Rijkswaterstaat
Ministerie van Infrastructuur en Milieu

WKS - Beheer op Afstand

System/Subsystem Specification (SSS)

Datum: 1 februari 2013

Documentversie: 1.0 (Definitief)

Colofon:

Uitgegeven door:	Ministerie van Infrastructuur en Milieu Rijkswaterstaat, Dienst Verkeer en Scheepvaart Data en ICT Dienst
Informatie:	ing P.P.J. Beckers
Telefoon:	06-15017917
Email:	paul.beckers@rws.nl
Uitgevoerd door:	RWS, Dienst Verkeer en Scheepvaart
Review:	Projectteam WKS
Datum:	1 februari 2013
Status:	Definitief
Versienummer:	1.0

Aanpassingsoverzicht

Versie	Status	Datum	Gereviseerd door	Reden
0.1	Concept	24-okt-2012	H.Quakkelaar	Opzet
0.2	Concept	6-nov-2012	H.Quakkelaar	Aanbieden voor pre-peer-review
0.3	Concept	12-nov-2012	H.Quakkelaar	Pre-peer-review binnen specificatieteam
0.8	Concept	26-nov-2012	H.Quakkelaar	Peer-review verwerkt Verwerking IRAM-analyse. Verwerking "Top 10 beveiligingbeheersdoelen voor IA vs01"
0.81	Concept	7-dec-2012	H.Quakkelaar	Verwerking RWS-reviewcommentaar
0.82	Concept	7-dec-2012	H.Quakkelaar	Omzetting naar nieuw SSS template n.a. RWS-review
0.9	Concept	8-dec-2012	H.Quakkelaar	Gereed voor markt-review
0.91	Concept	19-dec-2012	H.Quakkelaar	Nagekomen RWS-opmerkingen verwerkt
0.92	Concept	21-dec-2012	H.Quakkelaar	Commentaar review marktpartijen verwerkt.
0.93	Concept	21-dec-2012	P. Boontje	MISD interface verplaatst naar IRS-IDD
1.0	Definitief	1-feb-2012	H. Quakkelaar	Timing-eisen BOA4.3-120, BOA4.3-130, BOA4.4-130, BOA4.4-140 in overleg met marktpartijen verruimd. Gereed voor WKS release 1.3

Inhoudsopgave

1. Scope

1.1 Identificatie

Dit document heeft de identificatie DVS.WKS.SSS.BOA.

Het beschrijft de eisen die gesteld worden aan "Beheer op Afstand voor wegkantsystemen", in dit document "BOA" genoemd.

De identificatie van eisen in dit document wordt voorafgegaan door de prefix "BOA".

1.2 Systeemoverzicht

1.2.1 Doel

Wegkantsystemen en de aangesloten periferie, zoals signaalgevers, worden beheerd door RWS-externe *beheerpartij*en. Iedere *beheerpartij* beheert een deel van het areaal. "Beheer Op Afstand" ("BOA") ondersteunt de *beheerpartij* door het mogelijk te maken een aantal operationele beheeractiviteiten *op afstand* uit te voeren, waarmee bezoeken aan de kast langs de wegkant worden verminderd.

Door beheer op afstand in een aantal situaties mogelijk te maken realiseert BOA de volgende doelstellingen:

a. verminderen van beheerkosten, doordat minder wegafzettingen en ritten van *operationeel beheerder*s nodig zijn;

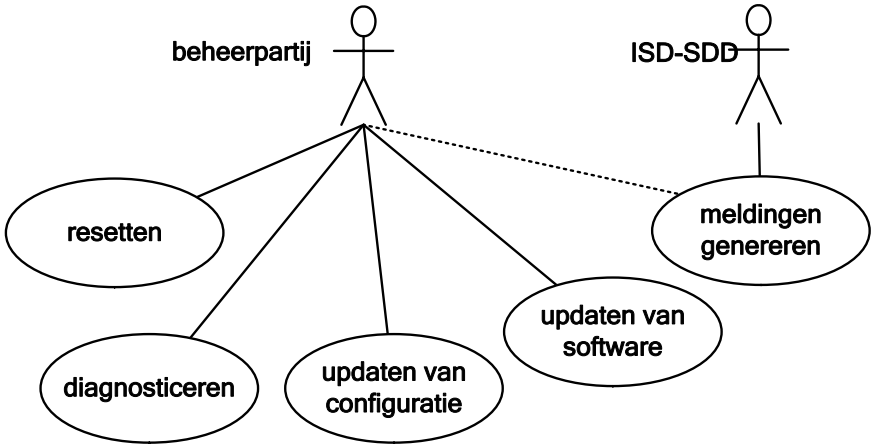
b. hogere beschikbaarheid van DVM-systemen, doordat functieverlies sneller gedetecteerd en opgelost kan worden;

c. verminderen van verkeershinder, doordat werkzaamheden sneller kunnen plaatsvinden en minder wegafzettingen nodig zijn.

De Rijkswaterstaat "ServiceDesk DVM" van de ISD ("ISD-SDD") is het meldpunt van alle storingen in DVM-systemen. "Beheer op Afstand" ("BOA") omvat ook het automatisch leveren van WKS-storingsmeldingen aan het MISD, het Meldingensysteem van de ISD, waarvan de ISD-SDD gebruik maakt.

De [BOA.OCD] beschrijft de context waarin BOA wordt gebruikt in meer detail.

1.2.2 Functies



Figuur 1 Beheer op afstand - actoren en functionaliteit

Binnen BOA wordt een aantal functies onderscheiden, die elk in het vervolg van deze specificatie worden uitgewerkt:

a. **meldingen genereren**
BOA bewaakt het functioneren van het WKS-areaal en genereert meldingen in geval dat er een storing wordt geconstateerd. Deze meldingen worden verstuurd naar het MISD ("Meldingensysteem van de ISD), zodat een ISD-SDD-medewerker actie kan ondernemen om de duur van het functieverlies te minimaliseren.
Optioneel worden deze meldingen ook naar de *beheerpartij* gestuurd. Hieraan worden in deze SSS geen eisen gesteld.

b. **diagnosticeren van storingen**
Zodra een storing is gedetecteerd moet de oorzaak hiervan worden achterhaald. Door middel van diagnose wordt productspecifieke statusinformatie en logdata opgehaald, en kunnen diagnostische tests worden uitgevoerd.

c. **resetten van (deel)systemen**
In een aantal gevallen kan een reset van een systeem of een functie een storing (tijdelijk) verhelpen. In deze gevallen is het noodzakelijk een nadere diagnose uit te voeren naar de oorzaak van de storing.

d. **updaten van configuratie**
De configuratie van een WKS is gebaseerd op de, voornamelijk, verkeerskundige configuratie van MTM en wordt aangevuld met WKS-leverancierspecifieke configuratiegegevens. Wijzigingen van verkeerskundige en systeemtechnische aard hebben vaak betrekking op alle WKS'en langs een bepaald traject. Via beheer op afstand kunnen deze snel worden doorgevoerd.

e. **updaten van software**
Gedurende de lifecycle van een WKS moet de software worden aangepast om functionele wijzigingen te realiseren en eventuele bugs te verwijderen. Beheer op afstand maakt het mogelijk deze updates snel en efficiënt te realiseren.

1.2.3 Systeemcontext

Beheer op afstand wordt gerealiseerd door een centraal toegankelijke *beheerfaciliteit* die communiceert met Wegkantstations. Uitgangspunt is dat iedere WKS-leverancier één

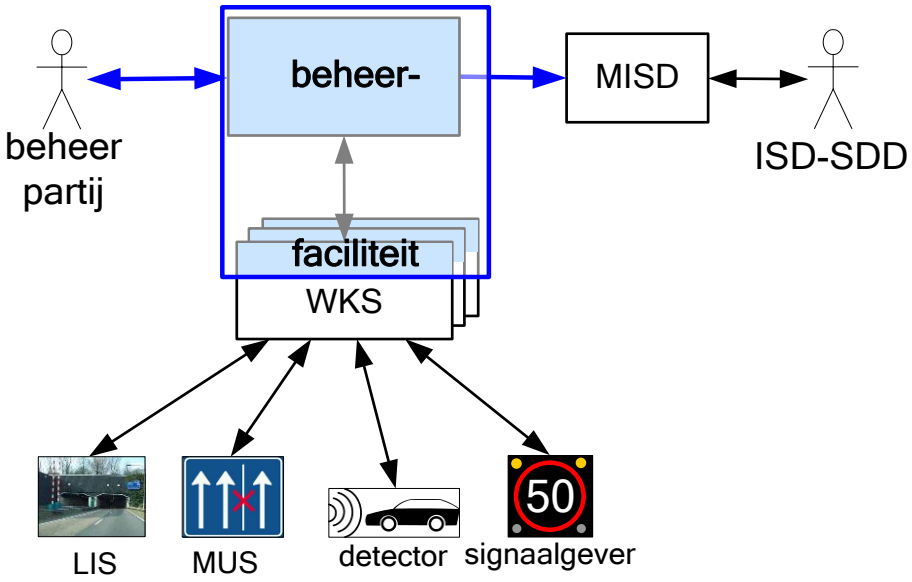
beheerfaciliteit levert waarmee het volledige operationele WKS-areaal[1] van die leverancier wordt beheerd.

Deze specificatie laat zich niet uit over de communicatie tussen WKS en *beheerfaciliteit*. Het is aan de leverancier van WKS en *beheerfaciliteit* om te bepalen welke beheerfunctionaliteit centraal, dan wel in een WKS langs de weg, wordt gerealiseerd en welke protocollen over RWSNet tussen centrale *beheerfaciliteit* en WKS'en worden gebruikt.

Deze SSS specificeert 2 groepen functionaliteit van de WKS *beheerfaciliteit*:

a. **Beheeracties** ten dienste van de *beheerpartij*. Het gaat hierbij om de volgende acties op het door de *beheerfaciliteit* beheerde WKS-areaal:
   - reset;
   - update van de configuratie;
   - update van de software dan wel firmware;
   - diagnosticeren van een of meerdere WKS'en.

b. **Meldingen** van het WKS-areaal aan het MISD. De *beheerfaciliteit* verzamelt storingsmeldingen en/of monitort de status van WKS'en en zendt op basis hiervan meldingen naar het MISD.



Figuur 2 Systeemoverzicht van beheer op afstand

Bij beheer op afstand is er interactie tussen 3 systemen:

a. **WKS**
   Op een *wegkantsysteem* (WKS) draaien één of meerdere *OS-applicatie*s die periferie, zoals signaalgevers en voertuigdetectoren, bewaken, aansturen en bevragen. Een *OS-applicatie* communiceert met de MTM-centrale, andere WKS'en, LIB/BIV-systemen en Monica.
   Communicatie ten behoeve van beheer op afstand vindt plaats tussen een WKS en de *beheerfaciliteit*. Het WKS ontvangt opdrachten voor beheeracties van de *beheerfaciliteit*. Omgekeerd stuurt het WKS diagnostische informatie aan de *beheerfaciliteit*.

[1] Met het "volledige areaal" wordt bedoeld alle WKS-systemen conform WKS-specificatie V1.3 of later.

b. *beheerfaciliteit*
De *beheerfaciliteit* is een centraal toegankelijk systeem, een geheel van centrale en decentrale apparaten en software waarmee, het WKS-areaal van een bepaalde WKS-leverancier wordt beheerd. De *beheerfaciliteit* maakt het de *operationeel beheerder* mogelijk *op afstand* beheeracties uit te voeren op een enkel WKS of een deelverzameling van het areaal. De *beheerfaciliteit* geeft de *beheerpartij* inzicht in de actuele toestand, statistieken en mogelijk trends m.b.t. tot het functioneren van het WKS en de periferie. De voor de ISD-SDD belangrijke gebeurtenissen worden door de *beheerfaciliteit* aan het MISD gemeld. Voor het totale WKS-areaal zullen in de praktijk meerdere *beheerfaciliteit*en, van verschillende leveranciers, actief zijn.

c. **MISD**
Het Meldingensysteem van de ISD ("MISD") is een landelijk centraal systeem dat storingsmeldingen ontvangt vanuit het gehele DVM-areaal, waaronder ook van de WKS-*beheerfaciliteit*. Het MISD ondersteunt de ISD-SDD-medewerker bij het analyseren, registreren en alloceren van problemen. Iedere (WKS-) *beheerfaciliteit* zal storingsmeldingen aan dit MISD verzenden.

1.3 Documentoverzicht

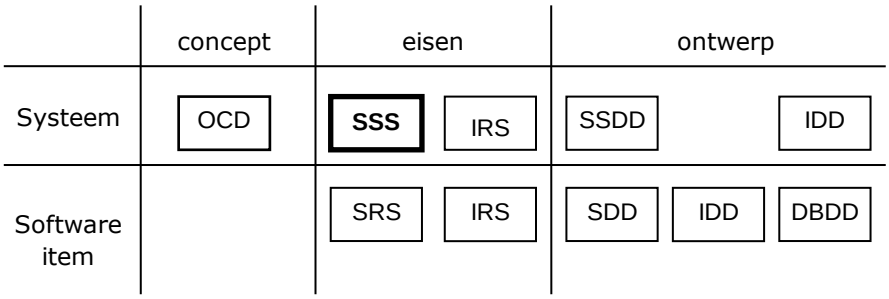
1.3.1 Doel van de SSS

Deze SSS, aangevuld met SSDD, wordt gebruikt als basis voor ontwerp en kwalificatietesten van een systeem of subsysteem.

De SSS definieert de systeemgrenzen en identificeert de externe interfaces. Ze beschrijft de kwaliteitseisen en de functionele eisen in termen van interactie van het systeem met diens omgeving.

1.3.2 Documentstructuur

De documentstructuur is opgezet en ingevuld conform de standaard J-STD-016 [J-STD-016]. In onderstaande figuur is aangegeven welke positie dit document inneemt in de documentstructuur.



Figuur 3 Documentstructuur

Hoofdstuk 1 geeft een overzicht van de inhoud en achtergronden van dit document.

Hoofdstuk 2 bevat een lijst van alle documenten die relevant zijn voor de inhoud van dit document en die op belangrijke punten aanvullende informatie kunnen leveren.

