwezig?		beheer en onderhoudsinstructies: ja/nee
Vervangings-instructies aanwezig?		Vervangingsinstructies: ja/nee
handleiding CS R16 Configuratie item/Asset aanwezig?		handleiding CS R16 Configuratie item: ja/nee
verantwoordelijken voor het onderhoud aanwezig?		verantwoordelijken voor het onderhoud: ja/nee
status onderhoud bekend?		status onderhoud bekend: ja/nee
Patch procedure aanwezig?	Beschrijft de werkwijze voor het implementeren of doorvoeren van een Patch	Patch procedure: ja/nee

Data-communicatienetwerkontwerp Asset-type

Een datacommunicatienetwerk is een netwerk voor data-overdracht tussen twee of meer apparaten. De apparaten kunnen telefoons, modems, Switches, Routers, computers of onderdelen ervan zijn, maar evengoed bijvoorbeeld ook weerstations, printers, stuursystemen, mobiele telefoons, enz. De structuur waarin de apparaten door middel van het netwerk gekoppeld zijn, wordt de netwerktopologie genoemd. (Bron:

<https://nl.wikipedia.org/wiki/Datacommunicatienetwerk>)

Het Data-communicatie-netwerk-ontwerp betreft de documentatie waarin met betrekking tot het betreffende CS Configuratie Item het volgende wordt vastgelegd :

- Fysieke topologie;
- Logische topologie;
- IP-plan; Zie de minimumeisen in de bijlage IP Plan.

Bron: RWS CSIR

Attribuut	Definitie	Schrijfwijze
Object ID		Invullen door RWS
Bron ID		(Uniek ID zoals geregistreerd bij opdrachtnemer)
Plaats	Waar kan de beheerdocumentatie worden gevonden?	Dit kan zowel een digitaal als fysiek adres zijn. Zo specifiek mogelijk dus indien van toepassing ook kamernummer en kast vermelden.
Datum laatst gewijzigd		d-m-jjjj (let op: streepjes noodzakelijk)
Verantwoordelijk		Naam, organisatie en contactgegevens van de persoon die verantwoordelijk is voor het Data-communicatie-netwerk-ontwerp.
Het Data-communicatie-netwerk-ontwerp gewijzigd door?		Naam, organisatie en contactgegevens van de persoon die de laatste wijziging van het Data-communicatie-netwerk-ontwerp heeft doorgevoerd.
Netwerkprotocol beschrijving aanwezig?	Een set van regels en afspraken voor de representatie van data, signalering, authenticatie en foutdetectie, nodig voor het verzenden van informatie over een communicatiemedium.	Netwerkprotocolbeschrijving: ja/nee
Fysieke topologie aanwezig?	Fysieke topologie verwijst naar het fysieke ontwerp van het netwerk. Het samenhangend geheel van elementen (o.a. routers, switches, koperdragers en glasvezels) waarover gegevens elektronische worden getransporteerd. (Bron: gebaseerd op definitie fysiek netwerk in Architectuur Netwerken en Telefonie RWS 2008-2014)	Fysieke topologie: ja/nee

Logisch topologie aanwezig?	Logische topologie verwijst naar hoe gegevens daadwerkelijk wordt overgedragen in een netwerk onafhankelijk van het fysieke ontwerp. (Bron: http://www.eecho-webdesign.com/computer-internet-technologie/network-topology/) Een voorbeeld van een logisch netwerk is het Virtual Private Network (VPN).	Logisch topologie: ja/nee
IP-plan van datacommunicatie-netwerk aanwezig?	Voor beoogde inhoud IP plan, zie de bijlage IP plan	IP-plan aanwezig: ja/nee
DNS	Domein Naam System:	

Data opslag

Onder het deelmodel Dataopslag worden de datadragers 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. (bron: Database - Wikipedia)
- Share
 - o 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. (bron: File share - Wikipedia)

We onderkennen de volgende typen Share:

- i. NFS
 - 1. 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
 - 1. wordt gebruikt voor het delen van linux-bestanden met Windows-netwerk ... \. De server wordt geconfigureerd om bestanden te delen met elke client op het netwerk zonder om een wachtwoord te vragen.

Database Asset-type

Veld	Soort veld	Waarde / naamgeving-conventie	Automatische sync?
Asset ID	Open veld	<i>Database naam</i>	Nvt (statisch)

Bron-ID (A/S-Nummer/ Leveranciers ID/Producent ID)	Open veld		
Soort	Vaste waarde	Database	Nvt (statisch)
Status	Vaste keuzes	Actief Inactief	Nee
Merk	Vaste keuzes		
Type database	Vaste keuzes	MsSQL Oracle Postgres	Nee
Specificatie (<i>optioneel</i>)	Open veld		Nee
Productdomein	Vaste keuzes	IRN BV Ontwikkeling en Services IRN IV Infrastructuur IRN IV Platformen OSR A en O Services OSR SVM Services OSR VM Services OSR WM Services	Nvt (statisch)
Aanspreekpunt	Vaste keuzes		Nee
DBMS versie	Vaste-keuzes		Nee
OTAP-omgeving	Vaste keuzes		Nee
Capaciteit (GB)	Open veld		Nee
LCM Afvoerdatum	Datumveld		Nee
Inventarisatiedatum	Datumveld		Nee

Share Asset-type

Veld	Soort veld	Waarde / naamgeving-conventie	Automatische sync?
Asset ID	Open veld	SHARE-000000	Nvt (statisch)
Bron-ID (A/S-Nummer/ Leveranciers ID/Producent ID)	Open veld		
Soort	Vaste waarde	Share	Nvt (statisch)
Type Share	Vaste keuzes	NFS Samba SMB	Nee
Status	Vaste keuzes	Actief Inactief	Nee
Specificatie (<i>optioneel</i>)	Open veld		Nee
Serienummer	Open veld	Share naam-kort	Nee
Aanspreekpunt	Vaste keuzes	<i>TAB-team</i>	Nee
Eigendom	Vaste keuzes	N.v.t.	Nee
Eigenaarschap		e-mail adres verantwoordelijke Service Delivery Manager (SDM-er)	
Notities	Open veld	Share naam-lang	
Productdomein	Vaste keuzes	IRN BV Ontwikkeling en Services IRN IV Infrastructuur IRN IV Platformen OSR A en O Services OSR SVM Services	Nee

		OSR VM Services OSR WM Services	
OTAP omgeving	Vaste keuzes		Nee
Capaciteit (GB)	Open veld		Nee
LCM Afvoerdatum	Datumveld		Nee
Inventarisatiedatum	Datumveld		Nee

Embedded Programmatuurversie Assettype

Embedded software is computer software, written to control machines or devices that are not typically thought of as computers, commonly known as embedded systems. It is typically specialized for the particular hardware that it runs on and has time and memory constraints. Embedded programmatuur is computerprogrammatuur die is geschreven om hardware en machines te sturen die niet vallen onder wat we in het dagelijkse spraakgebruik zien als computers.

Bron: https://en.wikipedia.org/wiki/Embedded_software

Onder Embedded programmatuurversie valt bijvoorbeeld Firmware en PROGRAMMABLE LOGIC CONTROLLER (PLC).

Voor de meest actuele versie en meer informatie over de soorten/Asset-types die onder Hardware vallen (bijvoorbeeld de definities e.d.): raadpleeg het model Infra & Hardware- KA, deze zal op aanvraag beschikbaar worden gesteld.

Attribuut	Definitie	Schrijfwijze
Object ID		Invullen door RWS
Bron ID		(Uniek ID zoals geregistreerd bij opdrachtnemer)
Soort		Keuzeveld: Firmware Overig
Status Programmatuur versie		Keuzeveld: Ge-Deïnstalleerd Geïnstalleerd Niet geïnstalleerd Ontwikkelen
Versie	Een specifieke variatie of verdere ontwikkeling van een origineel product	Zonder voorloop-V, nummers gescheiden door punten.
Merk	Uit het Model Infra & Hardware KA: De handelsnaam, waaronder een producent een productrange op de markt plaatst.	
Hostnaam		
Mac-adres		
IP-adres		
Taal	Taalcode van de software conform ISO-693-3	Taalcode van de software conform ISO-693-3
Maatwerktype	In hoeverre er hier sprake is van maatwerk en welk type maatwerk het betreft.	In hoeverre er hier sprake is van maatwerk en welk type maatwerk het betreft.
Aanschafprijs		
Sap referentie		
Aanspreekpunt invullen afhankelijk van contractuele afspraken: RWS of Opdrachtnemer		
Leverancier	optioneel	
Aanschafdatum		d-m-jjjj (let op: streepjes noodzakelijk)
Installatie Datum		d-m-jjjj (let op: streepjes noodzakelijk)

EOL-End of Life datum d-m-jjjj (let op: streepjes noodzakelijk)		
EOS-End of Support datum d-m-jjjj (let op: streepjes noodzakelijk)		
Vestiging		Vestigingen opzoeken in dropdownlijst in Topdesk Indien van toepassing Let op: vaak niet beschikbaar voor opdrachtnemer dan als alternatief de adresgegevens invullen. Zie Excel
Overige plaatsbepaling zoals kamernummer		<i>Indien van toepassing</i>
GPS Location Latitude		<i>Indien van toepassing</i>
GPS Location Longitude		<i>Indien van toepassing</i>
RD X- coördinaat		<i>Indien van toepassing</i>
RD Y- coördinaat		<i>Indien van toepassing</i>
Rack (kastnummer)		<i>Indien van toepassing</i>
Rack (kasthoogte)		<i>Indien van toepassing</i>

Fysieke server Assettype

Computer die centraal taken afhandelt voor een of meer clients. De computer kan in verschillende gedaantes voorkomen: Blade, Rack mounted en Desktop.

We kennen verschillende typen servers:

- **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. Bron: RWS Datamodel ServiceNow versie 1.4
- **Secure Network Server:** een Secure Network Server is een systeem dat zorgt voor geautoriseerde toegang tot verschillende netwerksystemen en applicaties. Bron: RWS Datamodel ServiceNow versie 1.4
- **Blade server:** Een 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. RWS Datamodel ServiceNow versie 1.4
- **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. RWS Datamodel ServiceNow versie 1.4
- **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. WS Datamodel ServiceNow versie 1.4.

- **ESX-Host:** Fysieke server waarop virtuele servers worden gedeployed.

Aandachtspunt: verschillende typen servers kunnen verschillende relaties hebben. Voorlopig worden ze beschouwd als verschillende Assettypes. Als vervolgstap op het model Infra en Hardware-ka versie 2.0 zal worden onderzocht in hoeverre een opschoning mogelijk is. In zijn algemeenheid geldt dat voor alle genoemde typen Server de onderstaande tabel geldt. Met als enige afwijking dat er (voorlopig nog) verschillende soortnamen en andere prefixen gelden voor de verschillende typen Servers.