Hoofdstuk 3 bevat een overzicht van de belangrijkste eisen zoals op dit moment voor het WKS zijn geïdentificeerd.

Hoofdstuk 4 geeft inzicht in de kwalificatiebepalingen die aangeven of en zo ja, op welke wijze de leverancier dient aan te tonen dat aan de eisen wordt voldaan die in Hoofdstuk 3 geformuleerd zijn.

Hoofdstuk 5 geeft de herleidbaarheid aan van eisen ten opzichte van andere eisen. Dit hoofdstuk

wordt alleen ingevuld wanneer er sprake is van eisen die zijn afgeleid van bovenliggende eisen die eerder zijn geformuleerd in een ander document.

Hoofdstuk 6 beschrijft de in dit document gehanteerde afkortingen, acroniemen en termen.

1.3.3 Aanwijzingen voor het lezen

Daar waar in dit document *hij* of *zijn* als verwijzing naar een gebruiker voorkomt, moet dit worden gelezen als *hij* of *zij* en *zijn* of *haar*.

In dit document worden de gebruikte begrippen zoveel mogelijk in eisen geïntroduceerd. Een aantal eisen heeft daardoor een definiërend karakter.

Een verwijzing naar een ander document heeft de vorm [<doc>], waarbij "<doc> de referentie is die wordt geïntroduceerd in de paragrafen 2.1 en 2.1.2.

Verwijzingen naar andere specificaties hebben de vorm: "[doc:spec]". Een voorbeeld: [WKS.SSS:WKS.2.2.5-110] verwijst naar eis "WKS.2.2.5-110" van document [WKS.SSS].

Verwijzingen naar additionele maatregelen in de IRAM hebben de vorm: "[IRAM:AMx]", waarbij "x" het nummer is, waarmee de additionele maatregel in paragraaf 3.7 van [IRAM] wordt beschreven.

Termen worden verklaard in sectie 6.2 en zijn in de tekst gemarkeerd door de volgende tekststijl: *dit is een term*.

1.3.4 Notatiewijze van eisen

Dit document bevat eisen en begeleidende tekst. Eisen en hun herkomst zijn expliciet vermeld. Iedere eis is weergegeven in een kader met grijze achtergrondkleur dat de volgende informatie bevat:

1. Een unieke identificatie van de eis binnen de totale specificaties.
   De identificatie bestaat uit:
   a De eis prefix: zie paragraaf 1.1;
   b Het nummer van de paragraaf binnen hoofdstuk 3 (Eisen) waarin de eis is opgenomen met optioneel het nummer van de subparagraaf en optioneel het nummer van de sub-subparagraaf;
   c De eis prefix en de paragraafnummers worden gescheiden door een punt '.'
   d Een volgnummer van de eis binnen de aangeduide paragraaf, subparagraaf of sub-subparagraaf.

      Opeenvolgende eisen behoeven niet opeenvolgend genummerd te zijn. Verder kunnen nummers van eisen ontbreken, omdat als gevolg van het ontwikkelingsproces van de specificatie de betreffende eisen zijn komen te vervallen. Bovendien zijn de eisen zo genummerd dat steeds enkele eisen tussengevoegd kunnen worden zonder de volgnummering te verstoren.

      Het volgnummer wordt voorafgegaan door een minteken, '-'.

   Vervallen identificaties worden niet opnieuw gebruikt.
2. Een alias van de identificatie, bestaande uit de eis prefix en een aantal steekwoorden;
3. De formulering van de eis;
4. De herkomst van de eis;
5. Een toelichting op de eis in die gevallen waar dat verhelderend werkt;

6. De wijzigingshistorie: indien een eis wijzigingen ondergaat wordt onder historie aangegeven wat er in welke documentversie door wie wanneer is aangepast. De wijzigingshistorie wordt alleen in een eis opgenomen indien de eis ooit een wijziging heeft ondergaan.

Hieronder een voorbeeld van een eis met als unieke identificatie BOA.2.1-000, die zich dus in paragraaf 3.2.1 bevindt:

BOA.2.1-000	**boa.func.voorbeeld**
Eis:	Hier de ondubbelzinnige formulering van één eis.
Herkomst:	Hier de herkomst van de eis voor zover deze naar bestaande documenten is te herleiden.
Toelichting:	Hier eventuele toelichtingen en/of opmerkingen.
Historie:	Optioneel veld voor de wijzigingshistorie van de eis, indien van toepassing

1.3.5 Beveiliging en intellectueel eigendom

Het intellectueel eigendom van dit document en gerelateerde documenten en producten ligt bij Rijkswaterstaat.

2. Aangehaalde documenten

2.1 Normatieve documenten

2.1.1 Systeemdocumenten

Om dit document beter onderhoudbaar te maken zijn in onderstaande lijst documentversies zo veel mogelijk weggelaten. De release-notes van een bepaalde WKS-versie specificeren van elk van deze documenten de vigerende versie.

DocumentID	Omschrijving
BOA.OCD	Operationeel concept WKS beheer (op afstand)
BOA-MISD.IRS	WKS Specificatie Interface-Eisen BOA-MISD.
WKS.SB	Wegkantsysteem voor Signaleren en Monitoren – Systeembeschrijving - SB
WKS.SSS	Wegkantsysteem voor Signaleren en Monitoren – Systeem Specificatie - SSS
SG.IRS	Wegkantsysteem voor Signaleren en Monitoren – WKS-CS – Specificatie Interface-Eisen, IRS
CS.IRS	Wegkantsysteem voor Signaleren en Monitoren –Interface WKS – Signaalgever - Interface Requirements Specification & Design, IRS-IDD
CGGOSALL	Wegkantsysteem voor Signaleren en Monitoren – Onderstation/OS-applicatie configuratie CGGOSALL- Interface Requirements Specification & Design, IRS-IDD
NNV.AANSL	Nieuwe Netwerkvoorziening Verkeer en Waterstaat – aansluitvoorwaarden.

2.1.2 Standaarden

DocumentID	Omschrijving
VIC.WWPOL	Wachtwoordpolicy VICnet/SPITS, v1.0, 16-02-2005
DID.BB	Baseline Beveiliging DID, 20-04-2010, definitief
TOP10	Top 10 beveiligingsbeheersdoelen voor Industriële Automatisering, opgenomen in Bijlage A: Afdekking beveiligingseisen.
RFC4180	Common Format and MIME Type for Comma-Separated Values (CSV) Files, The Internet Society, October 2005

2.2 Informatieve documenten

DocumentID	Omschrijving
IRAM	IRAM - Risicoanalyse, Beheer op afstand - WKS 1.3, versie 1.0 Definitief, 12-dec-2012
[J-STD-016]	16:1995 Standard for Information Technology - Software Life Cycle Processes - Software development: Acquirer-Supplier Agreement

3. Eisen

3.1 Doel

Het primaire doel van beheer op afstand verwoord in paragraaf 1.2.1.

3.2 Uitgangspunten

Uitgangspunten die gehanteerd zijn bij het bepalen van de eisen:

a. De leverancier van de *beheerfaciliteit* is dezelfde als de leverancier van een WKS. Een beheersysteem werkt uitsluitend samen met WKS'en van dezelfde leverancier.

b. De *beheerpartij* die van de *beheerfaciliteit* gebruik maakt, maakt deel uit van dezelfde organisatie als de leverancier.

3.3 Randvoorwaarden

Randvoorwaarden die gehanteerd zijn bij het bepalen van de eisen:

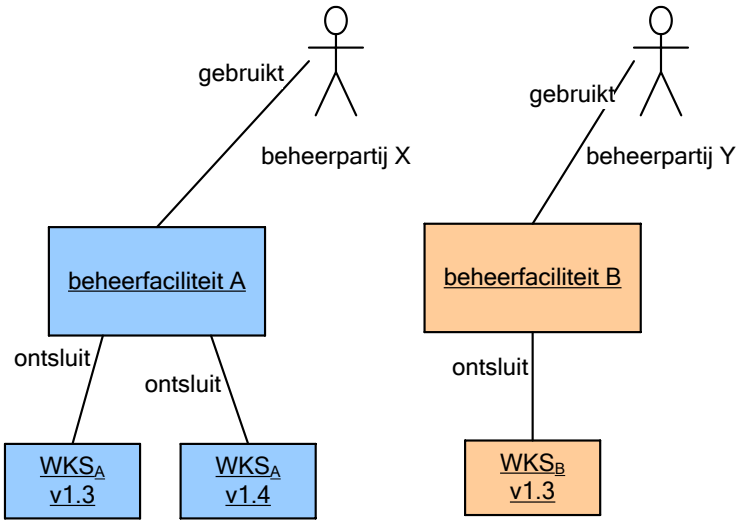
a. De bestaande functionaliteit van randapparatuur, zoals signaalgevers, wordt niet aangepast ten behoeve van beheer op afstand;

b. De bestaande architectuur van WKS, periferie en centrale systemen wordt niet aangepast ten behoeve van beheer op afstand.

3.4 Eisen t.a.v. systeemmogelijkheden (*capabilities*)

3.4.1 Algemene eisen beheerfaciliteit

De specificatie gaat uit van de huidige praktijk waarbij de WKS-leverancier tevens de *beheerpartij* is voor het WKS ("*boven de klemmenstrook*" in de WKS-kast inclusief detectorstation). Het hele WKS-areaal van een bepaalde leverancier wordt via één centraal toegankelijke *beheerfaciliteit* van die leverancier door de leverancier beheerd (zie Figuur 4).



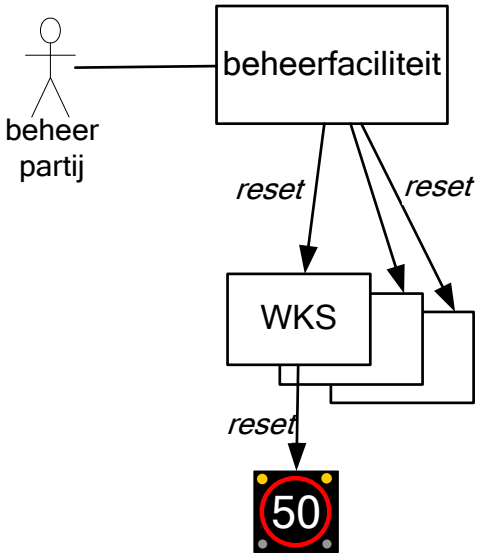
Figuur 4 Relatie tussen beheerfaciliteit, beheerpartij en WKS'en

BOA.4.1-010	**wks.boa.bhrfac.algemeen**
Eis:	Het WKS van een *leverancier* moet worden voorzien van één centrale *beheerfaciliteit* die een *beheerpartij* in staat stelt het gehele areaal van WKS'en van die *leverancier*, *op afstand* te beheren. Tot het areaal behoren tenminste alle WKS'en met versie 1.3 en hoger. WKS'en die onderdeel uitmaken van zogenaamde "DBFM"-contracten behoren niet tot het areaal.
Herkomst:	[BOA.OCD]
Toelichting:	- Deze eis is van toepassing op een WKS conform WKS-specificatie V1.3 en volgend. WKS'en conform oudere specificaties mogen ook door dezelfde faciliteit worden beheerd. - Het is dus niet toegestaan een *beheerfaciliteit* te leveren die specifiek is voor een bepaalde WKS-versie. - De *beheerfaciliteit* kan ook gebruikt worden voor WKS'en met een versie vóór 1.3. Dit wordt echter niet geëist.

BOA.4.1-030	**wks.boa.bhrfac.aansluitvoorwaarden**
Eis:	De *beheerfaciliteit* moet voldoen aan de NNV aansluitvoorwaarden [NNV.AANSL].
Herkomst:	[DID.BB:10.13-10]
Toelichting:	- De aansluitvoorwaarden stellen eisen aan een *beheerfaciliteit* zelf, de wijze van aansluiting van die faciliteit aan het RWSNet en aan de procedures rondom het gebruik van de faciliteit.

3.4.2 Remote reset

De *beheerfaciliteit* stelt de *beheerpartij* in staat om een of meerdere WKS'en of delen daarvan *op afstand* te resetten. Deze paragraaf legt de eisen vast die daaraan worden gesteld. Een reset op een operationeel WKS mag uitsluitend worden uitgevoerd met expliciete toestemming van Rijkswaterstaat.



Figuur 5 Reset van WKS en signaalgever

BOA.4.2-010	**wks.boa.reset.toestemming**
Eis:	Voordat een *operationeel beheerder* een WKS, een onderdeel daarvan, of een daaraan gekoppeld apparaat, reset, moet hiertoe expliciet toestemming zijn verleend door de verkeersleider.
Herkomst:	[BOA.OCD]
Toelichting:	-

BOA.4.2-100	**wks.boa.reset.besteenh.functie**
Eis:	De *beheerfaciliteit* stelt de *operationeel beheerder* in staat *op afstand* een *besturingseenheid* te herstarten.
Herkomst:	[BOA.OCD]
Toelichting:	-

BOA.4.2-105	**wks.boa.reset.besteenh.gedrag**
Eis:	Een herstart van een *besturingseenheid* omvat de volgende gedragingen in de gegeven volgorde: a. De *systeemsoftware* voert een clean shutdown uit. De *OS-applicatie*s worden gestopt, resources worden vrijgegeven en communicatieverbindingen opgezegd. Het systeem is mogelijk niet meer bereikbaar voor beheer op afstand. Mocht een "clean" shutdown niet mogelijk zijn dan moet een geforceerde shutdown worden uitgevoerd; b. De *systeemsoftware* wordt herstart. Het systeem is nu weer bereikbaar voor beheer op afstand; c. De op de *besturingseenheid* geconfigureerde *OS-applicatie*s worden alle herstart. Het systeem is weer vanuit te centrale aan te sturen.
Herkomst:	
Toelichting:	- Voor herstart van OS-applicaties zie "wks.boa.reset.os.functie".

BOA.4.2-110	**wks.boa.reset.os.functie**
Eis:	De *beheerfaciliteit* stelt de *operationeel beheerder* in staat *op afstand* een individuele *OS-applicatie* te herstarten.
Herkomst:	[BOA.OCD]
Toelichting:	

BOA.4.2-115	**wks.boa.reset.os.gedrag**
Eis:	Een herstart van een *OS-applicatie* omvat de volgende gedragingen: a. Tijdens de herstart verbreekt de *OS-applicatie* alle externe communicatieverbindingen inclusief die met periferie. b. Na de herstart i. is de *OS-applicatie* in de toestand "idle" [WKS.SSS; eis WKS.2.2.5-140]. ii. gedraagt de *OS-applicatie* zich zoals gespecificeerd is na koude start [WKS.SSS; eis WKS.2.2.5-142].
Herkomst:	[BOA.OCD]
Toelichting:	- Een reset van de *OS-applicatie* impliceert dat de aangestuurde signaalgevers hun verbinding verliezen en geen beeld (meer) tonen. - Ad a.: De eis betreft verbindingen op applicatieniveau. Het is mogelijk dat systeemsoftware nog steeds communicatieverbindingen met periferie onderhoudt.

BOA.4.2-130	**wks.boa.reset.sg.hard.functie**
Eis:	De *beheerfaciliteit* stelt de *operationeel beheerder* in staat *op afstand* de spanning van een individuele signaalgever tijdelijk te onderbreken, zodat de signaalgever een koude start uitvoert. De *operationeel beheerder* moet in staat zijn de duur van de spanningsonderbreking te bepalen.
Herkomst:	[BOA.OCD]

Toelichting:	- In de praktijk blijkt dat in sommige gevallen signaalgevers langdurig (> 15 minuten) spanningsloos gemaakt moeten worden om foutsituaties te resetten.

BOA.4.2-140	**wks.boa.reset.terugkoppeling**
Eis:	De *beheerfaciliteit* geeft de *operationeel beheerder* terugkoppeling of de reset-opdracht voor *besturingseenheid*, *OS-applicatie* of signaalgever wordt uitgevoerd of niet is geaccepteerd.
Herkomst:	specificatieteam
Toelichting:	- Een voorbeeld van een situatie waarin een reset-opdracht niet wordt geaccepteerd is als het WKS op dat moment niet via het netwerk te bereiken is.

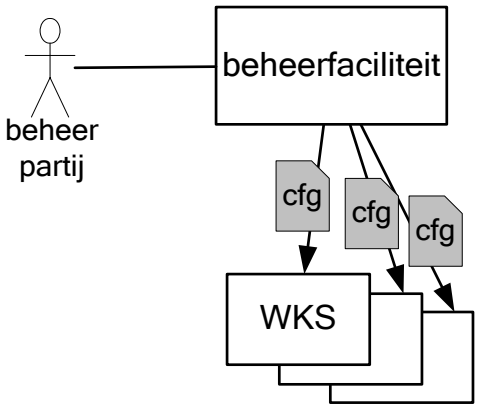
BOA.4.2-145	**wks.boa.reset.reactietijd**
Eis:	De *beheerfaciliteit* activeert een reset op een WKS of signaalgever binnen 5 seconden nadat de *operationeel beheerder* de opdracht heeft gegeven. De *beheerfaciliteit* geeft altijd terugkoppeling (zie eis BOA.4.2-140), binnen 5 seconden na het verstrekken van de opdracht. De genoemde reactietijden zijn exclusief vertragingen op het RWSNet.
Herkomst:	specificatieteam
Toelichting:	- Deze eis heeft geen betrekking op de duur van het resetten (afsluiten en weer opstarten) van het (sub-)systeem.

BOA.4.2-160	**wks.boa.reset.log.opdrachtsoort**
Eis:	De *beheerfaciliteit* logt de ontvangst van een resetopdracht conform eis BOA.10.2-020. Logging identificeert hierbij de volgende "opdrachtsoorten": a. herstart van een *OS-applicatie*; b. herstart van een *besturingseenheid*; c. herstart van een signaalgever; d. koude start van een signaalgever;
Herkomst:	BOA.10.2-010
Toelichting:	-

3.4.3 Remote configuratie-update

De configuratie van een WKS bepaalt het locatiespecifieke gedrag van de generieke WKS-software. De basis van de configuratie wordt gelegd door de CGGOSALL [CGGOSALL], die met name de verkeerskundige topologie (bijvoorbeeld de samenhang tussen verkeersstromen, rijstroken en signaalgevers op een raai) en verkeerskundige parameters vastlegt. Een *leverancier*specifieke configuratie bepaalt de technische aspecten, zoals de adressen van componenten en systeemparameters. Beide soorten configuratie worden in deze paragraaf bedoeld.

Configuratiewijzigingen worden doorgaans uitgevoerd op meerdere WKS'en tegelijkertijd, bijvoorbeeld op alle WKS'en langs een bepaald traject. Hierbij is het belangrijk dat de wijzigingen op deze WKS'en tegelijkertijd worden geactiveerd. In het geval dat er tijdens deze configuratiewijziging fouten worden ontdekt, bijvoorbeeld een WKS dat niet de nieuwste configuratie heeft geladen, dan kan de keuze worden gemaakt terug te schakelen naar de vorige configuratie voor de gehele "batch". Hierin moet de *beheerfaciliteit* ondersteunen.



Figuur 6 Configuratie-update van WKS'en

BOA.4.3-010	**wks.boa.cfupdate.toestemming**
Eis:	Voordat een *operationeel beheerder* de configuratie van een WKS wijzigt, moet hiertoe expliciet toestemming zijn verleend door de verkeersleider.
Herkomst:	[BOA.OCD]
Toelichting:	-

BOA.4.3-100	**wks.boa.cfgupdate.activeren**
Eis:	De *beheerfaciliteit* stelt de *operationeel beheerder* in staat *op afstand* een andere versie van de configuratie van een individuele *OS-applicatie* te activeren.
Herkomst:	[BOA.OCD]
Toelichting:	- Indien op een WKS meerdere *OS-applicatie*s actief zijn moet het dus mogelijk zijn de configuratie van één exemplaar te wijzigen. Een configuratiewijziging kan echter wel betrekking hebben op meerdere *OS-applicatie*s op één *besturingseenheid*.

BOA.4.3-140	**wks.boa.cfgupdate.voorwaarde**
Eis:	De *beheerfaciliteit* moet de opdracht tot het *op afstand* activeren van de configuratie van een *OS-applicatie* uitvoeren, onafhankelijk van de bedrijfstoestand van de *OS-applicatie*.

Herkomst:	
Toelichting:	- Ook in situaties dat er geen OS-applicatie draait of dat deze zich in fouttoestand bevindt, moet het laden van een configuratie mogelijk zijn.

BOA.4.3-101	**wks.boa.cfgupdate.resultaat**
Eis:	Na activering van zijn configuratie maakt de *OS-applicatie* gebruik van de nieuwe configuratiegegevens en is in de bedrijfstoestand "idle", zoals gespecificeerd in [WKS.SSS:WKS.2.2.5-141].
Herkomst:	[BOA.OCD]
Toelichting:	- Indien op een WKS meerdere *OS-applicatie*s actief zijn moet het dus mogelijk zijn de configuratie van één exemplaar te wijzigen. Een configuratiewijziging kan echter wel betrekking hebben op meerdere *OS-applicatie*s op één *besturingseenheid*.

BOA.4.3-105	**wks.boa.cfgupdate.identificatie**
Eis:	De versie van de configuratie van de *OS-applicatie* wordt geïdentificeerd door "OS-configuratienummer-in-OS", de identificatie uit CGGOSALL waarop de configuratie is gebaseerd. De beheerfaciliteit mag daarnaast ook andere identificaties voor de configuratie hanteren.
Herkomst:	[BOA.OCD]
Toelichting:	- De configuratie van een *OS-applicatie* omvat meer dan wat in de CGGOSALL is vastgelegd. Het is dus mogelijk de configuratie van een *OS-applicatie* aan te passen zonder dat "OS-configuratienummer-in-OS" wijzigt. Een identificatie naast de hier geëiste is voor een goed configuratiemanagement noodzakelijk.

BOA.4.3-110	**wks.boa.cfgupdate.activeren.expliciet**
Eis:	Een andere configuratie mag uitsluitend op een WKS worden geactiveerd door een specifieke opdracht hiertoe van de *beheerfaciliteit*.
Herkomst:	specificatieteam
Toelichting:	- Het wijzigen van configuratie zal over het algemeen batchgewijs plaatsvinden. Er kan enige tijd verstrijken tussen het laden van een configuratie en het activeren daarvan. Een tussentijdse reset (een voorbeeld van een opdracht) van een WKS mag dan niet leiden tot het activeren van deze configuratie op dat ene WKS. Dit sluit echter niet uit dat een reset mede noodzakelijk is om het activeren van een configuratie te bewerkstelligen. - Deze eis heeft geen betrekking op mogelijk aanwezige functionaliteit in een WKS om lokaal, langs de kant van de weg, de configuratie aan te passen.

BOA.4.3-120	**wks.boa.cfgupdate.activeren.doorlooptijd**
Eis:	De *beheerfaciliteit* stelt de *operationeel beheerder* in staat *op afstand* binnen 7,5 minuten 50 *OS-applicatie*s met een andere configuratie te activeren.
Herkomst:	specificatieteam

Toelichting:	- Deze eis betreft de doorlooptijd van het gelijktijdig activeren van configuraties, en niet op de tijd die nodig is om de configuraties te dirstribueren naar de WKS'en. Een fabrikant kan ervoor kiezen configuraties eerst te distribueren naar alle betrokken WKS'en en daarna pas te activeren. - Na een configuratiewijziging zal in veel gevallen een validatie op de weg plaatsvinden. Deze validatietijd valt ook buiten deze eis.

BOA.4.3-130	**wks.boa.cfgupdate.rollback**
Eis:	De *beheerfaciliteit* stelt de *operationeel beheerder* in staat *op afstand* binnen 15 minuten 50 *OS-applicatie*s met de vorige configuratie (te distribueren en) te activeren. Deze eis is niet recursief bedoeld; niet meer dan één vorige configuratie moet kunnen worden geactiveerd.
Herkomst:	specificatieteam
Toelichting:	- De rollback omvat zowel het eventueel opnieuw distribueren van de vorige versie als het activeren daarvan. Een *leverancier* kan ervoor kiezen de vorige versie in een WKS te handhaven zodat distributie niet nodig is. - Na een rollback zal in veel gevallen een validatie op de weg plaatsvinden. Deze validatietijd valt ook buiten deze eis.

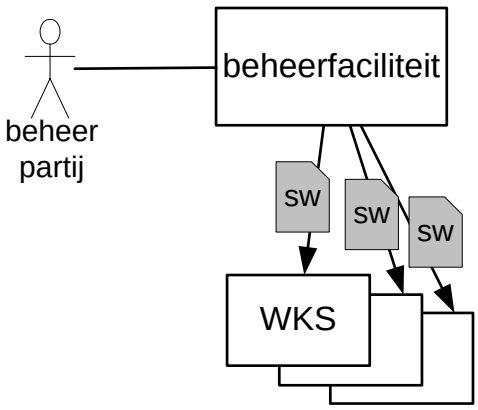
BOA.4.3-150	**wks.boa.cfgupdate.diagnostiek**
Eis:	De *beheerfaciliteit* is in staat de *operationeel beheerder*, op ieder moment, van elk WKS, de identificatie van de configuratie van de *OS-applicatie*, ter beschikking te stellen. De identificatie van de configuratie is gespecificeerd in eis BOA.4.3-105.
Herkomst:	specificatieteam
Toelichting:	- Afhankelijk van de implementatie, is deze informatie mogelijk niet beschikbaar indien de *beheerfaciliteit* geen verbinding heeft met het WKS waarover informatie wordt gevraagd.

BOA.4.3-160	**wks.boa.cfgupdate.log.opstarten**
Eis:	Bij het opstarten van een *OS-applicatie* op een WKS wordt de identificatie van de configuratie, door het WKS gelogd conform eis BOA.10.2-020. De identificatie van de configuratie is gespecificeerd in eis BOA.4.3-105.
Herkomst:	specificatieteam
Toelichting:	

3.4.4 Remote software-update

Door *op afstand* een software-update van een WKS te ondersteunen, wordt het eenvoudiger functionele wijzigingen in *applicatiesoftware* door te voeren en correcties aan te brengen in *systeem-* en *applicatiesoftware*.

Uitgangspunt van onderstaande eisen is dat software die in een WKS wordt geladen is gevalideerd. Hierdoor is de kans geminimaliseerd dat onjuist werkende software langs de weg wordt geladen.



Figuur 7 Software-update van WKS'en

BOA.4.4-010	**wks.boa.swupdate.toestemming**
Eis:	Voordat een *operationeel beheerder* de applicatie, of *systeemsoftware* van een WKS wijzigt, moet hiertoe expliciet toestemming zijn verleend door de verkeersleider.
Herkomst:	[BOA.OCD]
Toelichting:	-

BOA.4.4-020	**wks.boa.swupdate.validatie**
Eis:	Alvorens *applicatiesoftware* in een WKS te laden, moet deze door RWS zijn gevalideerd.
Herkomst:	[BOA.OCD]
Toelichting:	- Het RWS testcentrum voorziet in een validatieprocedure.

BOA.4.4-100	**wks.boa.swupdate.activeren.applic**
Eis:	De *beheerfaciliteit* stelt de *operationeel beheerder* in staat *op afstand* een andere versie van de *applicatiesoftware* op een WKS te activeren.
Herkomst:	[BOA.OCD]
Toelichting:	- Generieke *systeemsoftware* en eventuele middleware worden hier niet bedoeld. Zie hiervoor eis BOA.4.4-110. - Er wordt vanuit gegaan dat, indien meerdere *OS-applicatie*s actief zijn op hetzelfde WKS, alle dezelfde softwareversie hanteren.

BOA.4.4-105	**wks.boa.swupdate.applic.identificatie**
Eis:	*Applicatiesoftware* wordt geïdentificeerd door: a. de WKS-protocolversie en b. een versie-identificatie die de *applicatiesoftware* uniek identificeert.
Herkomst:	[BOA.OCD]
Toelichting:	- De WKS-protocolversie is de versie van de WKS-specificatie waaraan de *OS-applicatie* voldoet. In CGGOSALL terminologie wordt dit gegeven aangeduid met "protocolversie".