Voor de meest actuele versie en meer informatie over de soorten/Asset-types die onder Hardware vallen (bijvoorbeeld de definities e.d.): raadpleeg het model Infra & Hardware- KA, deze zal op aanvraag beschikbaar worden gesteld.

Type Server	Prefix voor Object ID	Soortnaam
Network DNS	SRVN-*	Network DNS
Secure Network Server	SRVS-*	Secure Network Server
Blade server	SRVB-*	Blade server
PC server	SRVP-*	PC server
Server	SRV-*	Server

Algemene tabel voor Server:

Veld	Soort veld	Waarde / naamgevingconventie
Object ID	Open veld	Invullen door RWS
Bron ID		Uniek ID zoals geregistreerd bij opdrachtnemer
Zonering		Invullen door RWS https://www.noraonline.nl/wiki/Beschouwingsmodel_zonering
MKS		Invullen door RWS
Merk	Vaste keuzes	
Type	Vaste keuzes	
Specificatie (optioneel)	Open veld	
Serienummer	Open veld	
Aanspreekpunt	Vaste keuzes	<i>Beschikbaarheid Topdesk</i>
Leverancier (optioneel)	Vaste keuzes	<i>Beschikbaarheid Topdesk</i>
Aanschafdatum	Datum veld	d-m-jyyy (let op: streepjes noodzakelijk)
Installatiedatum	Datum veld	d-m-jyyy (let op: streepjes noodzakelijk)
EOL-End of Life datum	Datum veld	d-m-jyyy (let op: streepjes noodzakelijk)
EOS-End of Support datum	Datum veld	d-m-jyyy (let op: streepjes noodzakelijk)
Status	Vaste keuzes	Voorraad Gereserveerd Actief Tijdelijke opslag Vermist Onderhoud

		Af te voeren Uit beheer Gedeactiveerd
Plaatskoppeling (<i>optioneel</i>)	Opzoekveld	Dropdownlijst (optioneel: indien beschikbaar gesteld door RWS)
Hostnaam	Open veld	
IP-adres	Open veld	
Beoogd gebruik	Vaste keuzes	Invullen door RWS Keuze mogelijkheden: - <u>Standaard</u> : ➔ extra keuzeveld: KA-vrij Niet-vrij. - <u>Productie</u> : Extra vrije tekstveld: waarin gegevens voor een koppeling naar de Services en een nadere sub verdeling over gebruik en/of applicatie kan worden in gevuld.
Eigenaarschap (Service Delivery Manager)	Opzoekveld	(service Delivery Manager) invullen door RWS dynamische dropdownlijst die refereert aan de persoonstabeltabel.
IP-adres (<i>optioneel</i>)	Open veld	
Hostnaam	Open veld	
IP Adres iLO (<i>Optioneel</i>)	Open veld	
OS Beheerder	Vaste keuzes	<i>invullen afhankelijk van contractuele afspraken:</i>
Operating System	Vaste keuzes	
SAP Referentie	Open veld	
Projectnummer	Open veld	
Aanschafprijs	Open veld	
Aantekeningen	Open veld	
Vestiging	Opzoekveld	Vestigingen opzoeken in dropdownlijst in Topdesk Indien van toepassing Let op: vaak niet beschikbaar voor opdrachtnemer dan als alternatief de adresgegevens invullen. Zie Excel
Overige plaatsbepaling zoals kamernummer	Opzoekveld	Locatie opzoeken in dropdownlijst met locaties in Topdesk Indien van toepassing
GPS Location Latitude	nummeriek	Indien van toepassing
GPS Location Longitude	nummeriek	Indien van toepassing
RD X-coördinaat	tekst	Indien van toepassing
RD Y-coördinaat	tekst	Indien van toepassing
Rack		

kast(nummer)		
Rack		
Kast(hoogte)		

Hardware Asset-type

Hieronder volgt een overzicht van de attribuuttypes die in zijn algemeenheid gelden voor Hardware assets.

Voor de meest actuele versie en meer informatie over de soorten/Asset-types die onder Hardware vallen (bijvoorbeeld de definities e.d.): raadpleeg het model Infra & Hardware- KA, deze zal op aanvraag beschikbaar worden gesteld. De inhoud is reeds opgenomen in de bijgeleverde CMDB Cybersecurity Industriële Automatisering Excel Format.

Object ID:	Unieke identificatiecode van het asset in de CMDB van Topdesk
Bron ID	Unieke identificatiecode van het asset in de brondatabase.
Zonering	Bijvoorbeeld van de opdrachtnemer of de regionale dienst. Alleen van toepassing op de Fysieke en Virtuele server. Invullen door RWS, zie: https://www.noraonline.nl/wiki/Beschouwingsmodel_zonering
Soort:	Functionaliteit van het item / Assettype. Zie voor de types het Tabblad Model Infra en Hardware KA in de bijgeleverde CMDB Cybersecurity Industriële Automatisering Excel Format.
Merk:	Merk van het betreffende item
Type:	Typebeschrijving die volgens de producent wordt gehanteerd.
Specificatie:	Open veld waar extra informatie over het item.
Serienummer:	Serienummer van het betreffende item. Vaak te achterhalen op de kast van het apparaat.
Aanspreekpunt:	Verantwoordelijke beheergroep (dropdownlijst behandelaarsgroep in Topdesk)
Leverancier:	Leverende partij, doorgaans een externe partij.
Aanschafdatum:	Leverdatum van het item. Datum staat op de pakbon genoteerd welke bij de levering wordt meegestuurd.
Installatie Datum:	
EOL End of life datum	Wordt gecommuniceerd door de leverancier,
EOS-End of support datum	Wordt gecommuniceerd door de leverancier, is een waarschuwing voor de EOL (zie boven). De leverancier biedt geen ondersteuning meer voor het betreffende item.
Status:	Geeft aan in welke toestand het item zich bevindt.
<i>Voorraad</i>	Item is beschikbaar voor inzet en bevindt zich doorgaans in een (de)centrale voorraad ruimte of magazijn.
<i>Actief</i>	Item is ingezet in de operatie en is onderdeel van de operationele keten.
<i>Tijdelijke opslag</i>	Item is tijdens een verbouwing of verhuizing van een kantoor tijdelijk opgeslagen.
<i>Vermist</i>	Item bevindt zich niet op de aangegeven locatie en is ook niet meer traceerbaar.
<i>Onderhoud</i>	Er wordt onderhoud gepleegd op het item. Status onderhoud is ook toepasbaar bij reparatie.
<i>Af te voeren</i>	Item is "End of Life" en kan daarom worden afgevoerd. De status is ook toepasbaar indien het item niet meer kan worden gerepareerd.
<i>Uit beheer</i>	Item is actief en aangesloten aan het netwerk maar wordt niet beheerd. Dit aangezien het item op dat moment geen deel uitmaakt van een dienst.
<i>Gedeactiveerd</i>	Item staat niet op voorraad, bevindt zich doorgaans in een server rack en kan aangesloten zijn met netwerkkabels en netsnoer. Het items is echter niet ingeschakeld en is dus gedeactiveerd.

<i>Gereserveerd</i>	Betreffende hardware is al ingericht voor een specifieke aanvrager maar nog niet in gebruik (het betreft meestal laptops)
Hostnaam:	Betreft de FQDN, het unieke adres van een computer op het RWS netwerk in de vorm van letters.
IP-adres:	Het unieke adres van een computer op het RWS netwerk in de vorm van cijfers. Dit betreft het zogenaamde Productie IP-adres waaraan ook de Hostnaam (FQDN) is gekoppeld.
Beoogd gebruik:	Geeft de beoogde gebruiksvorm aan van het item: Keuze mogelijkheden: - <u>Standaard</u>: Bij de keuze van "Standaard" hoort een extra keuze (veld) met de waarden "KA-vrij" en "Niet-vrij". - <u>Productie</u>: Bij de keuze Productie hoort de mogelijkheid voor vrije tekst (een extra vrijetekst veld) waarin gegevens voor een koppeling naar de Services en een nadere sub verdeling over gebruik en/of applicatie kan worden ingevuld.

Toelichting begrippen Standaard en Productie:

'Standaard'

Definitie *'Geautomatiseerde werkplek zoals die aan iedere medewerker van Rijkswaterstaat beschikbaar wordt gesteld. Deze werkplek wordt gedefinieerd volgens de standaarden en requirements van KA-services.'*

'Productie'

Definitie *'Geautomatiseerde werkplek met afwijkende standaarden en/of requirements ten opzichte van de standaarden en requirements zoals die door KA-services zijn gedefinieerd voor de Standaard werkplek.'*

Eigenaarschap (Service Delivery Manager): dynamische dropdownlijst die refereert aan de persoonstabeltabel.

OS-beheerder	Beheergroep van de Operating System (Wie voert OS patches uit?)
Operating system	Operating system van de server

SAP Referentie:	Referentie welke ook in het SAP systeem van RWS wordt herkend
Aanschafprijs:	
Projectnummer:	
Levert aan/Ouder-Kind relatie:	Zie de toelichting in hoofdstuk 2
Aantekeningen:	Losse aantekeningen die relevant zijn voor het beheer.
Vestiging	Indien van toepassing: Vestigingen opzoeken in dropdownlijst in Topdesk
Overige plaatsbepaling zoals kamernummer locaties in Topdesk	Indien van toepassing: Locatie opzoeken in dropdownlijst met
GPS Location Latitude	Indien van toepassing
GPS Location Longitude	Indien van toepassing
RD X- coördinaat	Indien van toepassing
RD Y- coördinaat	Indien van toepassing
Ruimte	Indien van toepassing
Rack (kast) nummer	Indien van toepassing
Rack (kast) hoogte	Indien van toepassing

IV Service

Definitie Service:

Een afgebakende prestatie van een persoon of organisatie, die voorziet in een behoefte van haar afnemers.

Kenmerken:

- Een service levert meestal één of meerdere assets als producten of beheert één of meerdere assets als beheerde objecten.
- Een service kan samengesteld zijn.
- Als een service een product levert, is het gespecificeerd welk product of producten het zijn en onder welke condities ze geleverd worden.
- Als een service een asset beheert, is het gespecificeerd welk asset of assets het zijn en onder welke condities ze worden beheerd. Denk bijvoorbeeld aan service levels.
- Afbakening van de prestatie wordt bepaald door de afspraken met de (interne en/of externe) afnemers, functionele beschrijvingen en andere afspraken over het wat en hoe te leveren of beheren.
- Een service heeft een integrale TCO (Total Costs of Ownership) - alle kosten gerelateerd aan de aanschaf en gebruik gedurende de levenscyclus van ingekochte goederen en diensten. Deze kosten worden vertaald naar kostprijsmodel.