BOA.4.4-110	**wks.boa.swupdate.activeren.systeem**
Eis:	De *beheerfaciliteit* stelt de *operationeel beheerder* in staat *op afstand* de *systeemsoftware* op een WKS te voorzien van een update.
Herkomst:	[BOA.OCD]
Toelichting:	- Hier wordt generieke *systeemsoftware*, zoals een operating system, en eventuele middleware bedoeld. - Een belangrijk doel is op eenvoudige wijze beveiligingsupdates door te voeren.

BOA.4.4-120	**wks.boa.swupdate.activeren.expliciet**
Eis:	Bij wijziging van de versie van *applicatiesoftware* en/of *systeemsoftware* mag deze uitsluitend op een WKS worden geactiveerd op een door de *beheerfaciliteit* bepaald moment.
Herkomst:	specificatieteam
Toelichting:	- Het wijzigen van software zal over het algemeen batchgewijs plaatsvinden. Er kan enige tijd verstrijken tussen het laden van andere software en het activeren daarvan. Een tussentijdse reset (een voorbeeld van een opdracht) van een WKS mag dan niet leiden tot het activeren van deze software op dat ene WKS. Dit sluit echter niet uit dat een reset mede noodzakelijk is om het activeren van een softwareupdate te bewerkstelligen. - Bij installatie- of reparatiewerkzaamheden waarbij een "kaal" WKS wordt voorzien van de, voor die locatie, actuele software, is geen sprake van wijziging van software en geldt deze eis niet.

BOA.4.4-130	**wks.boa.swupdate.activeren.doorlooptijd**
Eis:	De *beheerfaciliteit* stelt de *operationeel beheerder* in staat *op afstand* binnen 120 minuten 50 WKS'en met een andere softwareversie te activeren.
Herkomst:	specificatieteam
Toelichting:	Deze eis betreft het gelijktijdig activeren van software-updates, en heeft geen betrekking op de tijd die nodig is om de software-updates te distribueren naar de WKS'en.

BOA.4.4-140	**wks.boa.swupdate.rollback**
Eis:	De *beheerfaciliteit* stelt de *operationeel beheerder* in staat *op afstand* binnen 120 minuten 50 WKS'en met de vorige softwareversie te activeren. Met "vorige softwareversie" wordt de laatste operationele versie op dat WKS. Deze eis is niet recursief bedoeld; niet meer dan één vorige softwareversie moet kunnen worden geactiveerd.
Herkomst:	specificatieteam
Toelichting:	- De rollback omvat zowel het eventueel opnieuw distribueren van de vorige versie als het activeren daarvan. Een *leverancier* kan ervoor kiezen de vorige versie in een WKS te handhaven zodat distributie niet nodig is.

BOA.4.4-150	**wks.boa.swupdate.laadprobleem**
Eis:	Het falen van het activeren van een andere versie van *applicatiesoftware*, noch *systeemsoftware* mag in geen geval leiden tot een situatie waarin het niet meer mogelijk is software *op afstand* te laden.
Herkomst:	specificatieteam
Toelichting:	

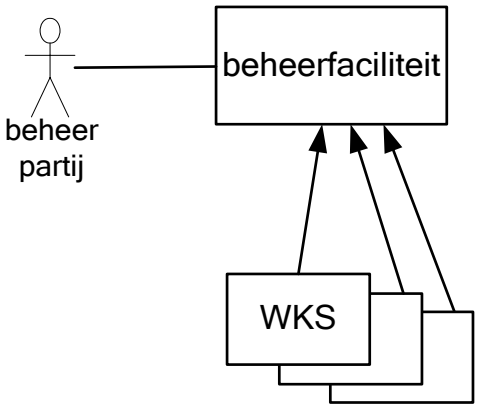
BOA.4.4-155	**wks.boa.swupdate.diagnostiek.appl**
Eis:	De *beheerfaciliteit* stelt de *operationeel beheerder* in staat op ieder moment van elke *OS-applicatie* de identificatie, volgens eis BOA.4.4-105 *op afstand* zichtbaar te maken.
Herkomst:	specificatieteam
Toelichting:	Software wordt per WKS geüpdate, versie van de software is per *OS-applicatie* opvraagbaar.

BOA.4.4-156	**wks.boa.swupdate.diagnostiek.syst**
Eis:	De *beheerfaciliteit* stelt de *operationeel beheerder* in staat op ieder moment de versies van *op afstand* uitwisselbare *systeemsoftware*componenten op een WKS *op afstand* zichtbaar te maken.
Herkomst:	specificatieteam
Toelichting:	- Bedoeling is inzichtelijk te maken welke versie(s) van *systeemsoftware*, inclusief evt. middleware, op een WKS aanwezig is. Met de term "uitwisselbaar" wordt verwezen naar het begrip "configuration item".

BOA.4.4-170	**wks.boa.swupdate.log.opstarten**
Eis:	Bij het opstarten van een *OS-applicatie* op een WKS wordt de identificatie van de software, volgens eis BOA.4.4-105, door op WKS-niveau gelogd conform eis BOA.10.2-020.
Herkomst:	specificatieteam
Toelichting:	

3.4.5 Remote Diagnose

Diagnostiek heeft tot doel om (dreigende) functiestoring te detecteren en, zodra functieverlies optreedt, de *beheerpartij*en in staat te stellen snel en adequaat een diagnose stellen.



Figuur 8 Diagnosticeren van WKS'en

Diagnosegegevens zijn in de twee groepen te verdelen:

a. Actuele status. Dit zijn (1) actuele statussen en (dreigende) storingen van functies, modules, (sub)systemen en periferie, en (2) identificatie- en configuratiegegevens van het areaal

b. Technische log: historische gegevens over het functioneren van de WKS'en en hun periferie.

Actuele status

Onderstaande eisen hebben betrekking op het diagnosticeren van de actuele status van WKS'en.

BOA.4.5-100	**wks.boa.diag.wks.functie**
Eis:	De *beheerfaciliteit* stelt de *operationeel beheerder* in staat *op afstand* elk individueel WKS te diagnosticeren.
Herkomst:	[BOA.OCD]
Toelichting:	Met "elk" WKS wordt elk WKS, vanaf versie 1.3, in het door de faciliteit beheerde areaal bedoeld.

BOA.4.5-120	**wks.boa.diag.componenten**
Eis:	De beheerfaciliteit moet van de volgende componenten diagnose *op afstand* bieden: a. *besturingseenheid*; b. *OS-applicatie*; c. signaalgever; d. voertuigdetector; e. MUS-bord; f. energievoorziening. Van elke component die in het veld hersteld of vervangen kan worden, moet diagnose *op afstand* beschikbaar zijn. De leverancier mag naast bovenstaande componenten diagnose *op afstand* van andere componenten mogelijk maken.
Herkomst:	specificatieteam
Toelichting:	- De componenten in bovenstaande lijst worden in de architectuur en specificaties van het WKS onderkend, zie [WKS.SB] en [WKS.SSS]. Dit zijn componenten die vervangen kunnen worden en die afzonderlijk aan een *beheerpartij* kan worden toegekend. - Met "signaalgever" worden rijstrooksignaalgever, argumentatiebord en tunnelsignaalgever bedoeld.

BOA.4.5-130	**wks.boa.diag.interfaces**
Eis:	De beheerfaciliteit moet van de volgende interfaces diagnose *op afstand* bieden: a. communicatie met CS; b. communicatie via VIV-C; c. communicatie via VIV-W; d. communicatie met Monica; e. communicatie met LIB en/of BIV. De leverancier mag naast bovenstaande interfaces diagnose *op afstand* van andere interfaces mogelijk maken.
Herkomst:	specificatieteam
Toelichting:	- Problemen met interfaces kunnen duiden op problemen met het netwerk zelf of het systeem waarmee wordt gecommuniceerd.

BOA.4.5-140	**wks.boa.diag.comp.dynamisch.gedrag**
Eis:	De *beheerfaciliteit* toont de *operationeel beheerder* op ieder gewenst moment of elk van componenten in eis BOA.4.5-120BOA.4.5-120BOA.4.5-120 al dan niet correct functioneert. Hierbij geldt: a. De gepresenteerde status van de componenten signaalgever, voertuigdetector en MUS-bord is gebaseerd op de informatie die het WKS via de gespecificeerde protocollen inwint. b. Ten aanzien van de component besturingseenheid moet minimaal zichtbaar zijn of de component voor beheer op afstand correct communiceert. c. Ten aanzien van de component energievoorziening moet minimaal zichtbaar zijn of het WKS gebruik maakt van noodvoeding of netvoeding. d. De gepresenteerde status mag daarbij niet meer dan 5 minuten op de daadwerkelijke status van de componenten achterlopen.
Herkomst:	[BOA.OCD]
Toelichting:	- De gespecificeerde maximale vertraging is de maat voor actualiteit van de gegevens. Op deze manier beschikt de beheerder over dezelfde gegevens als de ISD. - Met een "gespecificeerd protocol" wordt het binnen WKS gespecificeerde protocol tussen WKS en die componenten bedoeld.

BOA.4.5-145	**wks.boa.diag.if.dynamisch.gedrag**
Eis:	De *beheerfaciliteit* maakt aan de *operationeel beheerder* op ieder moment inzichtelijk of elk van de in eis BOA.4.5-130 genoemde interfaces al dan niet correct functioneert. De gepresenteerde status mag daarbij niet meer dan 5 minuten op de daadwerkelijke status van de componenten achterlopen.
Herkomst:	[BOA.OCD]
Toelichting:	- Zie toelichting bij eis BOA.4.5-140.

BOA.4.5-150	**wks.boa.diag.identificatie**
Eis:	De *beheerfaciliteit* moet iedere in eis BOA.4.5-120 onderkende component met de in [CGGOSALL] gegeven identifier identificeren. De *beheerfaciliteit* mag daarnaast aan een component een andere identificatie toekennen.
Herkomst:	[BOA.OCD]
Toelichting:	-

Logging

Onderstaande eisen hebben betrekking op loggegevens van zowel beheerfaciliteit als van WKS'en.

BOA.4.5-160	**wks.boa.diag.logging.inzien**
Eis:	De *beheerfaciliteit* moet de *operationeel beheerder* de mogelijkheid bieden de loggegevens van de *beheerfaciliteit*, inclusief die met betrekking tot elk WKS, *op afstand* in te zien. De loggegevens die ter beschikking worden gesteld omvatten minimaal de volgende: a. auditlogging van de beheerfaciliteit, zoals geëist in eis BOA.10.2-010; b. auditlogging op WKS-niveau, zoals geëist in eis BOA.10.2-012; c. storingslog op WKS-niveau, zoals geëist in eis BOA.4.5-190; d. WKS-logging zoals geëist in eis [WKS.SSS:WKS.2.2.2-020].
Herkomst:	[BOA.OCD]
Toelichting:	- Zie ook eis **Fout! Verwijzingsbron niet gevonden.**.

BOA.4.5-180	**wks.boa.diag.logging.export**
Eis:	De *beheerfaciliteit* moet de *operationeel beheerder* de mogelijkheid bieden loggegevens op WKS-niveau te exporteren naar CSV-formaat.
Herkomst:	[BOA.OCD]
Toelichting:	- Dit maakt het mogelijk voor een andere partij, met name RWS, de logging van een WKS te analyseren, bijvoorbeeld ten behoeve van audits. - Zie sectie 3.5.2 voor de specificatie van CSV-formaat

BOA.4.5-190	**wks.boa.diag.logging.storing**
Eis:	Het optreden van een storing, zoals gespecificeerd in eis BOA.4.5-140 en eis BOA.4.5-145, moet door het WKS worden gelogd.
Herkomst:	specificatieteam
Toelichting:	-

BOA.4.5-195	**wks.boa.diag.logging.storing.retentie**
Eis:	Een storingsloggegeven conform eis BOA.4.5-190 moet minimaal 5 dagen na het genereren van het gegeven bewaard blijven, ongeacht spanningsuitval of herstart in deze periode.
Herkomst:	specificatieteam
Toelichting:	- Deze specificatie stelt geen eisen aan de locatie waar de logging wordt bewaard.

3.5 Systeem externe interface-eisen

3.5.1 Interface met Meldingensysteem (EIF_BOA_MISD)

Deze paragraaf beschrijft de functionele eisen aan de interface tussen de beheerfaciliteit en het MISD ("Meldingensysteem van de ISD"). Deze interface wordt geïdentificeerd als "EIF_BOA-MISD".

De functionele en niet-functionele eisen met betrekking tot deze interface staan vermeld in [BOA-MISD.IRS], eisen beginnend met "IMISD.4".

3.5.2 CSV export (EIF_BOA_CSV)

Een aantal eisen in deze specificatie vereist de export van gegevens in naar een bestand waarin de gegevens volgens CSV-formaat zijn opgeslagen. Deze sectie specificeert de eisen die aan dit formaat worden gesteld.

BOA.5.2-010	**wks.boa.csv.formaat**
Eis:	De *beheerfaciliteit* exporteert gegevens in CSV-formaat volgens [RFC4180] en voldoet aan de volgende eisen: a. de eerste regel bevat een aanduiding van de inhoud van elke kolom. Dit wordt in [RFC4180] aangeduid met de "header"; b. In plaats van de in [RFC4180] genoemde "comma" mag ook de "semicolon", ";" code "%x3B", worden gebruikt.
Herkomst:	specificatieteam
Toelichting:	-

3.6 Systeem interne interface-eisen

BOA.6-010	**wks.boa.netwerk**
Eis:	De centrale *beheerfaciliteit* moet voor beheer *op afstand* communiceren met WKS'en uitsluitend via RWSNet.
Herkomst:	[TOP10:4.2]
Toelichting:	- Het is niet toegestaan een WKS *op afstand* te beheren via een eigen netwerk, zoals een draadloos netwerk.

3.7 Eisen ten aanzien van de interne gegevens van het systeem

Er worden geen eisen gesteld aan de interne gegevens van de *beheerfaciliteit*.

3.8 Eisen t.a.v. localisatie

Er worden geen eisen gesteld t.a.v. localisatie van de *beheerfaciliteit*.

3.9 Veiligheidseisen

BOA.9-010	**wks.boa.veilig**
Eis:	De *beheerfaciliteit* mag het verkeerskundige functioneren van WKS'en niet beïnvloeden, tenzij dit anders is gespecificeerd in dit document.
Herkomst:	specificatieteam
Toelichting:	- Voorbeeld van een beïnvloeding die is gespecificeerd in dit document: een reset van een OS-applicatie via BOA. - Ander voorbeeld: uitval van de beheerfaciliteit mag niet leiden tot uitval van een verkeerskundige functie.

3.10 Eisen t.a.v. beveiliging en privacybescherming

3.10.1 Beveiliging Beheerfaciliteit

Uitgangspunt van deze specificatie is dat de organisatie en processen van de *beheerpartij* voldoen aan de "Aansluitvoorwaarden NNV" [NNV.AANSL]. Deze specificatie legt eisen vast die gesteld worden aan de *beheerfaciliteit*, d.w.z. het fysieke systeem.

BOA.10.1-010	**wks.boa.bev.bhrfac.autorisatie**
Eis:	De *beheerfaciliteit* moet zijn functionaliteit uitsluitend voor geautoriseerde gebruikers toegankelijk maken.
Herkomst:	specificatieteam
Toelichting:	-

BOA.10.1-020	**wks.boa.bev.bhrfac.autorisatie.rollen**
Eis:	De *beheerfaciliteit* moet een aantal gebruikersrollen onderscheiden: a. operationeel (WKS-)beheerder; De *operationeel beheerder* voert beheeracties uit op WKS'en, zoals reset, configuratieupdate en diagnose, waaronder het opvragen loggegevens; b. faciliteitbeheerder; De faciliteitbeheerder beheert de *beheerfaciliteit* zelf. Zij is onder andere verantwoordelijk voor het onderhoud van de lijst van gebruikers, de lijst van de te beheren WKS'en, het exporteren van auditlogfiles en het instandhouden van de computersystemen, *systeemsoftware* en netwerk waarvan de *beheerfaciliteit* gebruik maakt. De *beheerfaciliteit* stelt aan een rol uitsluitend die functies ter beschikking die nodig zijn om die rol uit te voeren.
Herkomst:	[IRAM:AM17], [DID.BB:7.2-8]
Toelichting:	- Deze eis specificeert de verplichte rollen. Een beheersysteem mag een fijnmaziger autorisatieschema implementeren, mits de verplichte groepen aanwezig zijn. Zo kan het operationeel beheer worden opgedeeld in een rol die diagnosticeert en een rol die ook mag ingrijpen op een WKS. Binnen faciliteitbeheer is een onderverdeling in technisch beheer en applicatiebeheer gangbaar.

BOA.10.1-025	**wks.boa.bev.bhrfac.authen.functiescheiding**
Eis:	Eenzelfde persoon mag niet zowel operationeel beheerder als faciliteitbeheerder zijn.
Herkomst:	[DID.BB:7.2-8]
Toelichting:	- Kans op misbruik moet worden beperkt.

BOA.10.1-040	**wks.boa.bev.bhrfac.authen.persoonlijk**
Eis:	Iedere gebruiker van de *beheerfaciliteit* heeft een persoonsgebonden account die terug te voeren is tot die persoon.
Herkomst:	[DID.BB:11.7-1]

Toelichting:	- Iedere actie moet terug te voeren zijn op één natuurlijke persoon. Zie ook eis BOA.10.2-010.

BOA.10.1-050	**wks.boa.bev.bhrfac.authen.sterk**
Eis:	De *beheerfaciliteit* moet in het aanlogproces door gebruikers voldoen aan: a. *2-factor authenticatie*, en b. het gebruik van passwords conform [VIC.WWPOL].
Herkomst:	[TOP10:2.3], [BOA.10.1-010], [IRAM:AM10], [DID.BB:10.3-9], [DID.BB:10.13-2]
Toelichting:	-

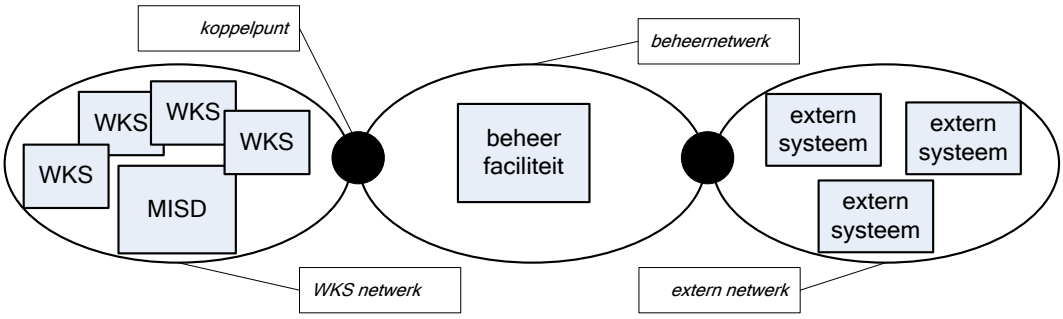
BOA.10.1-055	**wks.boa.bev.bhrfac.authen.versleuteld**
Eis:	De *beheerfaciliteit* moet authenticatiegegevens uitsluitend versleuteld opslaan en verzenden. De versleutelingstechniek moet gebaseerd een publiek algoritme dat gebruik maakt van asymmetrische sleutels en een vergelijkbare beveiliging biedt als een 2048-bit RSA sleutel.
Herkomst:	[DID.BB:11.4-1], [DID.BB:11.5-9]
Toelichting:	- Een voorbeeld van zo'n algoritme is RSA.

BOA.10.1-100	**wks.boa.bhrfac.segmentatie**
Eis:	Systemen waaruit de *beheerfaciliteit* van een *leverancier* is opgebouwd, moeten zijn ondergebracht in een separaat netwerksegment dat gecontroleerde toegang verleent tot het netwerksegment waarin de te beheren WKS'en zijn aangesloten.
Herkomst:	[IRAM:AM1]
Toelichting:	- Kwetsbaarheden worden geïsoleerd; hack-aanvallen, virussen en andere malware hebben zo een beperkte invloed op de omgeving. - Deze eis is verder uitgewerkt in onderstaande eisen.

BOA.10.1-120	**wks.boa.bev.netw.koppelpunt.wks**
Eis:	De communicatie tussen de *beheerfaciliteit* en het netwerk waarin de WKS-en zijn opgenomen verloopt via een centraal, beveiligd koppelpunt. Dit koppelpunt beperkt de communicatie tot die communicatieverbindingen a. waarvan het protocol in het ontwerp van de *beheerfaciliteit* is geïdentificeerd; b. met WKS'en behorende tot het te beheren areaal. Het koppelpunt kan daarnaast nog andere veiligheidsmaatregelen implementeren.
Herkomst:	[DID.BB:11.2-1, 11.2-2]
Toelichting:	- Zie Figuur 9 - Een voorbeeld van andere veiligheidsmaatregelen is het loggen en rapporteren van bepaalde communicatiegebeurtenissen.

BOA.10.1-130	**wks.boa.bev.netw.koppelpunt.extern**
Eis:	De communicatie tussen *beheerfaciliteit* en systemen bij de *beheerpartij* of daarbuiten verloopt via een centraal, beveiligd koppelpunt. Dit koppelpunt beperkt de communicatie tot die communicatieverbindingen a. waarvan het protocol in het ontwerp van de *beheerfaciliteit* is geïdentificeerd; b. met externe systemen die geautoriseerd zijn. c. van geautoriseerde gebruikers Het koppelpunt kan daarnaast nog andere veiligheidsmaatregelen implementeren.
Herkomst:	[DID.BB:11.2-1, 11.2-2, 10.13-16]
Toelichting:	- Zie Figuur 9 - ad c. De toetsing of een gebruiker geautoriseerd is kan door het koppelsysteem zelf worden uitgevoerd, bijv. in geval van een RAS-verbinding. In andere gevallen wordt dit geborgd door het geautoriseerde externe systeem en de daaraan gerelateerde operationele veiligheidsprocedures.

BOA.10.1-140	**wks.boa.bev.netw.ander**
Eis:	Er mag geen koppeling bestaan tussen *beheerfaciliteit* en een ander netwerk anders dan via de gespecificeerde koppelpunten (zie eisen BOA.10.1-120 en BOA.10.1-130).
Herkomst:	[TOP10:4.1]
Toelichting:	



Figuur 9 Netwerken en koppelpunten

BOA.10.1-200	**wks.boa.bev.bhrfac.malware**
Eis:	Systemen waaruit de *beheerfaciliteit* is opgebouwd, moeten a. zijn opgenomen in procedures b. en, indien het voor *beheerfaciliteit* gebruikte platform dit mogelijk maakt, zijn voorzien van middelen ter voorkoming en bestrijding van malware. Aangetroffen malware wordt vastgelegd in de securitylog.
Herkomst:	[IRAM:AM11], [DID.BB:10.6-4], [DID.BB:12.12-13]
Toelichting:	- Zowel tijdens ontwerp als exploitatie van de beheerfaciliteit is een veiligheidsbeleid ter voorkoming en bestrijding van malware.

BOA.10.1-210	**wks.boa.bev.bhrfac.patches**
Eis:	Beveiligingsupdates en patches t.b.v. systemen waaruit de *beheerfaciliteit* is opgebouwd, moeten volgens een, in de beheerorganisatie geborgde, procedure worden gesignaleerd en aangebracht. Deze procedure conformeert zich aan het patchbeleid van Rijkswaterstaat.
Herkomst:	[DID.BB:12.7]
Toelichting:	- Het patchbeleid van Rijkswaterstaat is, op het moment van schrijven van deze SSS, in ontwikkeling.

BOA.10.1-300	**wks.boa.bev.bhrfac.benoemd**
Eis:	De *beheerfaciliteit* moet voor en tijdens uitvoering van een beheeractiviteit aan de *operationeel beheerder* zichtbaar maken op welk(e) WKS('en) of sub-systeem de actie betrekking heeft.
Herkomst:	specificatieteam
Toelichting:	- Dit is een maatregel om te voorkomen dat een actie op een verkeerd WKS, *OS-applicatie* etc., wordt uitgevoerd.

BOA.10.1-400	**wks.boa.bev.bhrfac.fysiek**
Eis:	Fysieke toegang tot systemen waaruit de *beheerfaciliteit* is opgebouwd, moet uitsluitend voor hiertoe geautoriseerde personen mogelijk zijn.
Herkomst:	specificatieteam
Toelichting:	- De *leverancier* c.q. *beheerpartij* moet maatregelen treffen om de fysieke toegang tot de *beheerfaciliteit* te beperken tot die personen voor wie toegang op basis van hun functie, noodzakelijk is.

BOA.10.1-450	**wks.boa.bev.hardened**
Eis:	De *beheerfaciliteit* moet bestaan uit "hardened" systemen en netwerkcomponenten. Hardening omvat ingrepen in een computersysteem waarbij overbodige functies in het besturingssysteem zijn uitgeschakeld, om het systeem veiliger maken. Op een hardened systeem: a. draaien uitsluitend services die voor het functioneren en beheer noodzakelijk zijn; b. hebben alleen die gebruikers toegang die nodig zijn voor het utvoeren van de functionaliteit en het beheer van het systeem; c. zijn uitsluitend fysieke poorten en netwerkpoorten toegankelijk die voor het functioneren en beheer noodzakelijk zijn.
Herkomst:	[IRAM:AM4], [DID.BB:12.12-5], [DID.BB:12.12-11]
Toelichting:	- Deze eis geldt ook ten aanzien van beheerfunctionaliteit die wordt gerealiseerd op een wegkantstation. -

BOA.10.1-500	**wks.boa.bev.bhrfac.incidentproc**
Eis:	De *beheerpartij* heeft een geborgde procedure voor het melden, registreren en rapporteren van beveiligingsincidenten met betrekking tot *beheerfaciliteit*, de gerelateerde infrastructuur en processen. Deze procedure omvat minimaal het volgende: a. criteria voor en wijze van melden van beveiligingsincidenten; b. incidentrapportage aan RWS; c. wijze van afhandeling van beveiligingsincidenten; d. beveiligingsincidenten worden centraal vastgelegd; e. de incidentmanager bewaakt de voorgang van de incidentafhandeling; f. een incidentmanager ziet toe op naleving van de procedure g. wijze van voortgang van de dienstverlening aan RWS bij het op treden van een beveiligingsincident.
Herkomst:	[DID.BB:10.23]
Toelichting:	-

3.10.2 Logging door beheerfaciliteit

Beheeractiviteiten die van invloed kunnen zijn op het verkeerskundige gedrag van WKS'en moeten worden gelogd en kunnen door RWS worden opgevraagd.

BOA.10.2-010	**wks.boa.bhrfac.auditlog.functie**
Eis:	De *beheerfaciliteit* moet activiteiten van *operationeel beheerders*, beheerders van de *beheerfaciliteit*, uitzonderingen en informatiebeveiligingsgebeurtenissen vastleggen in een auditlog. Tenminste de volgende soorten activiteiten moeten worden gelogd: a. het ingrijpen door een *operationeel beheerder* op het functioneren van één of meerdere WKS-en; b. het succesvol aanloggen op de *beheerfaciliteit* c. het niet succesvolle aanloggen op de *beheerfaciliteit*; d. het afloggen van de *beheerfaciliteit* e. het wijzigen van configuratie van de *beheerfaciliteit*; f. het wijzigen van de software van de *beheerfaciliteit*;
Herkomst:	[DID.BB:10.10-1], [DID.BB:11.7-9]
Toelichting:	- Achtergrond: ingrepen op een WKS, zoals reset en configuratie-update, moeten traceerbaar zijn. Dit geldt ook voor ingrepen op de *beheerfaciliteit* zelf. - Voorbeelden van ingrijpen op het functioneren van een WKS zijn: een reset van een signaalgever en een software update.