NB: alleen de witte velden dienen door de opdrachtnemer te worden ingevuld.

Veld	Soort veld	Waarde / naamgevingconventie	Topdesk implementatie
Asset ID	tekst	Unieke IDnaam van de Service . Start met een punt. Topdesk accepteert geen dubbelingen Krijgt de naam van de instantie. Bijv:	Omdat dit op de hoofdkaart alleen maar gekoppeld kan worden
Entity ID	Database ID:tekst? Nog uitzoeken	De tool (Topdesk) zelf automatisch een nummer laten aanmaken	
Bron ID (S-nummer/KPN/Expertdesk) invullen afhankelijk van contractuele afspraken: RWS of Opdrachtnemer	tekst	In overleg met RWS eigen Bron ID van de opdrachtnemer of: Productlijn ID (s nummer) Of Expertdesk ID Of KPN ID	
IV Servicegroep/Categorie	Opzoekveld	Keuzewaarden: AOA services BOS services IVP Tooling VM Services	Verplicht in Topdesk

		SVM Services IRI connectivitservices (hieronder valt KPN)	
IV Servicenaam/Subcategorie	tekst		Verplicht in Topdesk
IV Service versie	tekst		
Status IV Service	Opzoekveld	Gepland Verkrijgen of bouwen Ontwikkeling en transitie Geleverd en ondersteund End of Service Statussen conform ITIL	Verplicht in Topdesk
OTAP Omgeving	Opzoekveld	Productie (default) Acceptatie Test Ontwikkeling Training	Verplicht in Topdesk
Servicemanager	Opzoekveld	Dit veld geeft een opzoeklijst met alle in TOPdesk bestaande personen.	verplicht
Service Delivery Manager	idem	Dit veld geeft een opzoeklijst met alle in TOPdesk bestaande personen.	verplicht
Applicatie-Product- Platformmanager invullen afhankelijk van contractuele afspraken: RWS of Opdrachtnemer	idem	Applicatie-Product- Platformmanager of soortgelijke manager op hetzelfde praktische niveau. Dit veld geeft een opzoeklijst met alle in TOPdesk bestaande personen.	verplicht
Functioneel Beheerder invullen afhankelijk van contractuele afspraken: RWS of Opdrachtnemer	idem	Dit veld geeft een opzoeklijst met alle in TOPdesk bestaande personen.	Niet verplicht
Informatiemanager	idem	Dit veld geeft een opzoeklijst met alle in TOPdesk bestaande personen.	Niet verplicht
Externe partij (leverancier en/of beheerder)		Externe partij met wie de CIV direct contact heeft.	
Vestiging	Opzoekveld		Vestigingen opzoeken in dropdownlijst in Topdesk Indien van toepassing

Overige plaatsbepaling zoals kamernummer	Opzoekveld		Locatie opzoeken in dropdownlijst met locaties in Topdesk Indien van toepassing
GPS Location Latitude	nummeriek		Indien van toepassing
GPS Location Longitude	nummeriek		Indien van toepassing
RD X- coördinaat	tekst		Indien van toepassing
RD Y- coördinaat	tekst		Indien van toepassing
Contractsoort Klantcontract		Vaste keuzes (verplicht)	Keuzes: -SLA = afspraak met de eindklant -Niet van toepassing want het betreft een CIV-levering.
Contractsoort Leveranciercontract		Vaste keuzes (verplicht)	OLA = afspraak tussen CIV- afdelingen. Underpinning contract = afspraak tussen CIV afdelingen met leveranciers/externe opdrachtnemers zoals KPN.

Locatie

Definitie locatie

Vanuit het OTL wordt de volgende definitie beschikbaar gesteld:

A composite element that is a conceptual or physical place or position where concepts are located (e.g., structure elements) or performed (e.g., behavior elements).

Bron: De Werkwijzer RWS. Deze bevat de ABDL: algemene begrippen en definitie lijst.

Vanuit configuratiemanagement is er behoefte aan een meer gedetailleerde definitie en attribuuttype. Daarom gebruiken we de volgende omschrijving (goedgekeurd door het ICMO en de IGA data architecte):

In de geografie is de locatie een positie of punt in de ruimte, uitgedrukt relatief ten opzichte van een ander punt of ding. Een absolute locatie kan vaak worden gedefinieerd met behulp van cartesische coördinaten, zoals gebruikmaking van specifieke breedtegraad en lengtegraad. Op Aarde kunnen de geografische coördinaten worden gebruikt om de locatie van een positie te specificeren.

Een locatie kan behalve absoluut – de exacte locatie van iets of iemand – ook relatief zijn, de positie van iemand ten opzichte van iets anders.

Bron: <https://nl.wikipedia.org/wiki/Locatie>

Opmerking: het is in de huidige CMDB van RWS nog niet mogelijk om Locatietabellen toe te voegen. Daarom zullen we **voorlopig** werken met het toevoegen van **Locatie-eigenschappen** aan de **attribuutvelden van de CI-items/Assets**. Zie hiervoor de attribuuttypes bij de uitgewerkte Asset.

Zie onder voor de Locatietabel

Locatie Tabel

Algemene business rule: alles wat van toepassing is, invullen. Wanneer de asset zich binnen een bekende vestiging bevindt, zijn coördinaten niet nodig.

Attribuut	Definitie	Schrijfwijze	Bron
Generiek			
UI	Unieke identificatiecode		idem
GPS Longitude		Volgens GPS format	Zo nauwkeurig als mogelijk, minimaal op vierkante meter nauwkeurig.
GPS Latitude		Volgens GPS format	Zo nauwkeurig als mogelijk, minimaal op vierkante meter nauwkeurig.
RD x-coördinaat		Volgens Rijksdriehoek	Zo nauwkeurig als mogelijk, minimaal op vierkante meter nauwkeurig.
RD y-coördinaat		Volgens Rijksdriehoek	Zo nauwkeurig als mogelijk, minimaal op vierkante meter nauwkeurig.
Specifiek			
BAG ID Indien het een BAG pand betreft, anders naar overig			ID zoals in de BAG geregistreerd.
IV locatie buiten ID			Bijv. KPN Voor infra buiten.
VM locatie ID			
SVM locatie ID			
WM locatie ID			
Asset Management locatie ID			
Vestiging			NU: Vestigingen opzoeken in dropdownlijst in Topdesk
Overige Plaatsbepaling zoals kamernummer			Locatie opzoeken in dropdownlijst met locaties in Topdesk.
Ruimte			
Rack (kast)nummer			
Rack (kast)hoogte			

Licentie Asset-type

Het recht op het gebruik van software/programmatuur en hardware

Bron: RWS CSIR

NB: dit Assettype is nog onder constructie. Voor de meest actuele versie en meer informatie over dit Asset-type: raadpleeg het model Programmatuur, deze zal op aanvraag beschikbaar worden gesteld

Attribuut	Definitie	Schrijfwijze
Object ID	Open veld	Invullen door RWS
Bron ID		Uniek ID zoals geregistreerd bij opdrachtnemer

Bestelnummer	Conform SAP. Niet elke licentie kent een BESTELNUMMER, alleen die, die niet onder een contract hangen. Ook wel '4500' genoemd.	Conform SAP. Niet uniek.
Onderhouds-contract	Het contract houdt in, dat de betreffende items door de leverancier in optimale conditie wordt gehouden.	'Ja' of 'Nee'.
Supportcontract	Het contract houdt in, dat de leverancier dienstverlening uitvoert ten behoeve van de afnemer.	'Ja' of 'Nee'.
Licentiecontract	Het contract houdt in, dat de leverancier de afnemer het recht geeft gebruik te maken van het gelicenceerde goed.	'Ja' of 'Nee'.
Soort licentie	Het soort licentie dat is afgesloten, Proprietary, Open Source of geen (PD)	Het soort licentie dat is afgesloten, Proprietary, Open Source of geen (PD)
Berekeningsbasis gebruiker	De wijze waarop de fee berekend wordt, die men verschuldigd is als gevolg van het aanvaarden van de licentie.	De wijze waarop de fee berekend wordt, die men verschuldigd is als gevolg van het aanvaarden van de licentie.
Berekeningsbasis installatie	De wijze waarop de fee berekend wordt, die men verschuldigd is als gevolg van het aanvaarden van de licentie.	De wijze waarop de fee berekend wordt, die men verschuldigd is als gevolg van het aanvaarden van de licentie.
Berekeningsbasis gebruik	De wijze waarop de fee berekend wordt, die men verschuldigd is als gevolg van het aanvaarden van de licentie.	De wijze waarop de fee berekend wordt, die men verschuldigd is als gevolg van het aanvaarden van de licentie.
Aantal	Het aantal legale, ingekochte licenties van deze soort en berekeningswijze.	Positief geheel getal.

Bron tabel: Conceptueel Datamodel Configuratie Management versie 1.0 vastgesteld.

Programmatuurbeschrijving Asset-type

Documentatie waarin met betrekking tot het betreffende CS R16 Configuratie Item -> Programmatuur Item het volgende wordt vastgelegd :

- Programmeertaal
- Communicatieprotocol (laag 7 van het OSI model), bijvoorbeeld:
 - LDAPversie
 - SMTPversie
 - HTTPversie

Bron: RWS CSIR

Attribuut	Definitie	Schrijfwijze
Object ID	Open veld	Invullen door RWS
Bron ID		Uniek ID zoals geregistreerd bij opdrachtnemer
Plaats	Waar kan de beheerdocumentatie worden gevonden?	Dit kan zowel een digitaal als fysiek adres zijn. Zo specifiek mogelijk dus indien van toepassing ook kamernummer en kast vermelden.
Datum laatst gewijzigd		ISO 8601 formaat: jjjj-mm-dd
Verantwoordelijk		Naam, organisatie en contactgegevens van de persoon die verantwoordelijk is voor de Programmatuurbeschrijving.
Programmatuur beschrijving Gewijzigd door?		Naam, organisatie en contactgegevens van de persoon die de laatste wijziging in de Programmatuurbeschrijving heeft doorgevoerd.
Aanleiding wijziging	Referentie aan Changeproces	
Programmeertaal		
Communicatie-protocol	Transportlaag (Laag 4) OSI model. (zie bijlage)	Keuzelijst: TCP, UDP of ISO-on-TCP(rfc1006) en het poortnummer (bv 80, 443, 22 etc).
Patch toegepast	Sprake van een Patch: ja/nee	
Datum laatste Patch		d-m-jjjj (let op: streepjes noodzakelijk)

Programmatuurversie Asset-type

De (door Opdrachtnemer op te leveren) set programmaregels 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

Bron: Bijzondere bepalingen Industriële Automatisering gerelateerde Programmatuur
Artikel 1: Begripsbepalingen Industriële Automatisering gerelateerde Programmatuur, 2n.