BOA.10.2-012	**wks.boa.wks.auditlog.functie**
Eis:	Het wegkantstation moet activiteiten van *operationeel beheerders*, uitzonderingen en informatiebeveiligingsgebeurtenissen vastleggen in een auditlog. Tenminste de volgende soorten activiteiten moeten worden gelogd: a. het ingrijpen door een *operationeel beheerder* op het functioneren van het WKS; en, indien van toepassing: b. het succesvol aanloggen op het WKS; c. het niet succesvol aanloggen op het WKS; d. het afloggen van het WKS;
Herkomst:	[DID.BB:10.10-1], [DID.BB:11.7-9]
Toelichting:	- Logging moet door het wegkantstation gebeuren, echter de gelogde gegevens kunnen elders, bijv. op een centrale logserver, worden vastgelegd. - Opvragen van diagnostische informatie heeft geen impact op de verkeerskundige functionaliteit en hoeft derhalve niet te worden gelogd. - Voorbeelden van ingrijpen op het functioneren van een WKS zijn: reset van een *OS-applicatie*, update van de software, update van de configuratie, en het stoppen van de *OS-applicatie*.

BOA.10.2-015	**wks.boa.bhrfac.auditlog.export**
Eis:	De *beheerfaciliteit* moet de applicatiebeheerder van de *beheerfaciliteit* de mogelijkheid bieden de auditlog te exporteren naar CSV-formaat.
Herkomst:	specificatieteam

Toelichting:	- Dit maakt het mogelijk voor de *beheerpartij* en RWS de logging van een WKS te analyseren, bijvoorbeeld ten behoeve van audits. - Zie sectie 3.5.2 voor de specificatie van CSV-formaat

BOA.10.2-020	**wks.boa.bhrfac.auditlog.inhoud**
Eis:	Van een beheeropdracht moet minimaal de volgende informatie worden gelogd: a) Soort opdracht b) Het tijdstip waarop de opdracht is gegeven. c) Identificatie van de persoon die de opdracht heeft gegeven. d) Identificatie van het doelsysteem waarop de opdracht betrekking heeft. e) Het resultaat van de beheeropdracht; hierbij moet minimaal aangegeven zijn of de opdracht is uitgevoerd of niet.
Herkomst:	[DID.BB:11.7-9]
Toelichting:	- Van welke beheeropdrachten een log moet worden gemaakt is gespecificeerd in eis BOA.10.2-010 - Het doelsysteem kan één of meerdere WKS'en of de *beheerfaciliteit* zelf zijn.

BOA.10.2-021	**wks.boa.bhrfac.auditlog.inhoud.persoon**
Eis:	Identificatie van personen in de auditlog moet op individuen terug te voeren zijn en niet bijvoorbeeld op een team. Dit geldt voor de duur van de log-retentieperiode (zie eis BOA.10.2-030)
Herkomst:	[DID.BB:11.7-9]
Toelichting:	- Dit betekent bijvoorbeeld dat ook personen die uit dienst zijn gedurende de log-retentieperiode geadministreerd moeten blijven.

BOA.10.2-030	**wks.boa.bhrfac.auditlog.retentie**
Eis:	Auditloginformatie moet minimaal 3 maanden na vastlegging bewaard blijven.
Herkomst:	[DID.BB:10.10-14]
Toelichting:	-

BOA.10.2-040	**wks.boa.bhrfac.auditlog.integriteit**
Eis:	De auditlog mag door geen enkele gebruiker van de *beheerfaciliteit* worden gewijzigd. Technische maatregelen verhinderen dat een *operationeel beheerder* informatie van de auditlog kan wijzigen of verwijderen.
Herkomst:	[IRAM:AM14]
Toelichting:	- De essentie van deze logging is traceerbaarheid van WKS-beheeractiviteiten. Deze informatie moet betrouwbaar zijn. - De geëiste technische maatregelen zijn een aanscherping van de algemene eis dat auditloggegevens niet mogen worden gewijzigd.

BOA.10.2-050	**wks.boa.bhrfac.auditlog.sync**
Eis:	Tijdstempels in de auditlog van beheerfaciliteit en alle WKS'en moet zijn gebaseerd op klokken die minder dan 0,1 seconde van elkaar verschillen.
Herkomst:	specificatieteam
Toelichting:	- Voor analyses is het noodzakelijk over de exacte volgorde van activiteiten te kunnen beschikken. - Binnen RWSNet is NTP als dienst beschikbaar. Deze moet over het algemeen wel worden aangevraagd.

3.10.3 Beveiliging WKS

BOA.10.3-010	**wks.boa.wks.autorisatie**
Eis:	Een WKS moet uitsluitend beheeropdrachten accepteren die afkomstig zijn van een geautoriseerde *beheerfaciliteit*. De authenticatiegegevens waarmee een *beheerfaciliteit* zich bij een WKS identificeert moeten *op afstand* te wijzigen zijn.
Herkomst:	[TOP10:2.1], [DID.BB:10.13-3]
Toelichting:	- Deze validatie moet door (software op) de *besturingseenheid* plaatsvinden, zodat personen/applicaties die toegang hebben tot het RWS-netwerk niet ook mogelijkerwijs toegang hebben tot bijv. de reset-functionaliteit. - Onder beheeropdrachten worden alle opdrachten bedoeld in het kader van de in dit document gespecificeerde *beheerfaciliteit*. Het betreft: reset, software update, configuratie update, diagnose en (MISD) meldingen. - De methode van authenticatie en autorisatie is aan de leverancier.

BOA.10.3-020	**wks.boa.wks.autorisatie.log.functie**
Eis:	Een WKS logt de volgende informatiebeveiligingsgebeurtenissen: a. elke poging tot het geven van een opdracht die niet afkomstig is van een geautoriseerde bron (zie eis BOA.10.3-010) is.
Herkomst:	[TOP10-6.1]
Toelichting:	- De *beheerpartij* moet deze kunnen rapporteren aan RWS.

BOA.10.3-030	**wks.boa.wks.autorisatie.log.inhoud**
Eis:	Van elke autorisatiegebeurtenis worden minimaal de volgende gegevens gelogd: a. tijdstip van de poging b. IP-adres waarvandaan poging werd gedaan
Herkomst:	[IRAM:AM14]
Toelichting:	-

3.10.4 Privacybescherming

De *beheerfaciliteit* bevat geen persoonsgegevens anders dan die van gebruikers. Privacybescherming van die gegevens is aan de beheerpartij. Hieraan worden door RWS geen eisen gesteld.

3.11 Omgevingseisen

Er worden geen eisen gesteld aan de omgeving waarin *beheerfaciliteit* zal opereren. Uitgangspunt is dat dit een standaardomgeving is, bijvoorbeeld een computerruimte.

3.12 Resource-eisen

3.12.1 Eisen t.a.v. computerhardware

Er worden geen eisen gesteld aan de computerhardware van de *beheerfaciliteit*.

3.12.2 Eisen t.a.v. gebruik computersoftware

BOA.12.2-010	**wks.boa.sw.ondersteuning**
Eis:	Gedurende de volledige lifecycle van de *beheerfaciliteit* moet de daarin toegepaste *systeemsoftware* door de *leverancier* van die software worden ondersteund.
Herkomst:	specificatieteam
Toelichting:	- Uit beveiligingsoverwegingen moet *systeemsoftware* ge-support worden door de *leverancier*.

3.12.3 Eisen t.a.v. computercommunicatie

BOA.12.3-010	**wks.boa.netw.bandbreedte**
Eis:	Communicatie ten behoeve van verkeerskundige functionaliteit mag niet worden gehinderd door de communicatie tussen een WKS en andere delen van de *beheerfaciliteit*.
Herkomst:	specificatieteam
Toelichting:	- Voorbeelden van communicatie voor verkeerskundige functionaliteit: communicatie met de centrale, met Monica en VIV-W/VIV-C communicatie.

3.13 Overige kwaliteitseisen

3.13.1 Betrouwbaarheid

Er worden geen specifieke eisen gesteld aan de betrouwbaarheid van de *beheerfaciliteit*.

3.13.2 Beschikbaarheid

In onderstaande eisen wordt de beschikbaarheid per functie gespecificeerd.

BOA.13.2-100	**wks.boa.reset.beschikbaarheid**
Eis:	Aan beschikbaarheid van de in paragraaf 3.4.2 gespecificeerde reset-functionaliteit worden de volgende eisen gesteld: a. de functionaliteit moet 24 uur per dag, alle dagen van het jaar beschikbaar zijn; b. PDF (Probability of Failure on Demand): 1 op 100

Herkomst:	specificatieteam
Toelichting:	- *Leverancier* moet aantonen dat aan bovenstaande beschikbaarheidseisen wordt voldaan.

BOA.13.2-110	**wks.boa.cfgupdate.functiebeschikbaarheid**
Eis:	Aan beschikbaarheid van de in paragraaf 3.4.3 gespecificeerde functionaliteit voor configuratie-update worden de volgende eisen gesteld: a. de functionaliteit moet 24 uur per dag, alle dagen van het jaar beschikbaar zijn; b. PDF (Probability of Failure on Demand): 1 op 100
Herkomst:	specificatieteam
Toelichting:	- In de huidige praktijk worden er per DVM-regio minder dan één databasewissel van de MTM centrale uitgevoerd. Een databasewissel impliceert een configuratiewijzing in en aantal onderstations.

BOA.13.2-120	**wks.boa.swupdate.beschikbaarheid**
Eis:	Aan beschikbaarheid van de in paragraaf 3.4.4 gespecificeerde functionaliteit voor software-update worden de volgende eisen gesteld: a. de functionaliteit moet 24 uur per dag, alle dagen van het jaar beschikbaar zijn; b. PDF (Probability of Failure on Demand): 1 op 100
Herkomst:	specificatieteam
Toelichting:	- *Leverancier* moet aantonen dat aan bovenstaande beschikbaarheidseisen wordt voldaan.

BOA.13.2-200	**wks.boa.bhrfac.backup**
Eis:	De *beheerpartij* heeft en volgt een geborgde procedure voor het maken en testen van backups van zowel de programmatuur als de data van de *beheerfaciliteit*.
Herkomst:	[DID.BB:10.11]
Toelichting:	- Doel van deze eis is het handhaven van de integriteit en beschikbaarheid van de *beheerfaciliteit*.

3.13.3 Onderhoudbaarheid

BOA.13-020	**wks.boa.syskwal.wijzigingsbeheer**
Eis:	De implementatie van wijzigingen aan de *beheerfaciliteit* moet verlopen volgens formele procedures voor wijzigingsbeheer. Deze procedure vereist minimaal het volgende: a. uitsluitend geautoriseerde wijzigingen worden geïmplementeerd; b. wijzigingen worden vastgelegd; c. de relatie tussen wijziging en softwareversie van de *beheerfaciliteit* wordt vastgelegd; d. er wordt een analyse uitgevoerd van de impact die de wijziging heeft op de veiligheid van het systeem; e. wijzigingen worden getest in een separate testomgeving; f. er is een terugvalscenario in geval van problemen van de uitrol van de gewijzigde software; g. Een change manager ziet toe op naleving van de procedure.
Herkomst:	[DID.BB:10.25]
Toelichting:	-

3.13.4 Veiligheid

Zie paragraaf 3.9.

3.13.5 Effectiviteit

Er worden geen specifieke eisen gesteld aan de effectiviteit van de *beheerfaciliteit*.

3.13.6 Bruikbaarheid

Er worden geen specifieke eisen gesteld aan de bruikbaarheid van de *beheerfaciliteit*.

3.13.7 Efficiëntie

Er worden geen specifieke eisen gesteld aan de efficiëntie van de *beheerfaciliteit*.

3.13.8 Portabiliteit

Er worden geen specifieke eisen gesteld aan de portabiliteit van de *beheerfaciliteit*.

3.13.9 Toekomstvastheid

BOA.13.9-010	**wks.boa.aanp.areaal**
Eis:	Via configuratie moet het te beheren areaal van de *beheerfaciliteit* kunnen worden aangepast.
Herkomst:	specificatieteam

Toelichting:	- Voor het begrip "areaal", zie sectie 1.2.3. - Het te beheren areaal wijzigt geregeld gedurende de levensduur van de *beheerfaciliteit*. - De *leverancier* moet het in de eis gestelde aan de hand van het ontwerp kunnen aantonen.

BOA.13.9-020	**wks.boa.aanp.melding**
Eis:	In het ontwerp van de *beheerfaciliteit* moet rekening worden gehouden met het uitbreiden van meldingen naar het MISD.
Herkomst:	specificatieteam
Toelichting:	- Het is te verwachten dat het aantal meldingen in de loop van de WKS-versies uitbreidt. - De *leverancier* moet het in de eis gestelde aan de hand van het ontwerp kunnen aantonen.

3.13.10 Vormgeving

Er worden geen specifieke eisen gesteld aan de vormgeving van de *beheerfaciliteit*.

3.13.11 Milieuhygiëne

Er worden geen specifieke eisen gesteld aan de milieuhygiëne van de *beheerfaciliteit*.

3.14 Randvoorwaarden ten aanzien van ontwerp en bouw

BOA.14-010	**wks.boa.ontwerp.inzage**
Eis:	De *leverancier* moet ten aanzien van de *beheerfaciliteit* documentatie beschikbaar stellen waarin tenminste de volgende zaken zijn weergegeven: a. de topologie van computersystemen en netwerkcomponenten vanaf de gebruiker van de *beheerfaciliteit* tot aan WKS; b. de wijze waarop van het RWS netwerk gebruik wordt gemaakt: a. koppelpunten; b. gebruikte protocollen; c. de beveiligingsvoorzieningen, ook ten aanzien aan de *beheerfaciliteit* gekoppelde systemen, zoals laptops van monteurs.
Herkomst:	[DID.BB:A.11-DID-11.4]
Toelichting:	- Deze documentatie moet kunnen worden overlegd aan RWS of een instantie die is aangewezen de veiligheid te toetsen.

3.14.1 Duurzaamheid

Er worden geen specifieke eisen gesteld aan de duurzaamheid van de *beheerfaciliteit*.