Voor de meest actuele versie en meer informatie over de soorten/Asset-types die onder het Data model Programmatuur vallen (bijvoorbeeld de definities e.d.): raadpleeg het Data model Programmatuur, deze zal op aanvraag beschikbaar worden gesteld. De inhoud is reeds opgenomen in de bijgeleverde CMDB Cybersecurity Industriële Automatisering Excel Format.

Attribuut	Definitie	Schrijfwijze
Object ID	Open veld	Invullen door RWS
Bron ID		Uniek ID zoals geregistreerd bij opdrachtnemer
Status Programmatuur versie	Keuzeveld	Keuzeveld: Ge-Deïnstalleerd Geïnstalleerd Niet geïnstalleerd Ontwikkelen
Missie Kritieke Systemen (MKS)	Het Programmatuur item is onderdeel van één of meer door Rijkswaterstaat vastgestelde Missie Kritieke Systemen. Deze informatie moet door Rijkswaterstaat worden aangeleverd.	Invullen door RWS Opsomming van de MKS(en) waarvan het Programmatuur item deel uitmaakt. Schrijfwijze zoals gehanteerd in lijst vastgestelde MKS.
Versie	Een specifieke variatie of verdere ontwikkeling van een origineel product	Zonder voorloop-V, nummers gescheiden door punten.
Programmatuur-type	Het soort applicatie/programmatuur, dat het hier betreft conform de indeling 'applicatietype'.	Keuzelijst: standalone applicatie, webapplicatie, client applicatie, mobile app, plug-in, clouddienst (SAAS), serverapplicatie (backend), Operating System
Producent	Overkoepelende naam, waaronder de 'Producent' zijn product verkoopt.	
Productnaam		Naam van de programmatuur zoals uitgegeven door de producent
Ordnummer Vendor		
Taal [ISO-639-3]		ISO codes (2 karakters): NL, DU, EN, etc.
Maatwerktype	In hoeverre er hier sprake is van maatwerk en welk type maatwerk het betreft.	Keuzelijst: keuzelijst: COTS, MOTS (modified of the shelf), maatwerk
A/B/C klassificatie	[A] Applicaties/Programmatuur die standaard worden geleverd op de standaard Werkstation. [B] Applicaties/Programmatuur die optioneel door iedere Werkplekgebruiker kunnen worden aangevraagd. [C] Overig. Vastgesteld door RWS-bestuur.	Keuzelijst: [A] Applicaties die standaard worden geleverd op de standaard Werkstation. [B] Applicaties die optioneel door iedere Werkplekgebruiker kunnen worden aangevraagd. [C] Overig.

Vestiging		Vestigingen opzoeken in dropdownlijst in Topdesk Indien van toepassing Let op: vaak niet beschikbaar voor opdrachtnemer dan als alternatief de adresgegevens invullen. Zie Excel
Overige plaatsbepaling zoals kamernummer		
GPS Location Latitude		
GPS Location Longitude		
RD X- coördinaat		
RD Y- coördinaat		

Virtueel Cluster Asettype

Indien van toepassing: Raadpleeg het model Infra & Hardware- KA, deze zal op aanvraag beschikbaar worden gesteld.

Virtuele server Asset-type

Virtualisatie maakt het mogelijk om op een fysieke server een (groot) aantal virtuele servers te gebruiken waardoor de fysieke server een veel groter deel van de tijd gebruikt wordt.

Bron: https://nl.wikipedia.org/wiki/Virtual_private_server

Raadpleeg voor de meest actuele versie ook het model Infa & Hardware-KA, deze zal op aanvraag beschikbaar worden gesteld.

Veld	Soort veld	Waarde / naamgeving-conventie
Object ID	Open veld	Invullen door RWS VM naam van virtuele server
Bron ID		Uniek ID zoals geregistreerd bij opdrachtnemer
Zonering		Invullen door RWS https://www.noraonline.nl/wiki/Beschouwingsmodel_zonering
Soort	Vaste waarde	Virtuele Server
Merk	Vaste keuzes	Windows Linux
Type	Vaste keuzes	Algemeen Applicatieserver (shared) Databaseserver Licentieserver Loadbalancer Webserver

		Servercapaciteit Werkstation
Specificatie (optioneel)	Open veld	
Serienummer (optioneel)	Open veld	(Oude VM-nummer van vóór de migratie)
Installatie door	Vaste keuzes	
Aanspreekpunt	Vaste keuzes	
Plaatskoppeling	Vaste waarde	Configuratie
Configuratie ID	Vaste keuzes	<i>Beschikbaarheid Topdesk</i>
Status	Vaste keuzes	o.a.: Actief Inactief
Aantal CPU'	Open veld	
RAM Geheugen	Open veld	GB, afgerond naar 1 decimaal
Toegekend schijfruimte	Open veld	Afgerond naar hele GB's
Productdomein	Vaste keuzes	IRN BV Ontwikkeling en Services IRN IV Infrastructuur IRN IV Platformen OSR A en O Services OSR SVM Services OSR VM Services OSR WM Services
Primair product	Open veld	
OTAP(L) omgeving	Vaste keuzes	Ontwikkel Test Acceptatie Productie Les
Infra service / bouwsteen		
Serienummer	Open veld	(het UUID van de VM volgens VMWare)
Hostnaam	Open veld	
IP-adres (optioneel)	Open veld	
OS Beheerder		
Eigenaarschap (Service Delivery Manager)		dynamische dropdownlijst die refereert aan de persoonstabeltabel.
Operating System	Open veld	
LCM Afvoerdatum	Datum veld	d-m-jyyy (let op: streepjes noodzakelijk)

Wijzigingendocument (Escrow) Asset-type

Soorten:

- Escrow
- Overig

Toelichting Escrow:

Het deponeren van (een kopie van) de Broncode van Standaardprogrammatuur 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.

Bron: Bijzondere bepalingen Industriële Automatisering gerelateerde Programmatuur
Artikel 1: Begripsbepalingen Industriële Automatisering gerelateerde Programmatuur, 2d.

Escrow omvat alle niet openbaargemaakte informatie die de Opdrachtgever redelijkerwijs nodig heeft voor fouthterstel, onderhoud, verder ontwikkelen en beheer van de Standaardprogrammatuur zodat hij daarvan het overeengekomen gebruik kan blijven maken. Escrow voldoet aan het geen dienaangaande ten tijde van het afsluiten daarvan op de Nederlandse markt gebruikelijk is. COTS Programmatuur valt buiten de scope van Escrow

Zie ook Bron: Bijzondere bepalingen Industriële Automatisering gerelateerde Programmatuur
Artikel 7: Escrow, bijlage A voor de eisen die aan Escrow worden gesteld.

Attribuut	Definitie	Schrijfwijze
Object ID	Open veld	Invullen door RWS
Bron ID		Uniek ID zoals geregistreerd bij opdrachtnemer
Escrow documentatie aanwezig?	Keuzeveld	Ja nee
Datum eerste deponering	Datum waarop de eerste deponering van de Escrow heeft plaatsgevonden	d-m-jjjj (let op: streepjes noodzakelijk)
Datum laatste deponering	Datum waarop de eerste deponering van de Escrow heeft plaatsgevonden	d-m-jjjj (let op: streepjes noodzakelijk)
Escrow agent	De in te zetten Escrow agent heeft expertise om het gedeponeerde Product en bijbehorende Materialen te controleren op aanwezigheid, volledigheid en bruikbaarheid. Het Product en bijbehorende Materialen	Naam, organisatie en contactgegevens van de Escrow agent.

De CMDB opbouw en onderhoud dient conform de CMDB Cybersecurity Industriële Automatisering Excel Format vorm gegeven te worden. De Excel Format is op verzoek verkrijgbaar bij het Security Centre van CIV.



CMDB
Cybersecurity Indust

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 storingsmeldingen. 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

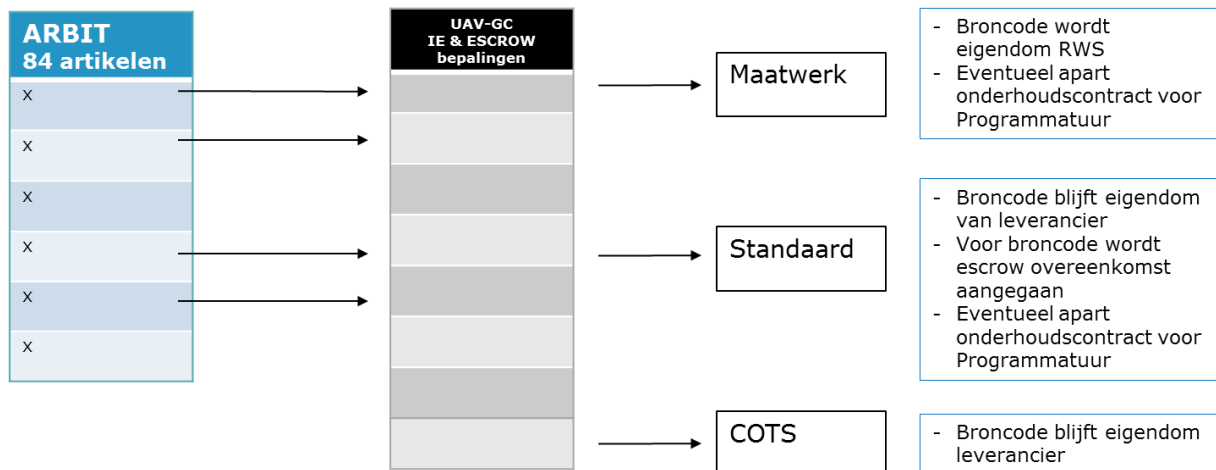
Intellectueel Eigendomsrechten zijn exclusieve rechten van rechthebbenden op een voortbrengsel van de menselijke geest. Een voorbeeld daarvan is het auteursrecht, waar Programmatuur onder valt. IE-rechten stellen de eigenaar in staat het werk (Programmatuur) te exploiteren.

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. De 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 gebedigde 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 vereenvoudigingen.
- 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 verwijdt geen aanduidingen van eigendoms- en/of auteursrechten bij het veelelvoudigen 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 aantoonbaar 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 gedeponereerd 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.

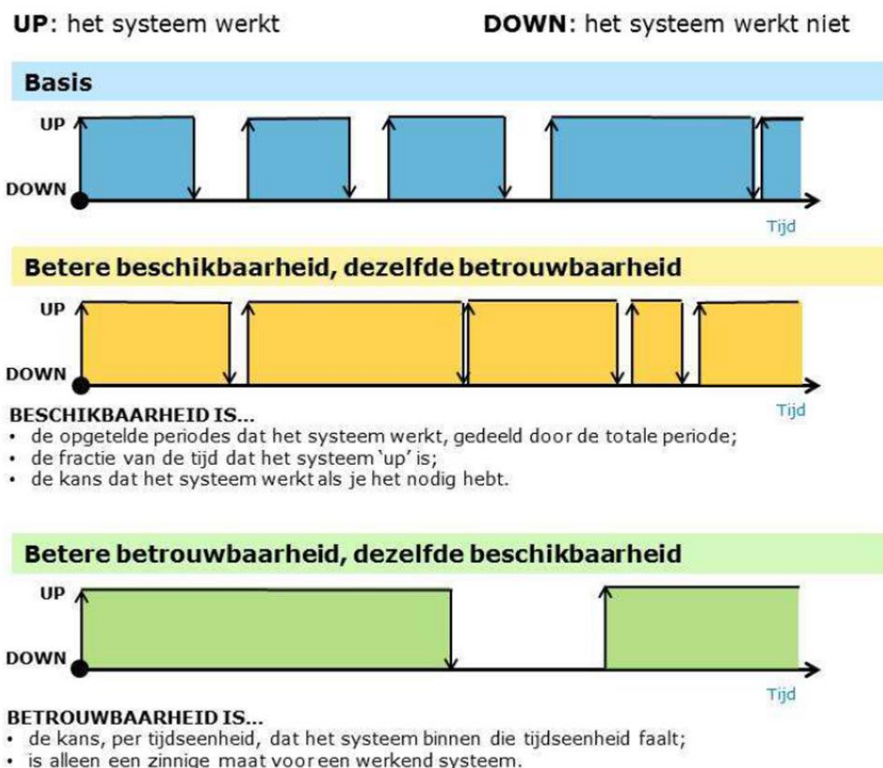
Beschikbaarheid (IA)

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 waarschijnlijkheid 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 ($t > 5 \text{ jaar}$)	De kans en daarmee het falen van de functie van het object wordt niet binnen 5 jaar verwacht;
2	Klein ($3 \text{ jaar} < t \leq 5 \text{ jaar}$)	De kans en daarmee het falen van de functie van het object wordt tussen 3 jaar en 5 jaar na nu verwacht;
3	Middelmatig ($2 \text{ jaar} < t \leq 3 \text{ jaar}$)	De kans en daarmee het falen van de functie van het object wordt tussen 2 jaar en 3 jaar na nu verwacht;
4	Groot ($1 \text{ jaar} < t \leq 2 \text{ jaar}$)	De kans en daarmee het falen van de functie van het object wordt tussen 1 jaar en 2 jaar na nu verwacht;
5	Zeker ($t \leq 1 \text{ jaar}$)	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 betreffend 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 moeilijker 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 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 de 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 betreffende 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 N – J-STD-016

Vraagspecificatie Proces – Raamovereenkomst

Realisatie Variabel onderhoud stalen bruggen West Nederland Zuid
Project Over-Bruggen



Zaaknummer: **31196743**

Datum: 14 januari 2025

Bijlage N - J-STD-016

Deze bijlage 'J-STD-016' geldt **generiek** voor alle Nadere Overeenkomsten.

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 VIOLATE THE LAW!

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 Documents 15 Inverness Way East Englewood, CO 80112-5704 or call U.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) **Is 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 Gray
Lewis 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.1 Scope	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 confidentiali-

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 has been 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 5.1 7 (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

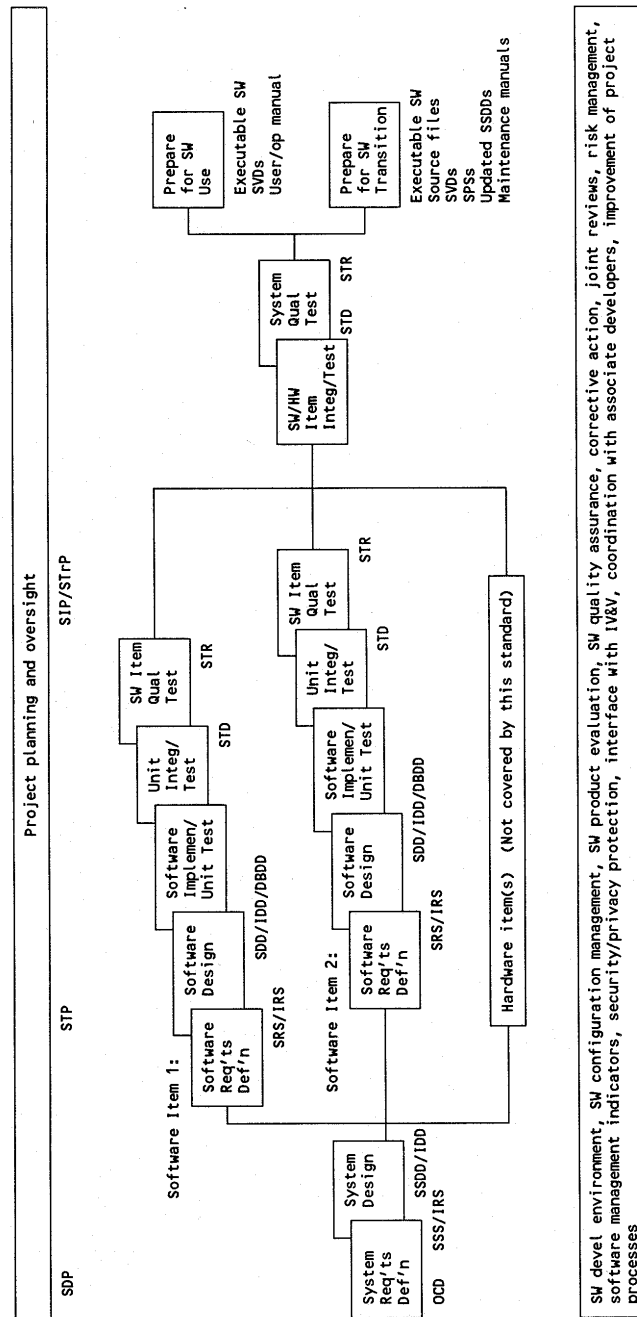
Planning the software builds on a project for each build may be accomplished in several ways. The acquirer might, for example, select an overall development strategy, leaving it to the developer to lay out the software builds. Alternatively, the acquirer might lay out the software builds as part of the 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	- User prefers all capabilities at first delivery	M
- System too large to do all at once	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



Note: All activities may be more ongoing, overlapping, and iterative than the figure is able to show.

Figure 4 — One possible way of applying this standard to the Once-Through development strategy