3.15 Personeel-gerelateerde eisen

BOA.15-010	**wks.boa.personeel.autorisatie**
Eis:	De *beheerpartij* moet aantonen dat de *beheerfaciliteit* uitsluitend wordt bediend en beheerd door daartoe getrainde medewerkers.
Herkomst:	specificatieteam
Toelichting:	- Gebruikers dienen zich bewust te zijn van de impact en risico's van de *beheerfaciliteit* ten aanzien van het functioneren van DVM-systemen.

3.16 Training-gerelateerde eisen

BOA.16-010	**wks.boa.documentatie**
Eis:	De *leverancier* moet voorzien in documentatie met betrekking tot gebruik en beheer van de *beheerfaciliteit*.
Herkomst:	specificatieteam
Toelichting:	- Met "gebruik" wordt gebruik door *operationeel beheerders* en met "beheer" het beheer van de faciliteit zelf bedoeld. - Zie toelichting bij eis BOA.15-010

3.17 Logistiek-gerelateerde eisen

Er worden geen specifieke eisen gesteld aan de logistiek rondom de *beheerfaciliteit*.

3.18 Andere eisen

Er zijn geen andere eisen.

3.19 Packaging-eisen

Er worden geen specifieke eisen gesteld aan de packaging van de *beheerfaciliteit*.

3.20 Prioriteit en afhankelijkheid van eisen

Er is geen onderlinge prioriteit van eisen in dit document.

4. Kwalificatiebepalingen

In de onderstaande tabel is per eis door middel van een identifier, volgens onderstaande lijst, aangegeven welke kwalificatiebepaling van toepassing is.

identifier	kwalificatiebepaling
(d of D) Demonstratie	De werking van het software-item, of een deel van het software-item, dat afhankelijk is van waarneembare functionele operation waarvoor het gebruik van instrumentatie, speciale testapparatuur of nadere analyse niet nodig is.
(t of T) Test	De werking van het software-item, of een deel van het software-item, waarbij gebruik wordt gemaakt van instrumentatie of andere speciale testapparatuur om gegevens te verzamelen voor latere analyse.
(a of A) Analyse	Het verwerken van verzamelde gegevens verkregen uit andere kwalificatiemethoden. Voorbeelden zijn reductie, interpretatie of extrapolatie van testresultaten.
(I of I) Inspectie	De visuele inspectie van software-item-code, - documentatie, etc.
(s of S) Speciale kwalificatiemethode	Alle speciale kwalificatiemethoden voor het software-item, zoals speciale gereedschappen, technieken, procedures, faciliteiten en acceptatiekaders.

eis	titel	kwalificatie
BOA.4.1-010	wks.boa.bhrfac.algemeen	I
BOA.4.1-030	wks.boa.bhrfac.aansluitvoorwaarden	I
BOA.4.2-010	wks.boa.reset.toestemming	I
BOA.4.2-100	wks.boa.reset.besteenh.functie	D
BOA.4.2-105	wks.boa.reset.besteenh.gedrag	D
BOA.4.2-110	wks.boa.reset.os.functie	D
BOA.4.2-115	wks.boa.reset.os.gedrag	D
BOA.4.2-130	wks.boa.reset.sg.hard.functie	D
BOA.4.2-140	wks.boa.reset.terugkoppeling	T
BOA.4.2-145	wks.boa.reset.reactietijd	T
BOA.4.2-160	wks.boa.reset.log.opdrachtsoort	T
BOA.4.3-010	wks.boa.cfupdate.toestemming	I
BOA.4.3-100	wks.boa.cfgupdate.activeren	D
BOA.4.3-101	wks.boa.cfgupdate.resultaat	D
BOA.4.3-105	wks.boa.cfgupdate.identificatie	D
BOA.4.3-110	wks.boa.cfgupdate.activeren.expliciet	D
BOA.4.3-120	wks.boa.cfgupdate.activeren.doorlooptijd	D
BOA.4.3-130	wks.boa.cfgupdate.rollback	D
BOA.4.3-140	wks.boa.cfgupdate.voorwaarde	I
BOA.4.3-150	wks.boa.cfgupdate.diagnostiek	D
BOA.4.3-160	wks.boa.cfgupdate.log.opstarten	D
BOA.4.4-010	wks.boa.swupdate.toestemming	I

eis	titel	kwalificatie
BOA.4.4-020	wks.boa.swupdate.validatie	D
BOA.4.4-100	wks.boa.swupdate.activeren.applic	D
BOA.4.4-105	wks.boa.swupdate.applic.identificatie	D
BOA.4.4-110	wks.boa.swupdate.activeren.systeem	D
BOA.4.4-120	wks.boa.swupdate.activeren.expliciet	D
BOA.4.4-130	wks.boa.swupdate.activeren.doorlooptijd	D
BOA.4.4-140	wks.boa.swupdate.rollback	D
BOA.4.4-150	wks.boa.swupdate.laadprobleem	D
BOA.4.4-155	wks.boa.swupdate.diagnostiek.appl	D
BOA.4.4-156	wks.boa.swupdate.diagnostiek.syst	D
BOA.4.4-170	wks.boa.swupdate.log.opstarten	D
BOA.4.5-100	wks.boa.diag.wks.functie	D
BOA.4.5-120	wks.boa.diag.componenten	D
BOA.4.5-130	wks.boa.diag.interfaces	D
BOA.4.5-140	wks.boa.diag.comp.dynamisch.gedrag	D
BOA.4.5-145	wks.boa.diag.if.dynamisch.gedrag	D
BOA.4.5-150	wks.boa.diag.identificatie	D
BOA.4.5-160	wks.boa.diag.logging.inzien	D
BOA.4.5-180	wks.boa.diag.logging.export	D
BOA.4.5-190	wks.boa.diag.logging.storing	D
BOA.4.5-195	wks.boa.diag.logging.storing.retentie	D
BOA.5.2-010	wks.boa.csv.formaat	T
BOA.6-010	wks.boa.netwerk	I
BOA.9-010	wks.boa.veilig	D
BOA.10.1-010	wks.boa.bev.bhrfac.autorisatie	D
BOA.10.1-020	wks.boa.bev.bhrfac.autorisatie.rollen	D
BOA.10.1-025	wks.boa.bev.bhrfac.authen.functiescheiding	D
BOA.10.1-040	wks.boa.bev.bhrfac.authen.persoonlijk	D
BOA.10.1-050	wks.boa.bev.bhrfac.authen.sterk	D
BOA.10.1-055	wks.boa.bev.bhrfac.authen.versleuteld	D
BOA.10.1-100	wks.boa.bhrfac.segmentatie	D
BOA.10.1-120	wks.boa.bev.netw.koppelpunt.wks	D
BOA.10.2-130	wks.boa.bev.netw.koppelpunt.extern	D
BOA.10.2-140	wks.boa.bev.netw.ander	D
BOA.10.1-200	wks.boa.bev.bhrfac.malware	D
BOA.10.1-210	wks.boa.bev.bhrfac.patches	D
BOA.10.1-300	wks.boa.bev.bhrfac.benoemd	D
BOA.10.1-400	wks.boa.bev.bhrfac.fysiek	I
BOA.10.1-450	wks.boa.bev.hardened	I
BOA.10.1-500	wks.boa.bev.bhrfac.incidentproc	I
BOA.10.2-010	wks.boa.bhrfac.auditlog.functie	D
BOA.10.2-012	wks.boa.wks.auditlog.functie	D

eis	titel	kwalificatie
BOA.10.2-015	wks.boa.bhrfac.auditlog.export	D
BOA.10.2-020	wks.boa.bhrfac.auditlog.inhoud	D
BOA.10.2-021	wks.boa.bhrfac.auditlog.inhoud.persoon	D
BOA.10.2-030	wks.boa.bhrfac.auditlog.retentie	D
BOA.10.2-040	wks.boa.bhrfac.auditlog.integriteit	D
BOA.10.2-050	wks.boa.bhrfac.auditlog.sync	D
BOA.10.3-010	wks.boa.wks.autorisatie	D
BOA.10.3-020	wks.boa.wks.autorisatie.log.functie	D
BOA.10.3-030	wks.boa.wks.autorisatie.log.inhoud	D
BOA.12.2-010	wks.boa.sw.ondersteuning	D
BOA.12.3-010	wks.boa.netw.bandbreedte	D
BOA.13.2-100	wks.boa.reset.beschikbaarheid	D
BOA.13.2-110	wks.boa.cfgupdate.functiebeschikbaarheid	D
BOA.13.2-120	wks.boa.swupdate.beschikbaarheid	D
BOA.13.2-200	wks.boa.bhrfac.backup	I
BOA.13-020	wks.boa.syskwal.wijzigingsbeheer	I
BOA.13.9-010	wks.boa.aanp.areaal	D
BOA.13.9-020	wks.boa.aanp.melding	D
BOA.14-010	wks.boa.ontwerp.inzage	I
BOA.15-010	wks.boa.personeel.autorisatie	D
BOA.16-010	wks.boa.documentatie	I

5. Herleidbaarheid van de eisen

In de verschillende paragrafen worden de gedefinieerde eisen benoemd die van toepassing zijn op de verschillende ontwerpteksten. De traceerbaarheid van de gestelde eisen wordt vermeld bij iedere eis bij het kopje “herkomst”.

Op BOA is een groot aantal veiligheidseisen van toepassing. Deze eisen hebben deels betrekking op ontwerp, bouw en installatie van de *beheerfaciliteit*; deze eisen zijn in de voorliggende SSS en bijbehorende SSDD vastgelegd. Voor het andere deel hebben deze veiligheidseisen betrekking op procedures rondom operationeel beheer. “Bijlage A: Afdekking beveiligingseisen“ geeft aan welke veiligheidseisen in de SSS zijn opgenomen en welke in procedures hun beslag krijgen.

6. Opmerkingen

6.1 Afkortingen en acroniemen

Acroniem/afkorting	Toelichting
BIV	Een BIV is een eenheid waaraan informatie wordt verstrekt over de actuele beelden die op een signaleringsraai worden getoond.
BOA	Beheer op Afstand
CS	Centraal Systeem; hiermee wordt de MTM2 centrale bedoeld die WKS'en verkeerskundig aanstuurt.
CSV	Comma Separated Values. Een gegevensformaat waarbij gegevenselementen in tekstuele vorm, van elkaar gescheiden door een speciaal teken (vaak een komma), worden weergegeven. Zie ook sectie 3.5.2.
DVM	Dynamisch VerkeersManagement, het deel van de werkzaamheden van de wegverkeersleider dat direct met het beheersen van verkeersstromen op het hoofdwegennet te maken heeft.
ISD	De afdeling ICT Servicemanagement Dynamisch Verkeersmanagement (ISD) staat voor de beschikbaarheid van DVM-ketens. De ISD biedt eerstelijns ondersteuning aan de wegverkeersleiders.
ISD-SDD	Service Desk DVM van de ISD
LIB	Een LIB is een eenheid die beeldopdrachten kan genereren voor een signaleringsraai van het *wegkantsysteem* waarop zij is aangesloten.
MISD	Meldingensysteem ISD
Monica	"Monitoring casco" een centraal systeem dat voertuigdetetciegegevens van WKS'en verzamelt.
MUS	Multi-sign bord
NNV	Nieuwe Netwerkvoorzieningen Verkeer en Waterstaat
NNV-NG	Zie RWSNet
RWS	Rijkswaterstaat
RWSNet	Landelijke Rijkswaterstaat Netwerkinfrastructuur. Bestaat uit "VicNet" en "NNV". RWSNet wordt ook wel aangeduid met "NNV-NG".
VicNet	De term VICnet wordt gebruikt om wegkantnetwerken en de regionale glasnetwerken aan te duiden. In dit document wordt de term"RWSnet" gebruikt, hoewel dit meer omvat dan alleen VicNet.
VIV-C	"Voertuig InformatieVerstrekker" interface tussen een WKS en een centraal systeem. Deze interface wordt gebruikt om voertuigdetectieinformatie van een WKS met een hogere frequentie dan één keer per minuut te verzenden aan het centrale systeem.

Acroniem/afkorting	Toelichting
VIV-W	"Voertuig InformatieVerstrekker" interface tussen twee WKS'en. Deze interface wordt met name gebruikt door een WKS om voertuigdetectieinformatie aan een WKS van een andere leverancier te leveren.
WKS	*Wegkantsysteem*

6.2 Terminologie

Term	Definitie
2-factor authenticatie	Een authenticatievorm waarbij op twee van de drie volgende vormen van identiteitsbewijs wordt getoetst: • kennis, bijv. een pincode, • bezit, bijv. een smartcard, • persoonlijke eigenschap, bijv. vingerafdruk.
applicatiesoftware	Applicatiesoftware omvat alle software die WKS-specifieke functionaliteit realiseert, zoals de *OS-applicatie*, inclusief de hier beschreven software t.b.v. beheer op afstand.
beheerfaciliteit	Een centraal toegankelijk systeem dat beheer op afstand voor alle wegkantsystemen van een bepaalde leverancier mogelijk maakt.
beheerpartij	Een organisatie, meestal buiten RWS, die verantwoordelijk is voor de instandhouding van de WKS-functionaliteit.
besturingseenheid	Een besturingseenheid is het totaal van hardware en *systeemsoftware* in een *wegkantsysteem* dat verantwoordelijk is voor alle functionele gedrag, aansturing van actuatoren en detectoren en communicatie met externe systemen. Een besturingseenheid heeft een eigen netwerkkaart. Er kunnen tot 4 besturingseenheden in een wegkantstation zijn ondergebracht.
boven de klemmenstrook	Het gedeelte van verkeerssignalering dat zich in de kast langs de kant van de weg bevindt. Op de klemmenstrook komen voeding en communicatielijnen met signaalgevers en andere periferie de kast binnen.
leverancier	De organisatie die een WKS en de daarbij behorende *beheerfaciliteit* ontwikkelt. De leverancier is verantwoordelijk voor de installatie van een *beheerfaciliteit*, waarin het koppelen aan het RWS-netwerk wordt begrepen.
OS-applicatie	De onderstation-applicatie is de softwarematige representatie van één MTM2-onderstation.
op afstand	"Op afstand" is de term die gebruikt wordt om aan te geven dat een *operationeel beheerder* vanaf een andere locatie dan langs de weg, bijvoorbeeld het kantoor van de *beheerpartij*, in staat is te communiceren met operationele wegkantsystemen.
operationeel beheerder	Een persoon die verantwoordelijk is voor de instandhouding van de WKS-functionaliteit. Een operationeel beheerder wordt ook aangeduid met de term monteur. De beheerder maakt deel uit van de *beheerpartij*.
rijstrookdetectiepunt	Punt op een detectieraai waarop voertuigpassages op een specifieke rijstrook worden waargenomen (gedetecteerd).
systeemsoftware	Generieke, applicatieonafhankelijke, software op een WKS, zoals een operating systeem, aangevuld met middleware, indien van toepassing.