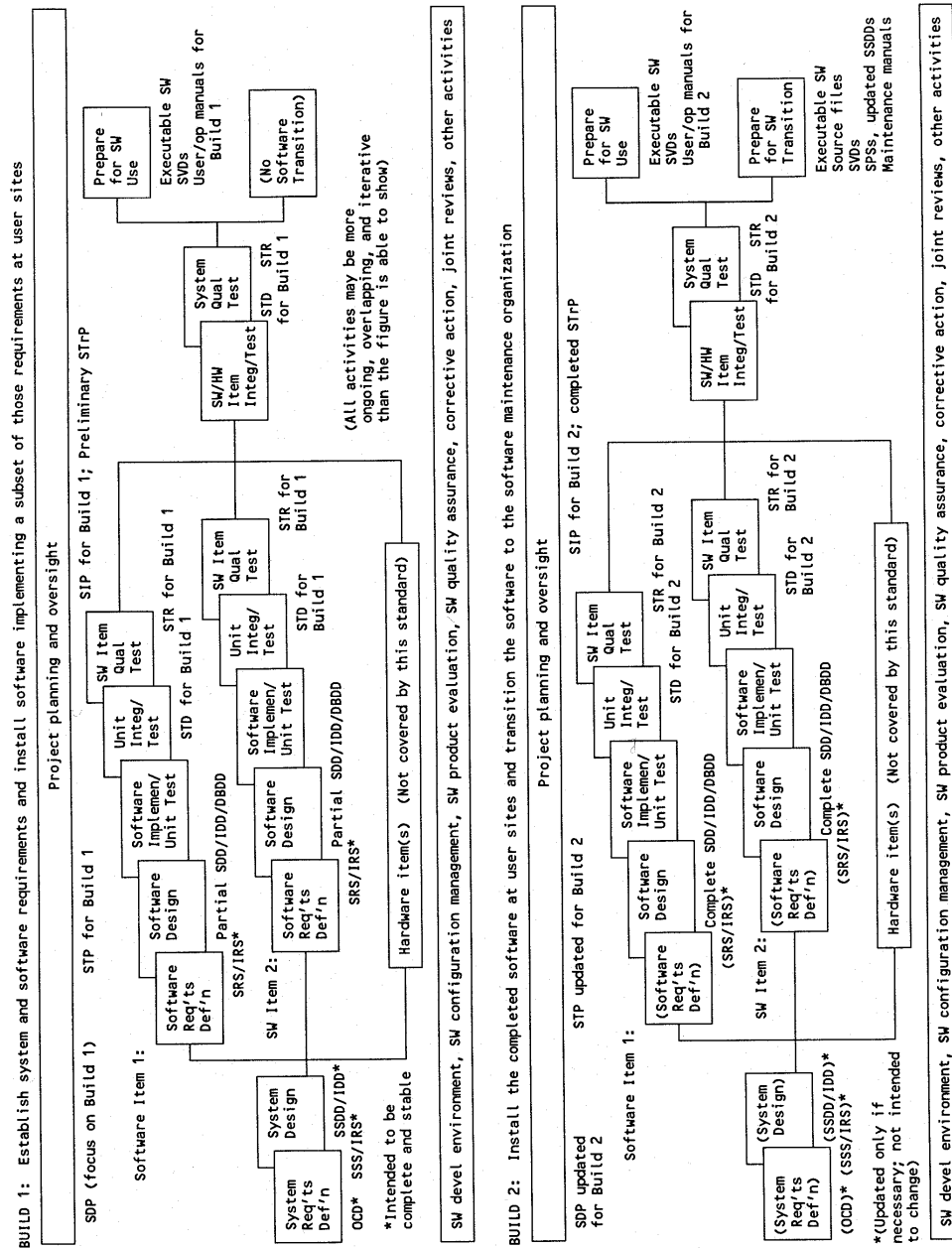
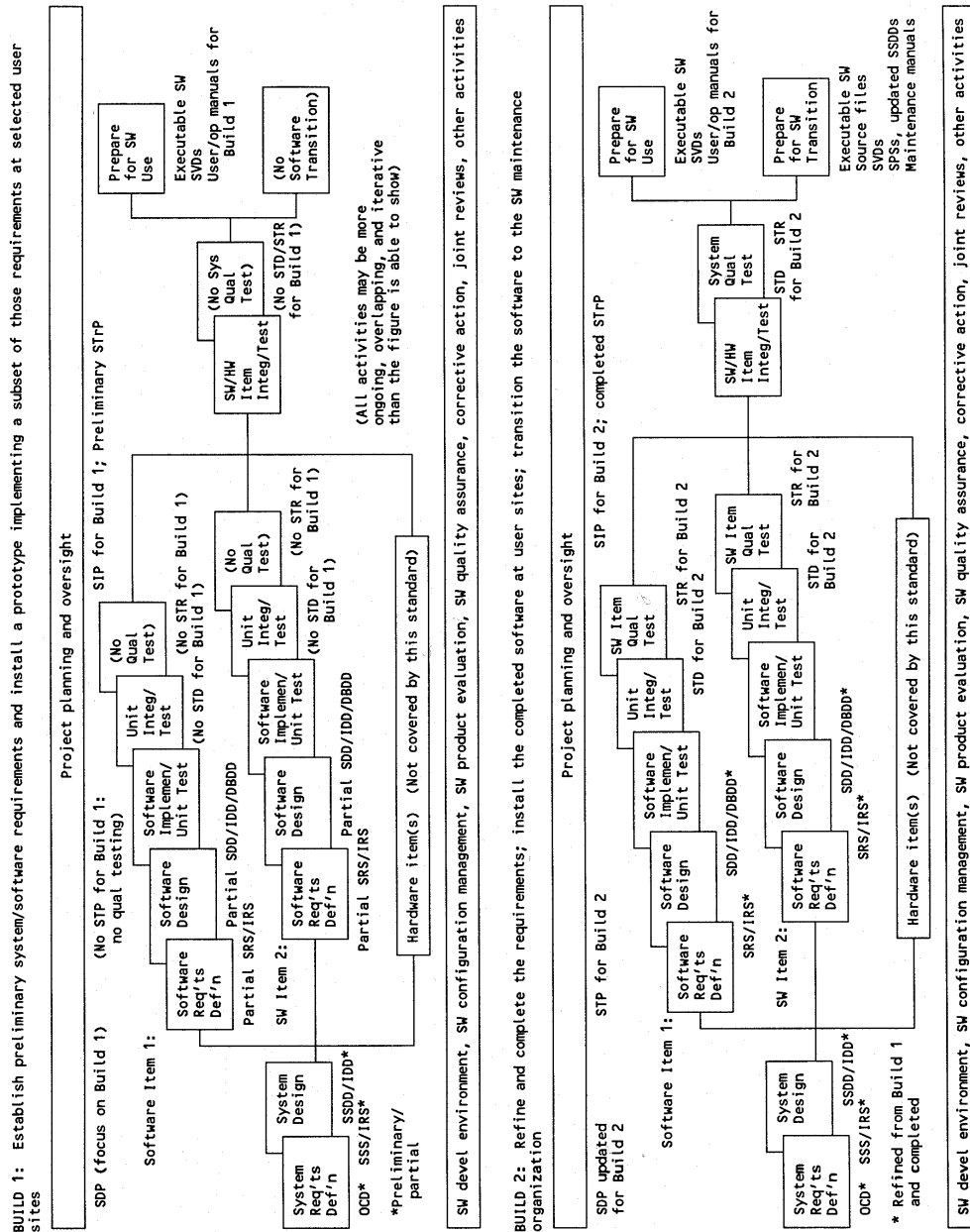


Figure 5 — One possible way of applying this standard to the Incremental development strategy



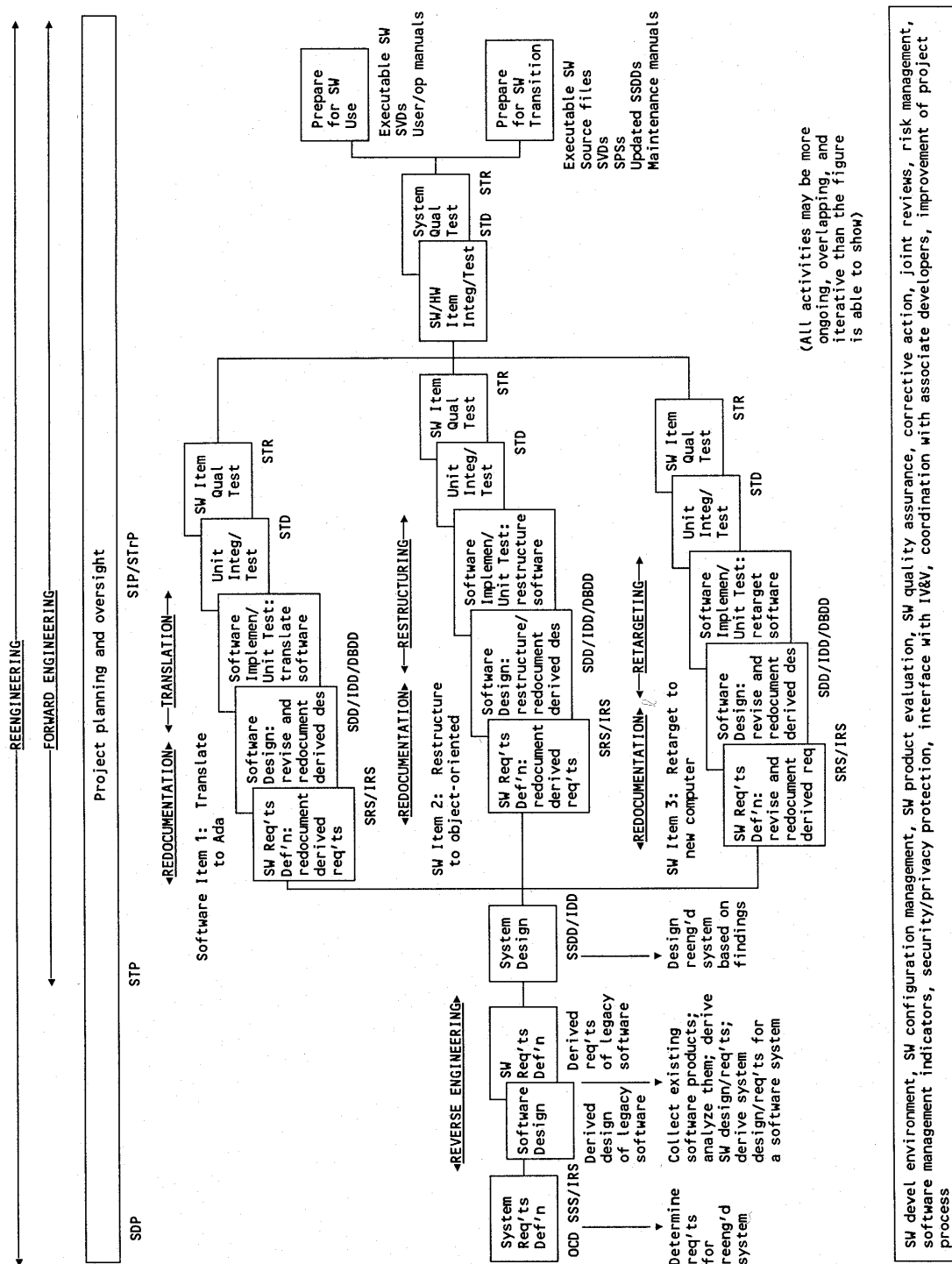


Figure7 — One possible way of applying this standard to a reengineering project

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 sub-clauses 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 No: No software item qual testing in this build	Yes: Plan Build 2 in detail; Builds 3-4 in general No: No software item qual testing in this build	Yes: Plan Build 3 in detail; Build 4 in general No: No software item qual testing in this build	Yes: Plan Build 4 in detail No: No software item qual testing in this build
5.1.2	Plan for software item 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 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 Yes: Very preliminary planning only	No: Let users install on their own Yes: Update preliminary plans	Yes: Plan to install at user sites Yes: Update preliminary plans	Yes: Update as needed for installation of Bld 4 Yes: Finalize transition planning
5.1.5	Plan for transitioning software to the maintenance organization	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
5.1.6	Follow plans; perform management review				
5.2	ESTABLISHING A SOFTWARE DEVELOPMENT 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 development 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 item'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

The 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 IRSSs.

- 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

The 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 sub-system-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

The 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 software item, 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 sub-clause 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

The 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 (IRSSs). For system testing, traceability from each system requirement in the system's System/Subsystem Specification (SSS) and associated IRSSs. 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

The 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

The 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		Overview	
Software Product		Annex	
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 (IRSSs) referenced from the SRS. The SRS, possibly supplemented by IRSSs, 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 (IRSSs) referenced from the SSS. The SSS, possibly supplemented by IRSSs, 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						Additional Criteria
	Contains all applic. info in:	Meets SOW, if applic.	Meets deliverables, if applic.	Understandable	Intern. consistent	Follows SW dev plan	
1. Software development plan (5.1.1)	a. E.2.1 (SDP)	b.	c.	d.	e.	f. (Updates)	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						Additional Criteria
	Contains all applic. info in:	Meets SOW, if applic.	Meets deliv reqts, if applic.	Understandable	Intern. consistent	Follows SW dev plan	
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						Additional Criteria
	Contains all applic. info in:	Meets SOW, if applic.	Meets deliv reqts, if applic.	Understandable	Intern. consistent	Follows SW dev plan	
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						Additional Criteria
	Contains all applic. info in:	Meets SOW, if applic.	Meets deliv reqts, if applic.	Understandable	Intern. consistent	Follows SW dev plan	
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 annexes 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/EIA 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		Multi-national		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 O - MIL-STD-1521B

Vraagspecificatie Proces – Raamovereenkomst

Realisatie Variabel onderhoud stalen bruggen West Nederland Zuid
Project Over-Bruggen



Zaaknummer: **31196743**

Datum: 14 januari 2025

Bijlage O - 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

Deze bijlage 'MIL-STD-1521B' geldt generiek voor alle Nadere Overeenkomsten.

MIL-STD-1521 B (USAF)

4 JUNE 1986

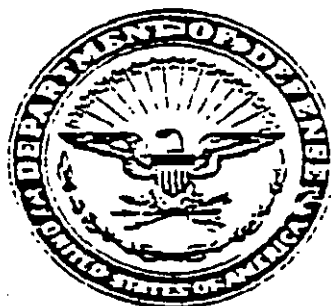
SUPERSEDING

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.