Term	Definitie
wegkantsysteem	Een besturingssysteem langs de kant van de weg volgens [WKS.SSS]. Een behuizing met de daarin aanwezige besturingseenheden voor signaleren en monitoren.

7. Bijlage A: Afdekking beveiligingseisen

Onderstaande tabel is een opsomming van alle beveiligingseisen die aan "WKS 1.3 – Beheer op Afstand" worden gesteld. De eisen zijn afkomstig uit de "Top 10 beveiligingsbeheersdoelen voor Industriële Automatisering", aangeduid met "top-10" en de aanvullende maatregelen, afkomstig uit "IRAM – Risicoanalyse, Remote–beheer WKS 1.3", aangeduid met "IRAM". De kolom "vastlegging" van deze tabel geeft aan waar deze eis is afgedekt, in de specificaties ("WKS - beheer op afstand, SSS") en ontwerp ("WKS - beheer op afstand, SSDD") of in procedures die zijn afgestemd met de *beheerpartij*. Deze procedures kunnen zijn vastgelegd in contracten of DAP's (Dossier Afspraken en Procedures).

bron	nr	beschrijving	vastlegging	opmerking
top-10	**1**	**Fysieke beveiliging**		
top-10	1.1	De fysieke beveiliging van objecten dient plaats te vinden conform het Corporate Beveiligingsmodel (CBM) van RWS.	SSS proc	*Beheerfaciliteit* zal kan in datacenter van RWS of bij *beheerpartij* zelf zijn ondergebracht. In procedures zal moet worden geborgd dat toegangsrechten aan de juiste personen worden verleend.
top-10	1.2	Voor de fysieke toegangsbeveiliging van de objecten dient de Rijkspas ingezet te worden.	n.v.t.	*Beheerpartij* beschikt niet over rijkspas
top-10	1.3	Voor de fysieke toegangsbeveiliging van de vitale zones waarin zich bedien, systeem en technische ruimten zich bevinden wordt de Rijkspas ingezet.	n.v.t.	*Beheerpartij* beschikt niet over rijkspas
top-10	**2**	**Logische toegangsbeveiliging**		
top-10	2.1	De toegang tot informatiesystemen en netwerk dient plaats te vinden na een succesvol identificatie, authenticatie en autorisatieproces waarbij de IAA gegevens in versleutelde vorm worden uitgewisseld en opgeslagen.	SSS	
top-10	2.2	Lokale logische toegang tot (missie)kritieke en/of ICS/SCADA systemen dient plaats te vinden door middel van smartcard logon.	n.v.t.	
top-10	2.3	Remote toegang tot RWS systemen, databases en netwerk voor productie doeleinden dient plaats te vinden met two factor authenticatie en via de centrale beveiligde voorzieningen van RWS.	SSS	*Beheerfaciliteit* is eigendom van *beheerpartij*. Authenticatie via RWS is niet van toepassing
top-10	2.4	Remote toegang tot RWS systemen, databases en netwerk voor beheer en onderhoud dient plaats te vinden conform de procedure toegang derden	proc	
top-10	2.5	De wachtwoordrichtlijnen voor ICS/SCADA systemen dienen in acht te worden genomen.	SSS/proc	

bron	nr	beschrijving	vastlegging	opmerking
top-10	2.6	Het koppelen van apparatuur van derden of removable media aan locale ICS/SCADA netwerken of het RWS netwerk door Opdrachtnemer dient plaats te vinden na autorisatie van Opdrachtgever.	proc	
top-10	**3**	**Beveiligingsincidenten en Incident Response Plan**		
top-10	3.1	Er is een geborgde procedure voor het melden, registreren en rapporteren van beveiligingsincidenten	SSS	
top-10	3.2	Er is een geborgde procedure voor het oplossen van beveiligingsincidenten.	SSS	
top-10	3.3	Er is een geborgde procedure voor incidentrespons en continuïteit van de ICT en ICS/SCADA dienstverlening ingeval van incidenten en calamiteiten	SSS	
top-10	**4**	**Netwerkkoppelingen**		
top-10	4.1	ICS/SCADA en de ondersteunende systemen en besloten (lokale) objectnetwerken dienen geen directe verbindingen te hebben met kantoornetwerken.	SSS	
top-10	4.2	De besloten (lokale) objectnetwerken dienen geen directe internet verbindingen te hebben alsmede draadloze WiFi en GPRS/UMTS etc.) of inbelvoorzieningen. Uitgezonderd zijn de netwerkverbindingen van het object met de centrale netwerkvoorzieningen van RWS en de door RWS toegestane verbindingen.	SSS	
top-10	4.3	Bij de inzet van communicatieprotocollen dient de beveiligde variant aangehouden te houden.	SSS	
top-10	4.4	Netwerkkoppelingen tot het RWS netwerk dienen plaats vinden via de beveiligde koppelpunten en conform de aansluitvoorwaarden van RWS.	SSS	
top-10	4.5	De ICS/SCADA systemen dienen gebruik te maken van een aparte infrastructuur. Deze infrastructuur is gescheiden van andere netwerken. De scheiding kan fysiek of logisch zijn ingericht.	SSS/SSDD	
top-10	4.6	Binnen de (object)netwerken dient segmentering van verkeersstromen voor productie, beheer en OTA toegepast te worden. De segmentering kan fysiek of logisch worden ingericht.	SSS/SSDD	De specificatie en het ontwerp vereisen een scheiding van productie- en beheerverkeersstromen. OTA-omgeving is aan de *leverancier*
top-10	4.7	Het aantal netwerkkoppelingen tussen ICS/SCADA systemen en andere netwerken dient beperkt te blijven tot alleen de noodzakelijke en dat het netwerk wordt gehardend door niet noodzakelijke netwerkservices uit te zetten.	SSS/SSDD	

bron	nr	beschrijving	vastlegging	opmerking
top-10	4.8	Alle toegestane lokale (LAN) netwerken, externe verbindingen en beveiligingsvoorzieningen dienen in kaart te zijn gebracht en gedocumenteerd. Dit overzicht en bijbehorende documentatie dient actueel gehouden te worden inclusief de interfacing naar andere systemen toe.	SSS	
top-10	**5**	**Bescherming tegen malware, hardening en patching**		
top-10	5.1	Er dient een geborgde procedure en voorzieningen te bestaan voor detectie en preventie tegen malware.	proc	
top-10	5.2	ICS/SCADA, beveiliging en ondersteunende ICT-systemen en netwerkelementen dienen te zijn gehardend door het uitschakelen van overbodige functies in besturingssystemen en/of van het systeem verwijderen en zodanige waarden toekennen aan beveiligingsinstellingen dat een maximale beveiliging ontstaat.	SSS	
top-10	5.3	ICT systemen die gekoppeld worden aan ICS/SCADA, beveiliging- en netwerkomgeving en de ICS/SCADA systemen zelf, dienen te zijn voorzien van alle recente beveiligingsupdates en patches. Kritieke patches dienen conform de patchrichtlijn te worden geïmplementeerd.	SSS	
top-10	**6**	**Logging en monitoring**		
top-10	6.1	Activiteiten van gebruikers, beheerders, uitzonderingen en informatiebeveiligingsgebeurtenissen dienen te worden vastgelegd in audit-logbestanden.	SSS	
top-10	6.2	Logbestanden van ICS/SCADA, beveiliging en ondersteunende ICT-systemen en -netwerkelementen dienen via het bedrijfsnetwerk gekoppeld te worden met het Cyber Security Operation Center van RWS voor analyse doeleinden.	SSS	SSS specificeert dat auditlog door RWS opvraagbaar is. Er is geen fysieke koppeling voorzien.
top-10	**7**	**Bewustwording en Training**		
top-10	7.1	Werknemers en ingehuurd personeel dienen bewust gemaakt te worden en geschikte training en regelmatige bijscholing te krijgen met betrekking tot het beveiligingsbeleid en procedures, voor zover relevant voor hun functie.	proc	
top-10	7.2	Informatiesystemen, ICS/SCADA systemen, databases en bedrijfsmiddelen dienen over actuele (technische) beheerdocumentatie, gebruikers- en/of installatiehandleiding te beschikken.	SSS	
top-10	**8**	**Gecontroleerd wijzigingen**		

bron	nr	beschrijving	vastlegging	opmerking
top-10	8.1	Er dient een geborgde wijzigingsprocedure te bestaan voor het op een gecontroleerde wijze doorvoeren van wijzigingen.	SSS proc	In SSS wordt deze eis aan de *leverancier* gesteld. Aanname is dat deze ook het applicatiebeheer doet.
top-10	**9**	**Beheer- en onderhoudscontracten**		
top-10	9.1	In de contracten met *leverancier*s dienen afspraken op het gebied van beveiliging voor logische en fysieke toegang, incident- en lograpportages, ondersteuning bij incident en calamiteitenafhandeling, logging en monitoring en beheer en onderhoud te worden opgenomen.	proc	
top-10	**10**	**Back-ups**		
top-10	10.1	De integriteit en beschikbaarheid van informatie en programmatuur dient te worden gewaarborgd door een geborgde procedure voor het maken en testen van back-ups.	SSS	
IRAM	1	Remote beheer kent een gescheiden VPN-beheer omgeving. De systemen zijn in apart gesegmenteerde netwerken binnen Vicnet geplaatst zodat kwetsbaarheden en hackaanvallen, virussen of malware zo min mogelijk invloed hebben op omgeving.	SSS/SSDD	
IRAM	2	De beheer omgeving kent een andere alternatieve omgeving in geval van een calamiteit (Dos aanval) die zo weinig mogelijk componenten deelt met de productie omgeving.	proc	
IRAM	3	Alle relevante systemen in de keten zijn opgenomen in het betreffende calamiteitenplan van de ruimte waar de systemen zijn geplaatst.	proc	
IRAM	4	Alle componenten moeten worden gehardened op basis van de laatste best practises	SSS	
IRAM	5	Er is een administratie aanwezig op wie toegang heeft en welke rechten en profielen er zijn. Herleidbaarheid van wijzigingen in gebruikersprofielen (rollen etc.)	proc	
IRAM	6	Er dient periodiek een security scan (PEN Test) te worden uitgevoerd op de verschillende componenten door een onafhankelijke partij (Blackbox en Whitebox test)	proc	

bron	nr	beschrijving	vastlegging	opmerking
IRAM	7	De aanvraag tot toegang wordt gefaciliteerd door RWS. Daarbij wordt een afweging gemaakt mbt tot de te beheren systemen. De toegang wordt centraal geadministreerd. Beheerders en externe partijen krijgen een overeenkomst te tekenen, met daarin: • De gedragsregels • Aansprakelijkheid • Beveiligingsincidenten • Regels rondom uitwisselen van bestanden • Wat de doen bij verlies en diefstal van de laptop of het token. Pas na het doorlopen van de procedure en het tekenen van de overeenkomst kan de toegang worden ingeregeld.	proc	Een *leverancier* zal 1 *beheerfaciliteit* koppelen aan het WKS-netwerk. Daarnaast kan de *beheerpartij* RAS-diensten aanvragen bij RWS, maar kan dit soort koppelingen ook via de (eigen) *beheerfaciliteit* laten lopen, buiten RWS om.
IRAM	8	Maken SLA's met hardware en software *leverancier*, waarin oplostijden van verstoringen en het oplossen van veiligheidslekken etc gewaarborgd is	SLA	
IRAM	9	Voor alle componenten dient een eigenaar of een custodian te worden aangewezen	proc	
IRAM	10	Het gebruik maken van Sterke Authenticatie tijdens het aanloggen op beschikbaar gestelde inlogprocedures.	SSS	
IRAM	11	Het dagelijks scannen van bekende kwetsbaarheden op het RWS domein via virus & Vulnerability scanners.	proc	
IRAM	12	Er is een change managemenr proces ingericht, waarbij rekening is gehouden met alle partijen in de keten	proc	
IRAM	13	Beheerders mogen alleen de noodzakelijke informatie raadplegen, bewerken en toevoegen. Ook moet er input validatie worden uitgevoerd	SSS	
IRAM	14	Logging moet beveiligd zijn tegen ongeautoriseerde gebruikers. Logging moet tevens veilig worden gesteld op bijvoorbeeld een syslog server.	SSS	
IRAM	15	RWS krijgt een maandelijkse rapportage met minimaal: • In detail aantal niet succesvolle aanloggen • In detail capaciteit en beschikbaarheid • Aantal beveiligingsincidenten • Aantallen gebruikers • Licentiemanagement en capaciteit • Trendanalyse	proc	
IRAM	16	De keten moet volledig in kaart gebracht zijn. Alle componenten in de keten moet actief worden beheerd. Er zijn duidelijke afspraken over de rollen van DID en andere *beheerpartij*en.	proc	
IRAM	17	Technisch afdwingen van functiescheiding binnen technisch, applicatie, functioneel beheer en gebruikers	SSS	

bron	nr	beschrijving	vastlegging	opmerking
IRAM	18	Beheer van systemen en netwerken wordt uitgevoerd door gekwalificeerd personeel, en afgebakend door beleid & procedures	proc	
IRAM	19	Redundantie van netwerkverbindingen en systemen van belangrijke locaties	nvt	*Leverancier* bepaalt zelf op basis van beschikbaarheidseisen of redundantie noodzakelijk is.
IRAM	20	De omgeving wordt gemonitord op beschikbaarheid en capaciteit (licenties).		