MIL-STD-1521B

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.

MIL-STD-1521B

FOREWORD

This standard has been designed to take advantage of current technological advancement and management procedures in conducting reviews and audits.

MIL-STD-1521B

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

MIL-STD-1521B**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

MIL-STD-1521B

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.

MIL-STD-1521B

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).

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) compatibility between software requirements and preliminary design, and (3) on the preliminary version of the

MIL-STD-1521B

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.

MIL-STD-1521B

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.

MIL-STD-1521B

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

MIL-STD-1521B

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 satisfactory

MIL-STD-1521B

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).

MIL-STD-1521B

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.

MIL-STD-1521B

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.

<u>Paragraph No.</u>	<u>Data Requirement Title</u>	<u>Applicable DID No.</u>
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.

MIL-STD-1521B

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

Figure 2 Sample Action Item Form

MIL-STD-1521B
-APPENDIX A

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

MIL-STD-1521B
APPENDIX A

- 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:

MIL STD 1521B

APPENDIX A

- 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.

MIL-STD-1521B

APPENDIX B

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

MIL-STD-1521B

APPENDIX B

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 Reviewed. 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

MIL-STD-1521B APPENDIX B

- 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

MIL-STD-1521B APPENDIX B

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.

MIL-STD-1521B
APPENDIX B

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 VECs (as applicable).

MIL-STD-1521B
APPENDIX B

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

MIL-STD-1521B

APPENDIX B

- 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 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 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.

MIL-STD-1521B
APPENDIX B

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.

MIL-STD-1521B
APPENDIX C

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

MIL-STD-1521B
APPENDIX C

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).

**MIL-STD-1521B
APPENDIX D**

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 HWC1 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,

**MIL-STD-1521B
APPENDIX D**

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 reliability/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 procure

MIL-STD-15219
APPENDIX D

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.

MIL-STD-1521B
APPENDIX D

- 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.

MIL-STD-1521B

APPENDIX D

- 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

**MIL-STD-1521B
APPENDIX D**

using existing, developmental, and proposed new SE. For mobile systems, review the mobility requirements of support equipment.

1. 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.

MIL-STD-1521B APPENDIX D

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.

MIL-STD-1521B APPENDIX D

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 HWCIs 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 HWCIs 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.

MIL-STD-1521B APPENDIX D

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.

MIL-STD-1521B APPENDIX D

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 HWC Development Specification.

40.9.2 Insure that the contractor clearly understands the effect of, and the interactions between, the natural aerospace environment and HWC 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

MIL-STD-1521B
APPENDIX D

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.

MIL-STD-1521B
APPENDIX D

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/Maintainability/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:

MIL-STD-1521B

APPENDIX C

- a. Contractor's Value Engineering organization, policies and procedures.
- b. Contractor's Value Engineering Training Program.
- c. Potential Value Engineering projects, studies and VECs.
- d. Schedule of planned Value Engineering tasks/events.
- e. Policies and procedures for subcontractor Value Engineering Programs.

40.12 Transportability

40.12.1 Review HWCs 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 HWCs requiring special temperature and humidity control or those possessing sensitive and shock susceptibility characteristics. Determine special transportation requirements and availability for use with these HWCs.

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, HWC 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.

**MIL-STD-1521B
APPENDIX D**

- 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:

MIL-STD-1521B
APPENDIX D

- 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.

**MIL-STD-1521B
APPENDIX D**

- 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,

MIL-STD-1521B
APPENDIX D

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.

MIL-STD-1521B
APPENDIX D

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.

**MIL-STD-1521B
APPENDIX D**

- 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.

**MIL-STD-1521B
APPENDIX E**

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, drawings, schematics, mockups, etc., shall be reviewed against the HWC1 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

MIL-STD-1521B
APPENDIX E

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

MIL-STD-1521B

APPENDIX E

- (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 CSC's.

- 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.

MIL-STD-1521B

APPENDIX E

- 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

MIL-STD-1521B
APPENDIX E

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 LLCSC design requirements.

MIL-STD-1521B APPENDIX E

- 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 CSCIs, 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 HWCI's. 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

-MIL-STD-1521B
APPENDIX E

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.

MIL-STD-1521B
APPENDIX E

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 HWC 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

MIL-STD-1521B

APPENDIX E

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

MIL-STD-1521B

APPENDIX E

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 VECs presented per the terms of the contract.

50.11.2 Review any new areas of potential Value Engineering considered profitable to challenge.

MIL-STD-1521B
APPENDIX E

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, material, or process must meet to be acceptable.

50.13.5 Review all test documentation required to support test

MIL-STD-1521B

APPENDIX E

requirements of Section 4.0 of HWC 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.

**MIL-STD-1521B
APPENDIX E**

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 HWC1, 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 HWC1 to determine if a category I container is required. The analysis of the proposed container or handling, shipping equivalent shall encompass as a minimum:

**MIL-STD-1521B
APPENDIX E**

- 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.

MIL-STD-1521B
APPENDIX E

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.

**MIL-STD-1521B
APPENDIX F**

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.

MIL-STD-1521B
APPENDIX F

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.

MIL-STD-1521B
APPENDIX G

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.):

MIL-STD-1521B
APPENDIX G

- 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.

MIL-STD-1521B
APPENDIX G

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 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.

MIL-STD-1521B
APPENDIX G

- d. All ECPs that have been approved shall be reviewed to ensure that they have been technically incorporated and verified.
- e. All updates 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.

**MIL-STD-1521B
APPENDIX H**

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 replacement 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 (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

MIL-STD-1521B
APPENDIX H

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.

MIL-STD-1521B APPENDIX H

- 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:

MIL-STD-1521B
APPENDIX H

- 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 reviewed 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.

MIL-STD-1521B

APPENDIX H

- (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 reviewed 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 drawing 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 reviewed for purpose of determining the contractor's present and most recent past performance.

MIL-STD-1521B
APPENDIX H

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.

MIL-STD-1521B
APPENDIX H

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 HWC1 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 and 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

MIL-STD-1521B
APPENDIX H

- 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.

MIL-STD-1521B

APPENDIX I

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

MIL-STD-1521B
APPENDIX I

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 reviewed, 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.

MIL-STD-1521B

APPENDIX 1

SAMPLE CERTIFICATION ATTACHMENT

PRE-FCA CHECK SHEET

NOMENCLATURE _____

CONFIGURATION ITEM NO. _____

DATE _____

CONTRACTOR REQUIREMENTSYESNO

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

MIL-STD-1521B
APPENDIX I

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

MIL-STD-1521B

APPENDIX I

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.

MIL-STD-1521B

APPENDIX I

SCOPE/PURPOSEScope:

Functional Configuration Audit (FCA) was conducted on the following configuration item:

<u>Configuration Item No.</u>	<u>Nomenclature</u>	<u>Part No.</u>	<u>Serial No.</u>

PURPOSE: The purpose of this FCA was to verify that the configuration item's performance complies with the Type B Development Specification.

MIL-STD-1521B

APPENDIX I

FUNCTIONAL CONFIGURATION AUDITCERTIFICATION 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 adequate, 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 _____

MIL-STD-1521B
APPENDIX I

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

MIL-STD-1521B

APPENDIX I

FUNCTIONAL CONFIGURATION AUDITCERTIFICATION 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

MIL-STD-1521B

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

MIL-STD-15218

APPENDIX I

WAIVERS/DEVIATIONS

CONFIGURATION ITEM NO. _____ NOMENCLATURE _____			
REFERENCE (Spec, STD, Etc.)	CCB OR MRD APPROVAL/DIRECTIVE	REQUIREMENT WAIVED	REMARKS

Figure 3
Page 10 of 11

MIL-STD-1521B

APPENDIX I

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)

_____	_____
_____	_____
_____	_____
_____	_____
_____	_____
_____	_____

MIL-STD-1521B
APPENDIX I

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:

	<u>Yes</u>	<u>No</u>
(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

MIL-STD-1521B
APPENDIX I

SAMPLE CERTIFICATION ATTACHMENT
SAMPLE PCA CHECKLIST (CONTINUED)

	<u>Yes</u>	<u>No</u>
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

MIL-STD-1521B

APPENDIX I

SAMPLE CERTIFICATION ATTACHMENT
PHYSICAL CONFIGURATION AUDIT (PCA)

FOR

CONFIGURATION ITEM NO. (s) _____

CONTRACT NO. _____

PRIME CONTRACTOR:

EQUIPMENT MANUFACTURERS:

APPROVED BY _____ (DESIGNEE)
CONTRACTOR

APPROVED BY _____ (DESIGNEE)
CONTRACTING AGENCY

DATE _____

DATE _____

Figure 4
Page 2 of 20

MIL-STD-1521B

APPENDIX I

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 note 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.

Figure 4
Page 3 of 20

MIL-STD-1521R
APPENDIX I

SCOPE/PURPOSE

A Physical Configuration Audit (PCA) was conducted on the following end items of equipment/computer software:

<u>CONFIGURATION ITEM</u>	<u>NOMENCLATURE</u>	<u>PART NUMBER</u>	<u>SERIAL NO.</u>	<u>NSN</u>

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.

Figure 4
Page 4 of 20

MIL-STD-1521E
APPENDIX I

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:

<u>SPEC NO.</u>	<u>ASSEMBLY TOP DRAWING NO.</u>	<u>ISSUE</u>	<u>EQPT./COMP. SOFTWARE NOMENCLATURE</u>	<u>CONFIGURATION ITEM NO.</u>

Signature(s) of PCA Team Member(s)

**	_____	_____
*	_____	_____
	_____	_____
	_____	_____
	_____	_____
	_____	_____

**Team Chairperson

*Sub-Team Chairperson

MIL-STD-1521B

APPENDIX I

PHYSICAL CONFIGURATION AUDITCERTIFICATION 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

MIL-STD-1521B

APPENDIX I

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

<u>SPEC NO.</u>	<u>PART NO.</u>	<u>DATE</u>	<u>EQPT./COMP. SOFTWARE NOMENCLATURE</u>	<u>CONFIGURATION ITEM NO.</u>

2. Specifications Reviewed and Disapproved:
(Provide attachment for causes.)

MIL-STD-1521B
APPENDIX I

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

MIL-STD-1521B
APPENDIX I

- 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

MIL-STD-1521B
APPENDIX I

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

MIL-STD-1521B
APPENDIX I

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

MIL-STD-1521B
APPENDIX I

- A. Review of Shortages and Unincorporated Design Changes. All shortages and unincorporated 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.

MIL-STD-1521B
APPENDIX I

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

MIL-STD-1521B
APPENDIX I

- 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

MIL-STD-1521B

APPENDIX I

PHYSICAL CONFIGURATION AUDITCERTIFICATION 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 included 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

MIL-STD-15210
APPENDIX I

- 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

APPENDIX I

PHYSICAL CONFIGURATION AUDITCERTIFICATION 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

MIL-STD-1521 B

APPENDIX I

PHYSICAL CONFIGURATION AUDITCERTIFICATION 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

**MIL-STD-1521B
APPENDIX I**

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 with 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

MIL-STD-1521B

APPENDIX I

PHYSICAL CONFIGURATION AUDITCERTIFICATION 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

MIL-STD-1521B

APPENDIX J

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 Tailoring100.4.1 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

MIL-STD-1521B APPENDIX J

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 effective 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

MIL-STD-1521B APPENDIX J

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

<u>Review</u>	<u>Time Phase</u>	<u>Primary Documentation</u>
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

**MIL-STD-1521B
APPENDIX J**

<u>Review</u>	<u>Time Phase</u>	<u>Primary Documentation</u>
	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),

**MIL-STD-1521B
APPENDIX J**

<u>Review</u>	<u>Time Phase</u>	<u>Primary Documentation</u>
		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).

MIL-STD-1521B
APPENDIX K

110. Production Readiness Review (PRR)

110.1 For specific guidance, see AFSCR 64-2, Production Readiness Review.

MIL-STD-1521B

Custodian:
Air Force - 13

Preparing Activity:
Air Force - 13

Review Activity:
Air Force - 10,11,80,85

(Project CMAN-0-006)

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 inner edge (**DO NOT STAPLE**), and mailed. In block 5, 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. 7526 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

STANDARDIZATION DOCUMENT IMPROVEMENT PROPOSAL

(See Instructions - Reverse Side)

1. DOCUMENT NUMBER

2. DOCUMENT TITLE

NAME OF SUBMITTING ORGANIZATION

4. TYPE OF ORGANIZATION (Mark one)

☐ VENDOR☐ USER☐ MANUFACTURER☐ OTHER (Specify): _____

3. ADDRESS (Street, City, State, ZIP Code)

5. PROBLEM AREAS

A. Paragraph Number and Wording:

B. Recommended Wording:

C. Reason/Rationale for Recommendation:

6. REMARKS

NAME OF SUBMITTER (Last, First, MI) - Complete

D. WORK TELEPHONE NUMBER (Include
Code) - Complete

MAILING ADDRESS (Street, City, State, ZIP Code) - Complete

E. DATE OF SUBMISSION (YYMMDD)

19 Dec 1985

**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.

MIL-STD-1521B
19 Dec 1985

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 (PCA)	75
I. Formal Qualification Review (FQR)	83
J. Application Guide for Tailoring MIL-STD-1521	117
K. Production Readiness Review (PRR)	123

MIL-STD-1521B

19 Dec 1985

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 APR 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.

3.15 Engineering Data: Engineering documents such as drawings, associated lists, accompanying 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.

Supersedes page 7/8 of 4 June 1985

MIL-STD-1521B

APPENDIX A

19 Dec 85

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 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

Supersedes page 19 of 4 June 1985

MIL-STD-1521B
4 June 1985
APPENDIX A

- 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:

MIL-STD-1521B

APPENDIX B

19 Dec 85

- 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. 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

Supersedes page 25 of 4 June 1985

MIL-STD-1521B

APPENDIX B

19 Dec 1985

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.

Supersedes page 26 of 4 June 1985

MIL-STD-1521B

APPENDIX B

19 Dec 85

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.

MIL-STD-1521B

APPENDIX B

19 Dec 85

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.

Supersedes page 30 of 4 June 1985

MIL-STD-1521B
 APPENDIX D
 19 Dec 85

equipment shall be made available for review by the contracting agency.

2. 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, MOS)), 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
- ae. Support equipment requirements.

0.2.2 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.

ersedes page 35 of 4 June 1985

MIL-STD-1521B

4 June 1985

APPENDIX D

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.

MIL-STD-1521B

4 June 1985

APPENDIX D

n. Operation and support documents. The preliminary versions of the CSOM, SUM, CSDM, and CRISD shall be reviewed for technical content and compatibility 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 available 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

MIL-STD-1521B

APPENDIX D

19 Dec 85

using existing, developmental, and proposed new SE. For mobile systems, review the mobility requirements of support equipment.

1. 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. 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 Specification and Interface Requirements Specification(s).

Supersedes page 38 of 4 June 1985

MIL-STD-1521B

APPENDIX D

19 Dec 85

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.

MIL-STD-1521B

APPENDIX E

19 Dec 85

- (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 EHCI 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 VECs and/or formal VECs
 - 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.

Supersedes page 55 of 4 June 1985

MIL-STD-1521B
APPENDIX E
19 Dec 85

- 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.

MIL-STD-1521B

APPENDIX E

19 Dec 1985

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

MIL-STD-1521B

APPENDIX G

19 Dec 1985

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.):

MIL-STD-1521B

4 June 1985

APPENDIX G

- 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 PCA 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.

MIL-STD-1521B

APPENDIX G

19 Dec 1985

70.4.5 Test reports, procedures, and data used by the PCA team shall be made a matter of record in the PCA 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 EMC 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 PCA for the configuration item. See Pre-PCA checklist.

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 PCA 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 PCA 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 PCA 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.

Supersedes page 73 of 4 June 1985

MIL-STD-1521B

4 June 1985

APPENDIX G

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 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.

70.5.2 The accomplishment of the PCA shall be recorded on the configuration item Development Record by the contractor.

MIL-STD-1521B

APPENDIX B

19 Dec 1985

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 reprourement 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 Manual (SUM), Computer System Diagnostic Manual (CSDM), Software Programmer's Manual (SPH), Firmware Support Manual (PSM)) to check format, completeness, and conformance with applicable data item descriptions.

80.1.5. Continuing with the results of the Functional 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

Supersedes page 75 of 4 June 1985

MIL-STD-1521B

4 June 1985

APPENDIX B

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.

MIL-STD-1521B

APPENDIX J

19 Dec 1985

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.

MIL-STD-1521B
APPENDIX J
19 Dec 1985

TABLE 1
SCHEDULING REVIEWS AND AUDITS

<u>Review</u>	<u>Time Phase</u>	<u>Primary Documentation</u>
SER	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

MIL-STD-1521B

4 June 1985

APPENDIX K

110. Production Readiness Review (PRR)

110.1 For specific guidance, see APSCR 84-2, Production Readiness Review.

MIL-STD-1521B

19 Dec 1985

FIGURE 5

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?

Supersedes page 124 of 4 June 1985

MIL-STD-1521B

19 Dec 1985

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.

MIL-STD-1521B
19 Dec 1985

Custodian:
Air Force - 13

Preparing Activity:
Air Force - 13

Review Activity:
Air Force - 10, 11, 80, 85

(Project CHAN-0-006)



BIJLAGE P – Invulinstructie format LV BRO

Vraagspecificatie Proces – Raamovereenkomst

Realisatie Variabel onderhoud stalen bruggen West Nederland Zuid
Project Over-Bruggen



Zaaknummer: **31196743**

Datum: 14 januari 2025

Bijlage P - Invulinstructie format LV BRO

Deze bijlage 'Invulinstructie format LV BRO' geldt **generiek** voor alle Nadere Overeenkomsten.

Deze bijlage bevat een invulinstructie ten aanzien van het format van de 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) <i>Toelichting: het KvK nummer van Rijkswaterstaat ter identificatie als bestuursorgaan</i>
Object-ID	<Vul WBS element in> <i>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.</i> <i>Niet bekend met het nummer? Vraag het de betrokken adviseur bedrijfsvoering.</i>
Data-leverancier	Het KvK nummer van de hoofdopdrachtnemer. (ALTIJD) <i>Toelichting: dit is een invulinstructie voor de Opdrachtnemer</i>
Kwaliteits-regime	IMBRO (ALTIJD)
Kader aanlevering	<Vul het inwinkader in> (PROJECTSPECIFIEK) <i>Toelichting: Rijkswaterstaat kiest in welk kader de onderzoeken zijn uitgevoerd; keuze uit:</i> <i>a. Opdracht publieke taakuitvoering,</i> <i>b. Rechtsgrond Waterwet.</i>
Kader inwinning	Invullen door diegene die de opdracht verstrekt tot het onderzoek naar de ondergrond. Keuze uit 7 opties. <i>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:</i> <i>1. eigenschappen van de ondergrond rondom waterkeringen te verkennen,</i> <i>2. eigenschappen van de ondergrond rondom bouwwerken en constructies te verkennen,</i>

	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. <i>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.</i> <i>De eigenaar moet gespecificeerd worden o.b.v. KVK-nummer. In het geval dat Rijkswaterstaat eigenaar is, moet KVK-nummer 27364178 worden ingevuld.</i>
Onderhoudende 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. <i>Toelichting: de onderhoudende instantie moet gespecificeerd worden o.b.v. KvK-nummer.</i>
Initiële functie	Invullen door diegene die opdracht geeft tot het aanleggen van een grondwatermonitoringput. Keuze uit 5 opties: <i>Toelichting: keuze uit:</i> 1. Brandput, 2. Monitoring grondwaterstand, 3. Monitoring grondwatersamenstelling, 4. Monitoring grondwaterstand en grondwatersamenstelling, 5. Grondwateronttrekking.



BIJLAGE Q – Melding inzet zelfstandige hulppersoon

Vraagspecificatie Proces – Raamovereenkomst

Realisatie Variabel onderhoud stalen bruggen West Nederland Zuid
Project Over-Bruggen



Zaaknummer: **31196743**

Datum: 14 januari 2025

Bijlage Q - Melding inzet zelfstandige hulppersoon

Deze bijlage 'Melding inzet zelfstandige hulppersoon' geldt **generiek** voor alle Nadere Overeenkomsten.

Het Uniform Europees Aanbestedingsdocument wordt als apart document als een interactief pdf-formulier ter beschikking gesteld via TenderNed.



BIJLAGE R – Aanvullende eigen verklaring inzake Russische partijen

Vraagspecificatie Proces – Raamovereenkomst

Realisatie Variabel onderhoud stalen bruggen West Nederland Zuid
Project Over-Bruggen



Zaaknummer: **31196743**

Datum: 14 januari 2025

Bijlage R - Aanvullende eigen verklaring inzake Russische partijen

Deze bijlage 'Aanvullende eigen verklaring inzake Russische partijen' geldt **generiek** voor alle Nadere Overeenkomsten.

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: