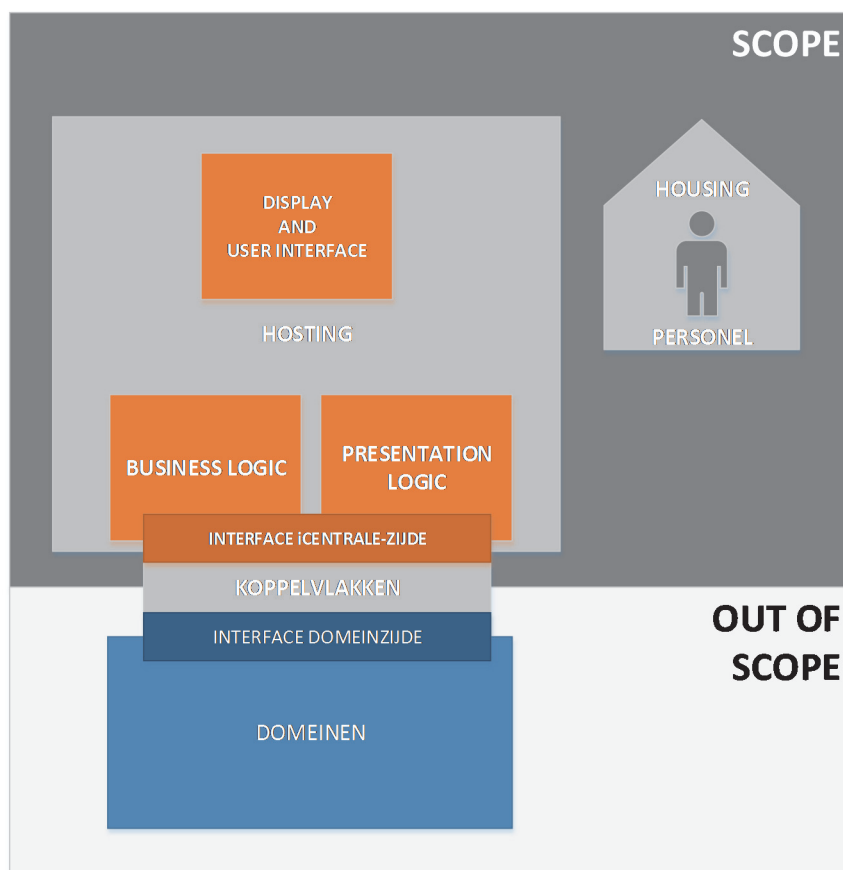


iCENTRALE PROJECT 4.05

VEILIGHEIDSKADERS



Datum: 05-04-2018

Versie: 3.0

Inhoud

Inhoud	2
1 Inleiding	5
1.1 Doelstelling	5
1.2 Reikwijdte veiligheid	6
1.3 Leeswijzer	6
1.4 Revisieoverzicht	7
1.5 Gerefereerde documenten	7
1.6 Afkortingen	7
1.7 Actualiteit van dit document	7
2 Veiligheidsthema's	8
2.1 Identificatie Veiligheidsthema's	8
2.2 Toepasbaarheid Veiligheidsthema's	9
3 Gevolgde aanpak per veiligheidsthema.....	10
3.1 Inventarisatie veiligheidsdocumenten	10
3.1.1 Europese Richtlijnen	11
3.1.2 Nationale Wet	11
3.1.3 Besluiten en Regelingen	11
3.1.4 Normen	11
3.2 Uitwerking door selecteren en koppelen relevante teksten	12
3.2.1 (Systeem)Functie Coördineren.....	13
3.2.2 (Systeem)Functie Attenderen.....	13
3.2.3 (Systeem)Functie Observeren	13
3.2.4 (Systeem)functie Communiceren	14
3.2.5 (Systeem)Functie Managen.....	14
3.2.6 (Systeem)Functie Veilig Ingrijpen	14
3.2.7 Cross-reference configuratie-items <-> systeemfuncties	14
3.3 Knelpunten inventarisatie en oplossingsrichtingen.....	15
4 Veiligheidsthema Arbeidsveiligheid.....	16
4.1 Inventarisatie documenten.....	16
4.2 Uitwerking.....	16
4.2.1 Richtlijn arbeidsmiddelen	16
4.2.2 Arbeidsomstandighedenwet.....	16
4.2.3 Arbobesluit.....	17
4.2.4 Arbeidsomstandighedenregeling	20
4.2.5 Overig	21
4.3 Knelpunteninventarisatie en Oplossingsrichtingen	22
5 Veiligheidsthema Verkeersveiligheid	23
5.1 Inventarisatie documenten.....	23
5.2 Uitwerking.....	24
5.3 Knelpunteninventarisatie en Oplossingsrichtingen	26
6 Veiligheidsthema Nautische veiligheid.....	27
6.1 Inventarisatie documenten.....	27
6.2 Uitwerking.....	27
6.2.1 Verkeersbegeleiding en brug- en sluisbeheer	28
6.2.2 Beschouwing systeemfuncties brug- en sluisbeheer	31
6.2.3 Ondersteunen bij incident- en calamiteitenbestrijding	32
6.3 Knelpunteninventarisatie en Oplossingsrichtingen	34

7	Veiligheidsthema Externe veiligheid	35
7.1	Inventarisatie documenten.....	35
7.2	Uitwerking.....	35
7.2.1	Wet veiligheidsregio's.....	35
7.2.2	Wet vervoer gevaarlijke stoffen	35
7.3	Knelpunteninventarisatie en Oplossingsrichtingen	36
8	Veiligheidsthema Veiligheid beweegbare objecten.....	37
8.1	Inventarisatie documenten.....	37
8.2	Uitwerking.....	38
8.2.1	Beschouwing systeemfuncties.....	41
8.2.2	Aandachtspunten bij migratie naar centrale bediening	43
8.3	Knelpunteninventarisatie en Oplossingsrichtingen	44
9	Veiligheidsthema Tunnelveiligheid.....	45
9.1	Inventarisatie documenten.....	45
9.2	Uitwerking.....	45
9.2.1	Beschouwing systeemfuncties.....	48
9.3	Knelpunteninventarisatie en Oplossingsrichtingen	49
10	Veiligheidsthema Integrale beveiliging	51
10.1	Inventarisatie documenten.....	51
10.2	Uitwerking.....	52
10.2.1	Cybersecurity	52
10.2.2	Cameratoezicht.....	54
10.3	Knelpunteninventarisatie en Oplossingsrichtingen	55
10.3.1	Knelpunten Cybersecurity	55
10.3.2	Knelpunten Cameratoezicht	59
11	Input andere projecten	61
11.1	Project 1.2: Verantwoordelijkheidsverdeling publiek-privaat als randvoorwaarde voor de iCentrale	61
11.2	Project 1.3: Back-up- Overnametaken.....	61
11.3	Project 1.5: Combineren functies binnen de verschillende domeinen.....	62
11.4	Project 1.7: Functionele Koppelvlakken.....	62
11.5	Project 2.3: High Level MMI: bedienproces verschillende domeinen.....	62
11.6	Project 2.4: Uniforme bediening iCentrale.....	62
11.7	Project 4.1: Functionele Architectuur	63
11.8	Project 4.2: Technische koppelvlakken.....	63
12	Conclusie	64
13	Lijsten.....	65
13.1	Referentie Configuratie-items naar documentpassage	65
13.2	Figuren.....	67
13.3	Tabellen	67
14	Bijlagen.....	68
14.1	Onderzochte veiligheidsdocumenten	68
14.2	Bevindingen per veiligheidsthema.....	69
14.3	Configuratie-items veiligheid	70

Opsteller/ projectteam:



Projectleider: B. Kollmer

Teamleden

Dynniq	- Casper Moerbeek, Bob Kollmer
Siemens	- Ron Hendriks
Technolution	- Paul van Koningsbruggen, William Meijer
Vialis	- Tom Steijvers, Pepijn Leenaers
Arcadis	- Leon Ziengs

1 Inleiding

1.1 Doelstelling

Voor u ligt het document iCentrale Project 4.05 Veiligheidskaders. Dit document is een leidraad voor implementatie van veiligheid voor iCentrale producten/diensten en is bedoeld voor een ieder die betrokken is bij de implementatie van iCentrale producten/diensten. Deze iCentrale producten/diensten kunnen enerzijds bij de ontwikkeling en of aanpassing van het iCentrale-systeem zelf zijn, dan wel voor implementatie van een of meerdere domeinen (Verkeersmanagement, Tunnelbediening/bewaking, Brug- en sluisbediening, stads-/cameratoezicht, crowdmanagement, parkeerbeheer) voor een iCentrale-systeem.

Dit document behandelt de veiligheidskaders die gelden voor centrale monitorings- en bedieningsactiviteiten. Het geeft antwoord op de vraag of het mogelijk is, conform de geldende kaders, een centrale breder, multidisciplinair, groter te maken of uit te besteden.

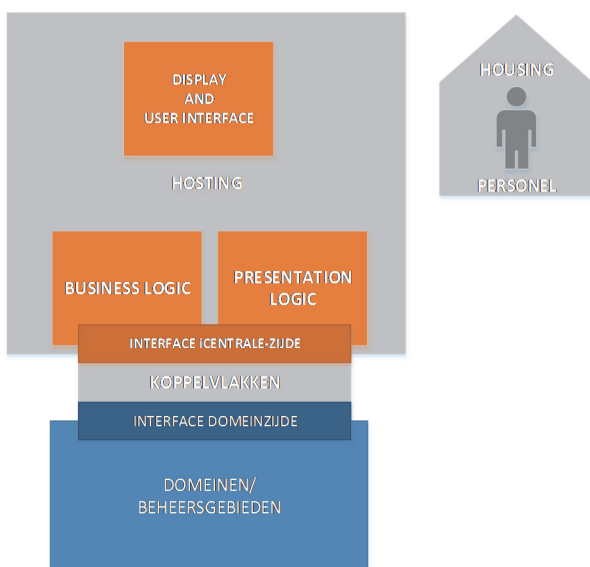
Dit document heeft de volgende doelstellingen m.b.t. veiligheid:

1. Ondersteunt de op te stellen modeluitvragen en modelcontracten
2. Geeft inzicht bij de verdeling van taken, bevoegdheden en verantwoordelijkheden tijdens het uitvraag en aanbiedingsproces
3. Geeft handvatten voor het opstellen van de specifieke uitvraag, aanbieding en daarmee het contract

Veiligheid is voor veel gebieden verankerd in wet- en regeling. Voor iCentrale producten/diensten heeft dit ook effect op taken, bevoegdheden en verantwoordelijkheden voor zowel aanvrager als aanbieder.

Dit document is zowel bedoeld voor uitvragers als aanbieders van iCentrale producten/diensten. Omdat in dit document veiligheid centraal staat en als keten wordt benaderd, worden de volgende hoofdzaken onderscheiden:

1. Personeel en huisvesting daarvan
2. iCentrale systeem en hosting daarvan
3. Domeinen met de daarvoor relevante koppelvakken



Figuur 1 Hoofdzaken veiligheid

Dit document project levert uiteindelijk een bruikbare leidraad op, die inzicht geeft in de mogelijkheden en onmogelijkheden voor wat betreft iCentrale gerelateerde uitvragen en aanbiedingen en randvoorwaardelijke kaders schept. Eisen, wensen en verwachtingen omtrent de mogelijkheden voor realisatie worden hiermee verduidelijkt en op realiseerbaarheid getoetst.

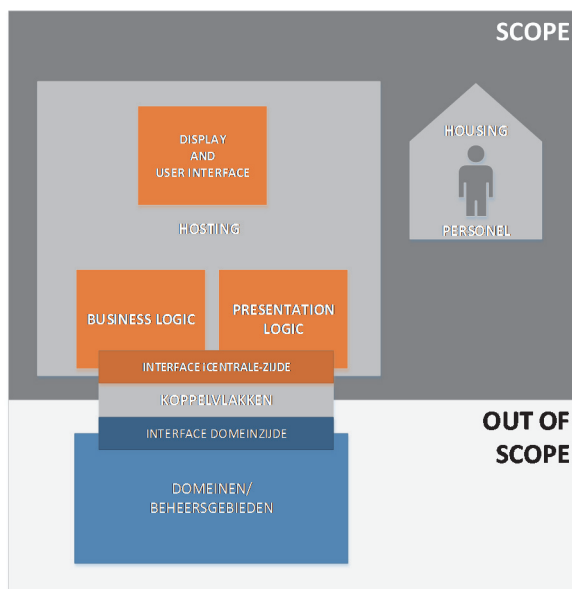
1.2 Reikwijdte veiligheid

iCentrale producten/diensten worden toegepast op domeinen die bediend, bestuurd en bewaakt worden. Als uitgangspunt hierbij geldt dat het domein zelf aan de vereiste veiligheidskaders voldoet. Dit betekent dat bv. een brug als object zelf aan de wettelijke kaders en vereiste normen voldoet. Aangezien een brug bediend kan worden, wordt de 'veiligheidsketen' verlengd tot aan de operator.

De dan verkregen reikwijdte is afgebeeld in Figuur 2 Weergave reikwijdte veiligheid.

Binnen de scope zijn het iCentrale personeel met huisvesting, de iCentrale systemen en hosting en de koppelvlakken aan de iCentrale zijde.

Buiten scope zijn de domeinen met hun eigen systemen, koppelvlakken naar de iCentrale en het personeel binnen het domein.



Figuur 2 Weergave reikwijdte veiligheid

1.3 Leeswijzer

In hoofdstuk 2 *Veiligheidsthema's* worden de veiligheidsthema's geïdentificeerd en gealloceerd naar iCentrale producten/diensten. In hoofdstuk 3 *Gevolgd aanpak per veiligheidsthema* is aangegeven hoe deze veiligheidsthema's uitgewerkt worden, opdat ze handvatten geven, die in de hoofdstukken 4 t/m 10 per veiligheidsthema op een identieke wijze worden uitgewerkt. In hoofdstuk 11 *Input andere projecten* is de relatie met andere projecten uitgewerkt.

Voor een duidelijke context verdient het aanbeveling dit document samen te lezen met de blauwdruk iCentrale [3] en begrippenlijst iCentrale [4].

1.4 Revisieoverzicht

Rev.	Status	Datum	Omschrijving.	Auteur
0.1	Concept	03-2017 t/m 06-2017	Concept	B. Kollmer
0.2	Concept	28-07-2017	Concept	B. Kollmer
0.3	Concept	18-09-2017	Concept	B. Kollmer
0.4	Concept	----	In bewerking	B. Kollmer
0.5	Concept	----	In bewerking	B. Kollmer/R. de Klerk
0.6	Concept	----	In bewerking. Redigeerversie.	B. Kollmer
0.7	Concept	----	In bewerking. Redigeerversie.	B. Kollmer
0.8	Concept	----	In bewerking. Redigeerversie.	B. Kollmer
1.0	Definitief	22-12-2017	Eerste uitgave	B. Kollmer
2.0	Definitief	16-02-2018	Deel Integrale Beveiliging verder uitgewerkt	B. Kollmer
3.0	Definitief	05-04-2018	Extern reviewcommentaar verwerkt	B. Kollmer

1.5 Gerefereerde documenten

Ref. nr.	Omschrijving	Documentcode	Rev.	Datum	Status
[1]	IBEDIENFILOSOFIE	Bedienfilosofie - iHMI v 1.1 FINAL	1.1	20-02-2017	Final
[2]	Beheereisen PNH VM	Eisen t.a.v. ICT en Beheer voor DVM	0.3	25-11-2015	Draft
[3]	Blauwdruk	Blauwdruk v2.0	2.0	04-09-2018	Definitief
[4]	Begrippenlijst	Begrippenlijst iCentrale	-	22-02-2018	-

1.6 Afkortingen

De onderstaande tabel geeft een verklaring van de in dit document gebruikte afkortingen.

Afkorting	Verklaring
-	-

1.7 Actualiteit van dit document

Bij het opstellen van dit document is zorgvuldig gekeken naar vigerende wet- en regelgeving. Deze zijn echter aan verandering onderhevig. Bij daadwerkelijke toepassing van dit document dient onderzocht te worden of de hier geanalyseerde wet- en regelgeving die tot dit veiligheidskader geleid heeft, nog van toepassing is.

2 Veiligheidsthema's

2.1 Identificatie Veiligheidsthema's

Om relevante veiligheidsthema's te kunnen afbakenen wordt de visie van Integrale Veiligheid gehanteerd, die wordt toegepast in het kader van veiligheidsmanagement bij Rijkswaterstaat. Deze benaderwijze is goed toepasbaar binnen het thema veiligheidskaders van de iCentrale omdat de thema's aansluiten bij iCentrale domeinen.

Integrale veiligheid van een Rijkswaterstaatobject betekent het beheersen van alle soorten veiligheid: arbeidsveiligheid, constructieve veiligheid, verkeersveiligheid, sociale veiligheid enz.

Beheersen houdt o.a. in, het stap voor stap en systematisch ontwikkelen en beheren van veiligheidsproducten.

Er zijn 11 veiligheidsthema's gedefinieerd.

1. Arbeidsveiligheid
Definitie: De veiligheid van personen die beroepshalve aanwezig zijn.
2. Verkeersveiligheid
Definitie: De veiligheid van verkeersdeelnemers, als gevolg van deelname aan het wegverkeer rondom de werkzaamheden.
3. Nautische veiligheid
Definitie: Veiligheid van het transport over zee en de binnenvaart.
4. Veiligheid tegen overstromen
Definitie: Veiligheid van personen of objecten met betrekking tot hoog water.
5. Externe veiligheid
Definitie: De kans om te overlijden als rechtstreeks gevolg van een ongewoon voorval bij het transport van een gevaarlijke stof (via weg, water, spoor en/of leiding).
6. Veiligheid beweegbare objecten (machineveiligheid)
Definitie: De veiligheid voor (vaarweg-, weg- en algemene) gebruikers en onderhouds- en bedienend personeel van machines.
7. Tunnelveiligheid
Het beperken van risico's voor personen die gebruikmaken van of zich bevinden in geheel omsloten wegconstructies.
8. Constructieve Veiligheid
Definitie: De veiligheid van personen met betrekking tot het bezwijken van een constructie.
9. Sociale Veiligheid
De mate waarin personen beschermd zijn en zich beschermd voelen tegen persoonlijk leed door misdrijven (criminaliteit), overtredingen en overlast door andere mensen.
10. Brandveiligheid
Definitie: De veiligheid van personen met betrekking tot brand en de gevolgen van brand voor een constructie.

11. Integrale Beveiliging

Definitie: De bescherming of veiligheid van inrichtingen, personen en infrastructuur tegen moedwillige verstoringen.

2.2 Toepasbaarheid Veiligheidsthema's

Om de veiligheidsaspecten toepasbaar te maken worden de veiligheidsthema's in Figuur 3 Allocatie Veiligheidsthema's geprojecteerd op de 6 domeinen en iCentrale Systeem. De dan verkregen matrix geeft aan welk veiligheidsthema van toepassing is of kan zijn bij implementatie van veiligheid voor iCentrale producten/diensten.

							
	iCentrale systeem	VERKEERSVEILIGHEID	ARBEIDSVEILIGHEID	NAUTISCHE VEILIGHEID	EXTERNE VEILIGHEID	VEILIGHEID BEWEEGBARE OBJECTEN	TUNNELVEILIGHEID
ARBEIDSVEILIGHEID (H4)	X		X	X			X
VERKEERSVEILIGHEID (H5)		X					
NAUTISCHE VEILIGHEID (H6)	X			X			
VEILIGHEID TEGEN OVERSTROMEN							
EXTERNE VEILIGHEID (H7)		X					
VEILIGHEID BEWEEGBARE OBJECTEN (H8)	X			X			X
TUNNELVEILIGHEID (H9)	X	X	X				
CONSTRUCTIEVE VEILIGHEID							
SOCIALE VEILIGHEID							
BRANDVEILIGHEID							
INTEGRALE BEVEILIGING (H10)	X	X	X	X	X	X	X

Figuur 3 Allocatie Veiligheidsthema's

Zoals is te zien, zijn van de 11 veiligheidsthema's er 7 van toepassing om als basis voor veiligheidskader te dienen. De van toepassing zijnde veiligheidsthema's worden per veiligheidsthema in een apart hoofdstuk uitgewerkt. De 4 niet behandelde thema's zijn minder van toepassing dan de overige thema's. Ze beschrijven aspecten zoals bijvoorbeeld veiligheid bij rampen, crisis en calamiteiten die de techniek van de iCentrale minder direct raken. De techniek van de iCentrale voorziet standaard al in communicatievoorzieningen voor dergelijke scenario's. De thema's moeten worden uitgewerkt aan de hand van personeel en scenario's en niet de techniek. Daarom worden in het vervolg van dit document niet meer beschouwd.

Als er een relatie van een thema met een domein is, is dit met een kruisje aangegeven. Dit is gedaan aan de hand van de bevindingen in bijlage 14.2

3 Gevolgde aanpak per veiligheidsthema

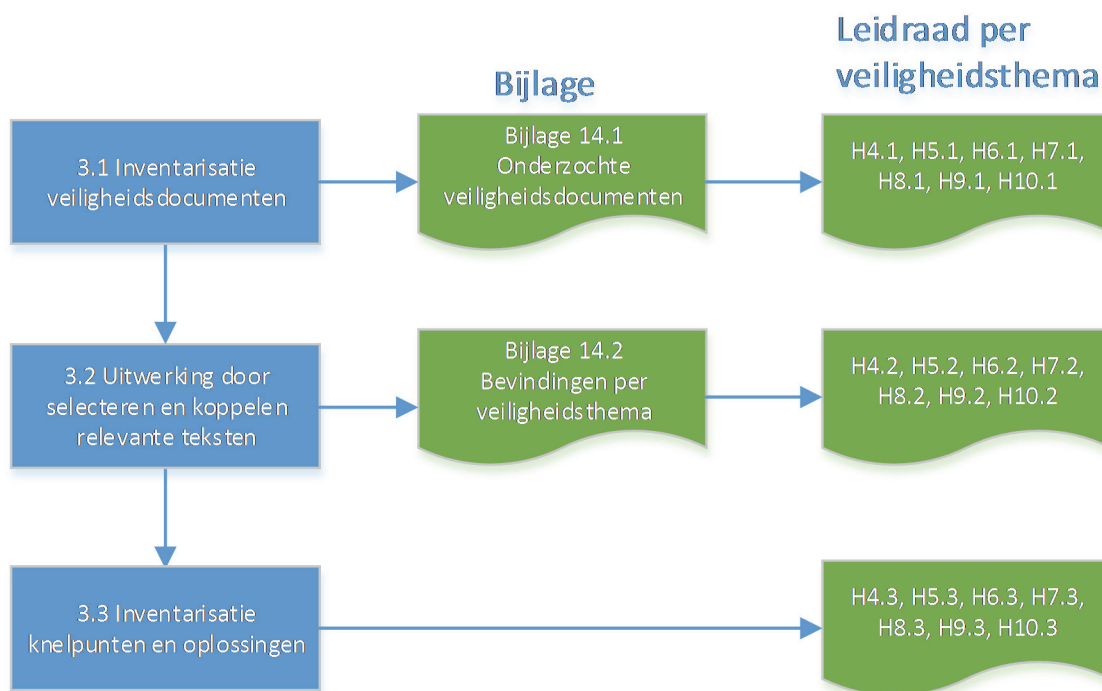
In Figuur 4 *Gevolgde aanpak per veiligheidsthema*, zijn de aanpak en de daarbij behorende resultaten weergegeven.

In 3.1 Inventarisatie *veiligheidsdocumenten* is beschreven hoe de inventarisatie per veiligheidsthema heeft plaatsgevonden. De totale uitwerking daarvan is vastgelegd in 14.1 *Onderzochte veiligheidsdocumenten*. De daadwerkelijk relevante documenten zijn weergegeven per veiligheidsthema in de hoofdstukken 4.1, 5.1, 6.1, 7.1, 8.1, 9.1, en 10. als onderdeel van de leidraad.

Per veiligheidsthema zijn de relevante teksten geselecteerd en gekoppeld aan systeemketen en zogeheten configuratie-items (zie 3.2) van de iCentrale product/dienst. Dit proces is beschreven in 3.2 *Uitwerking door selecteren en koppelen relevante teksten*.

De totale uitwerking daarvan is vastgelegd in 14.2 *Bevindingen per veiligheidsthema* en uitgewerkt in de hoofdstukken 4.2, 5.2, 6.2, 7.2, 8.2, 9.2 en 10.2.

Tot slot zijn van ieder veiligheidsthema knelpunten en daar waar mogelijk oplossingsrichtingen aangegeven in de hoofdstukken 4.3, 5.3, 6.2.3, 7.3, 8.3, 9.3 en 10.3.



Figuur 4 *Gevolgde aanpak per veiligheidsthema*

De stappen zijn doorlopen door middel van expert judgement. Er is geen gebruik gemaakt van standaard risicoanalysemethoden.

3.1 Inventarisatie veiligheidsdocumenten

Per veiligheidsthema is een inventarisatie gemaakt van relevante documenten.

Daarbij is gekeken op 4 bestuurlijke niveaus:

- Europees
- Nationaal
- Provinciaal
- Lokaal

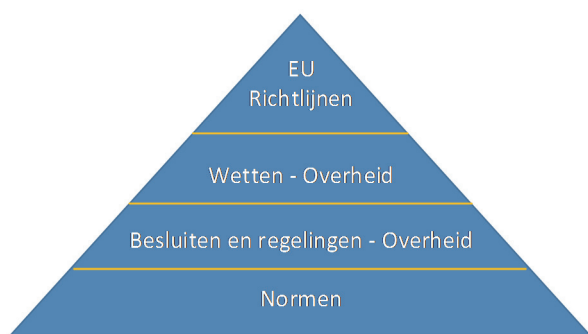
Binnen de bestuurlijke niveaus is gekeken naar de volgende soorten documenten:

- Richtlijnen
- Wetten
- Wettelijk verplichte bijlagen zoals meerjarenprogramma's
- Beleid
- Besluiten
- Regelingen/Reglementen
- Normen
- Beleid
- Visie
- Verordeningen

Deze documenten zijn onder te verdelen in:

- Verplichtingen in de vorm van regelgeving zoals wetten, besluiten en normen
- Beleid en visie om doelstellingen te realiseren

De regelgeving is als volgt opgebouwd:



Figuur 5 Regelgeving

3.1.1 Europese Richtlijnen

De Europese richtlijnen zijn van toepassing op producten, installaties, voorzieningen etc. . Elke Europese lidstaat is verplicht goedgekeurde richtlijnen op te nemen in een nationale wet.

3.1.2 Nationale Wet

Een nationale wet bevat algemene bepalingen, geen concrete regels en wordt daarom een kaderwet genoemd.

3.1.3 Besluiten en Regelingen

Uitwerking van de wet in de vorm van concrete regels.

Een besluit is een gedetailleerdere beschrijving van de wet. In een besluit staat verder uitgewerkt hoe (een deel van) de wet uitgelegd moet worden.

Een regeling wordt meestal afgeleid van een besluit. De regeling is de meest concrete uitleg van de wet.

3.1.4 Normen

Door private sector ontwikkeld om uniformiteit en eenduidigheid te bevorderen.

Ook de EU geeft de nationale normalisatie instituten opdracht een norm te maken, die past in een bepaalde Europese richtlijn.

Het toepassen van dit type norm geeft de fabrikant van een machine een 'vermoeden van overeenstemming' met de bepalingen van de richtlijn. Dit maakt het voor de fabrikant eenvoudiger om aan de richtlijn te voldoen.

Het is niet zonder meer verplicht normen toe te passen.

Normen zijn wel verplicht als deze:

- De overheid de norm in een wet of besluit vermeld
- De norm in een zakelijke overeenkomst wordt vermeld

Europese Normen welke machineveiligheid beschrijven zijn onverdeeld in 3 typen:

- Type A: Fundamentele veiligheidsnormen
- Type B1: Veiligheidsaspect
- Type B2: Veiligheidsmiddel
- Type C: Specifieke machinecategorie

Geharmoniseerde normen

De EU geeft in een aantal gevallen de nationale normalisatie instituten opdracht een norm te maken, die past in een bepaalde Europese richtlijn.

Als deze EN (Europese Norm) -normen zijn vastgesteld, worden ze gepubliceerd in het blad van de Europese gemeenschap. Vanaf dat moment zijn het geharmoniseerde normen.

Alle onderzochte documenten zijn opgenomen in 14.1. *Onderzochte veiligheidsdocumenten*.

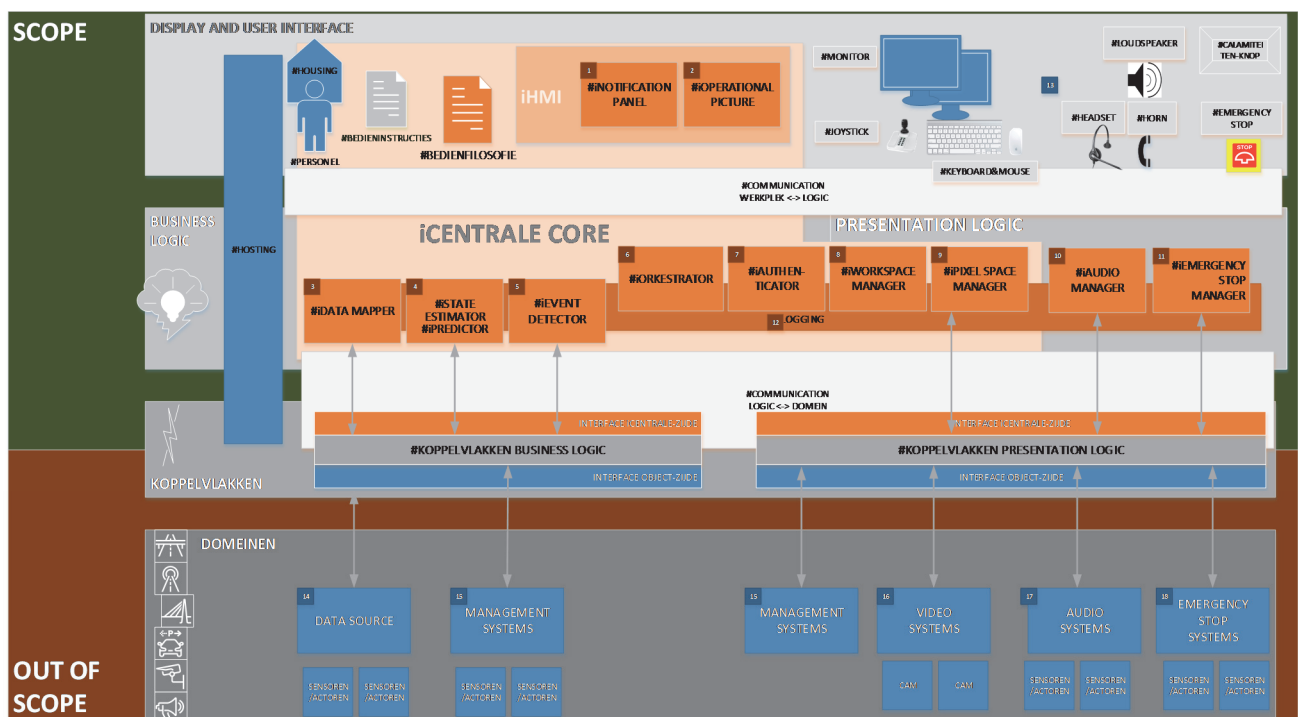
3.2 Uitwerking door selecteren en koppelen relevante teksten

Als er een relevante tekst gevonden is binnen een document in 14.1. *Onderzochte veiligheidsdocumenten*, dan is deze tekst vastgelegd in 14.2 Bevindingen *per veiligheidsthema* voorzien van naam, artikel / paragraaf en eventueel bladzijde.

Vervolgens wordt de tekst of een samenvatting daarvan gerelateerd door middel van een systeemketen en een **configuratie-item**. Een **configuratie-item** kan onderdeel zijn van een of meerdere systeemketens en is te beschouwen als een onderdeel van het geheel in 'scope' in Figuur 2 *Weergave reikwijdte veiligheid*. Een configuratie-item wordt voorafgegaan door een #. Een systeemketen is een keten voorzien van configuratie-items, welke tezamen een bepaalde functie vervullen.

Deze geabstraheerde weergave is verder uitgewerkt in 14.3 Configuratie-items veiligheid.

Zie voor de verkleinde weergave Figuur 6 *Snapshot configuratie-items veiligheid (14.3 Configuratie-items veiligheid)*



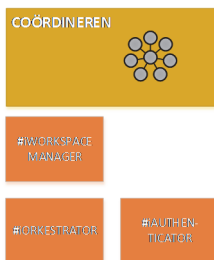
Figuur 6 Snapshot configuratie-items veiligheid (14.3 Configuratie-items veiligheid)

Zoals te zien is in deze figuur, zijn dit veel configuratie-items. Voor een aantal veiligheidsthema's is daarom gekozen om de uitwerking te richten op (systeem)functies die een rol hebben in de veiligheidsketen. Zo worden er gelijktijdig meerdere configuratie-items geïdentificeerd. Dit verhoogt de bruikbaarheid van deze leidraad.

De veiligheidsthema's waarvoor dit zo opgesteld wordt zijn *Verkeersveiligheid*, *Veiligheid Beweegbare Objecten* en *Tunnelveiligheid*.

3.2.1 (Systeem)Functie Coördineren

Coördineren vervult de centrale functie binnen het systeem. Bij binnenkomende events bepaald dit mechanisme bijvoorbeeld wat er met het event moet gebeuren en wie een taak ten gevolge van een event, moet afhandelen. Het betreft dus geen coördinatie door een persoon.



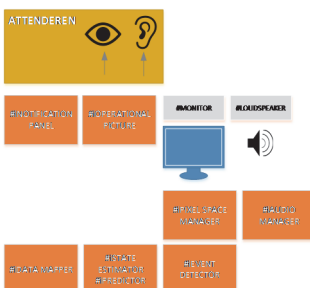
Figuur 7 Coördineren

3.2.2 (Systeem)Functie Attenderen

Attenderen betekent het visueel of auditief informeren van de gebruiker van het iCentrale-systeem. Attenderen heeft betrekking op de status of de verandering in status van relevante informatie uit een van de 6 domeinen of van het iCentrale systeem zelf.

Visueel attenderen gebeurt door middel van presentatie op het notificatie panel en/of operational picture.

Auditief attenderen gebeurt door middel van weergave van geluid op de luidspreker op de werkplek.



Figuur 8 Attenderen

3.2.3 (Systeem)Functie Observeren

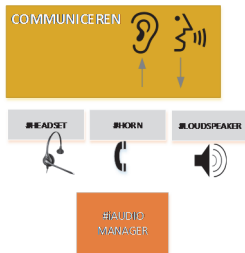
Observeren is het bekijken van camerabeelden. Hieronder valt ook het wijzigen van het gekozen camerabeeld door middel van beeldselectie of pan-, tilt-, zoom-acties.



Figuur 9 Observeren

3.2.4 (Systeem)functie Communiceren

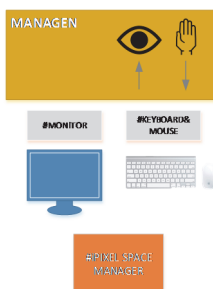
Communiceren houdt in: het verbaal communiceren met het beheersgebied/domein, maar ook binnen de iCentrale zelf.



Figuur 10 Communiceren

3.2.5 (Systeem)Functie Managen

Managen is het bedienen en bewaken van een beheersgebied via een managementsysteem (bijvoorbeeld SCADA-bediening van een brug).



Figuur 11 Managen

3.2.6 (Systeem)Functie Veilig Ingrijpen

Veilig Ingrijpen is het ingrijpen in een proces binnen een domein op technisch veilige wijze.



Figuur 12 VEILIG INGRIJPEN

3.2.7 Cross-reference configuratie-items <-> systeemfuncties

Configuratie Item	FUNCTIONELE SYSTEEMKETEN					
	Coördineren	Attenderen	Observeren	Communiceren	Managen	Veilig ingrijpen
#Notification panel		J				
#Operational picture		J			J	
#Monitor		J	J		J	
#Joystick			J			
#Keyboard&mouse		J	J		J	
#Headset				J		
#Horn				J		
#Loudspeaker				J		
#Calamiteitenknop						J
#Emergency stop						J
#Data mapper		J				
#State Estimator and predictor		J				
#Event detector		J				
#Orkestrator	J					
#Authenticator	J					
#workspace manager	J					
#pixelspace manager		J	J		J	
#Audio manager				J		
#Emergency stop manager						J
#koppelvlakken business logic					J	
#koppelvlakken presentation logic		J	J	J	J	J

Figuur 13 Cross-reference systeemfuncties met configuratie-items

3.3 Knelpunten inventarisatie en oplossingsrichtingen

Van alle kaders wordt per configuratie-item een groepering gemaakt en onderzocht op onderlinge tegenstrijdigheden en op tegenstrijdigheden met de architectuur (zie [3] Blauwdruk) van de iCentrale.

Voorts wordt dat knelpunt en indien mogelijk ook de oplossingsrichting opgenomen bij het betreffende veiligheidsthema of bij meerdere veiligheidsthema's.

4 Veiligheidsthema Arbeidsveiligheid

4.1 Inventarisatie documenten

Niveau	Regelingen	Opmerking
EU Richtlijnen	Richtlijn Arbeidsmiddelen	-
Wetten NL	Arbeidsomstandighedenwet	-
Besluiten en Regelingen NL	Arbeidsomstandighedenregeling Arbeidsomstandighedenbesluit	-
Normen en Visie	-	-
Provinciaal Beleid en Visie	-	-
Lokaal Beleid en Visie	-	-

Tabel 1 Inventarisatie documenten Arbeidsveiligheid

4.2 Uitwerking

4.2.1 Richtlijn arbeidsmiddelen

De doelstellingen uit deze Europese richtlijn zijn op nationaal niveau overgenomen in Arbowet, -besluit en -regelingen en worden daarom niet afzonderlijk behandeld.

Als er doelstellingen op hoog niveau moeten worden geformuleerd, geeft de richtlijn wel duidelijke teksten, die eventueel kunnen worden overgenomen.

4.2.2 Arbeidsomstandighedenwet

De Arbowet (voluit Arbeidsomstandighedenwet) is een kaderwet waarin geen concrete regels staan. Die zijn verder uitgewerkt in Arbobesluit en -regeling. Wel geeft de Arbowet de uitgangspunten voor beleid. De werkgever dient een arbobeleid te voeren gericht op zo optimaal mogelijke arbeidsomstandigheden en het veilig gebruik van arbeidsmiddelen (alle op de arbeidsplaats gebruikte machines, installaties, apparaten en gereedschappen). In dit beleid dient rekening gehouden te worden met onder andere de volgende zaken:

Artikel 3 Arbobeleid

- Werk heeft geen nadelige invloed op de veiligheid en de gezondheid van de werknemer.
#Personnel
- Gevaren en risico's voor de veiligheid of de gezondheid van de werknemer zoveel mogelijk bij de bron aanpakken.
#Personnel #Housing
- Inrichting van de arbeidsplaatsen, de werkmethoden en de bij de arbeid gebruikte arbeidsmiddelen, arbeidsinhoud worden zoveel mogelijk aangepast aan de persoonlijke eigenschappen van werknemers.
#Housing
- Monotone en tempo-gebonden arbeid wordt zoveel mogelijk beperkt.
#iOrkestrator #iOrkestrator.knelpunt1

- Doeltreffende maatregelen worden getroffen op het gebied van de eerste hulp bij ongevallen, de brandbestrijding en de evacuatie van werknemers en andere aanwezige personen, en doeltreffende verbindingen worden onderhouden met de desbetreffende externe hulpverleningsorganisaties.
- Elke werknemer moet bij ernstig en onmiddellijk gevaar voor zijn eigen veiligheid of die van anderen, rekening houdend met zijn technische kennis en middelen, de nodige passende maatregelen kunnen nemen om de gevolgen van een dergelijk gevaar te voorkomen.

Verder dient de werkgever, binnen het algemeen arbeidsomstandighedenbeleid, een beleid te voeren gericht op voorkoming en indien dat niet mogelijk is beperking van psychosociale arbeidsbelasting.

De verplichting van de werkgever om een hierop gericht beleid te voeren geldt ook voor de iCentrale. Bij uitbesteding van iCentrale-diensten aan een private partij wordt mogelijk verwacht dat dit beleid de verantwoordelijkheid van de private partij wordt. Dit dient zorgvuldig te worden getoetst omdat in principe taken wel, maar verantwoordelijkheden niet kunnen worden gedelegeerd.

#Personnel Artikel 5 Inventarisatie en evaluatie van risico's

Bij het voeren van het arbeidsomstandighedenbeleid legt de werkgever in een inventarisatie en evaluatie schriftelijk vast welke risico's de arbeid voor de werknemers met zich brengt. Deze risico-inventarisatie en -evaluatie bevat tevens een beschrijving van de gevaren en de risico-beperkende maatregelen en de risico's voor bijzondere categorieën van werknemers.

De verplichting om een risico-inventarisatie en -evaluatie ten aanzien van gevaren op de werkvloer vast te leggen geldt ook voor de werkgever (private partij) van de medewerkers van de iCentrale.

4.2.3 Arbobesluit

In het Arbobesluit zijn de uitgangspunten uit de Arbowet ('de wet') verder vormgegeven.

Artikel 3.4. Elektrische installaties

1. Elektrische installaties zijn zodanig ontworpen, ingericht, aangelegd, onderhouden en gekenmerkt, dat een veilig gebruik van elektriciteit zo goed mogelijk is gewaarborgd. Hiertoe zijn de nodige voorzieningen en beschermingsmaatregelen aangebracht. Daarbij is rekening gehouden met bijzondere eisen die kunnen voortkomen uit de wijze van het gebruik, de gebruiksomstandigheden, de te verwachten uitwendige invloeden en onderhoudswerkzaamheden.
2. In een elektrische installatie zijn doeltreffende maatregelen genomen tegen het gevaar van brand, ontploffing, directe en indirecte aanraking en te dichte nadering.
3. Van iedere elektrische installatie zijn duidelijke, steeds bijgewerkte schema's beschikbaar alsmede alle overige gegevens die nodig zijn voor een veilig gebruik van de elektrische installatie.
4. Het derde lid is niet van toepassing op elektrische installaties voor laagspanning van beperkte omvang.

#Housing #Hosting

Voor de iCentrale betekent dit dat de gebruikte elektrische installaties zullen moeten voldoen aan de hierboven genoemde voorschriften.

Aan de verplichtingen kan worden voldaan door het toepassen van de normen:

We gaan er hierbij vanuit dat de installaties laagspanningsinstallaties betreffen, welke zich in een 'gewone' omgeving bevinden.

- NEN 1010 Veiligheidsbepalingen voor laagspanningsinstallaties
- NEN 3140 Bedrijfsvoering van elektrische installaties – Laagspanning
- NEN-EN 50110 Bedrijfsvoering van elektrische installaties Deel 1: Algemene eisen

Artikel 3.5. Elektrotechnische, bedienings- en andere werkzaamheden aan of nabij een elektrische installatie

1. Elektrotechnische werkzaamheden en bedieningswerkzaamheden die gevaren kunnen opleveren, worden door deskundige, voldoende onderrichte en daartoe bevoegde werknemers uitgevoerd.
2. Een ruimte waarin zich een elektrische installatie voor hoogspanning bevindt waarvan de delen niet of onvoldoende zijn beschermd tegen directe of indirecte aanraking dan wel te dichte nadering, wordt slechts betreden in aanwezigheid van een tweede daartoe bevoegd persoon.
3. Werkzaamheden aan of in de nabijheid van een elektrische installatie worden slechts uitgevoerd, indien de installatie of het gedeelte waaraan of in de nabijheid waarvan wordt gewerkt, spanningsloos is.
4. De daartoe bevoegde werknemer neemt doeltreffende maatregelen om een veilig verloop van de werkzaamheden te waarborgen.
5. Het derde lid is niet van toepassing op werkzaamheden die worden verricht aan of in de nabijheid van een elektrische laagspanningsinstallatie, indien:
 - a. de dringende noodzaak van het onder spanning uitvoeren van die werkzaamheden is aangetoond;
 - b. tot het uitvoeren van die werkzaamheden door de daartoe bevoegde werknemer uitdrukkelijk opdracht is gegeven, en
 - c. de installatie tevens geschikt is voor het onder spanning uitvoeren van die werkzaamheden en door de daartoe bevoegde werknemer doeltreffende maatregelen zijn genomen om de aan die werkzaamheden verbonden gevaren te voorkomen.
6. Het derde lid is niet van toepassing op werkzaamheden die worden uitgevoerd aan of in de nabijheid van een elektrische installatie voor hoogspanning, bestaande uit:
 - a. het nemen en opheffen van veiligheidsmaatregelen, waaronder begrepen het met geschikt materieel knippen of schieten van kabels;
 - b. het uitvoeren van metingen en beproevingen, of
 - c. het reinigen van elektrisch materieel.
7. Werkzaamheden bestaande uit het reinigen van elektrisch materieel in een elektrische installatie voor hoogspanning als bedoeld in het zesde lid, onder c, worden slechts uitgevoerd, indien:
 - a. tot het uitvoeren van die werkzaamheden door de daartoe bevoegde werknemer uitdrukkelijk opdracht is gegeven;
 - b. gebruik wordt gemaakt van de voor deze werkzaamheden geschikte arbeidsmiddelen, reinigingsmiddelen en persoonlijke beschermingsmiddelen, en
 - c. de werknemers zich met de arbeidsmiddelen waarmee zij fysiek in contact staan, niet behoeven te begeven in de gevarenzone van de installatie of delen daarvan die onder spanning staan.

#Housing #Hosting

Voor de iCentrale betekent dit dat elektrotechnische, bedienings- en andersoortige werkzaamheden aan of nabij de aanwezige elektrische installaties moeten plaatsenvinden op de hierboven beschreven wijze.

Aan de verplichtingen van artikel 3.4 en 3.5 kan worden voldaan door het toepassen van de normen:

- NEN 1010 Veiligheidsbepalingen voor laagspanningsinstallaties
- NEN 3140 Bedrijfsvoering van elektrische installaties – Laagspanning
- NEN-EN 50110 Bedrijfsvoering van elektrische installaties Deel 1: Algemene eisen

We gaan er hierbij vanuit dat de installaties laagspanningsinstallaties betreffen, welke zich in een 'gewone' omgeving bevinden.

#Personnel

#Housing

Artikel 5.2 Voorkomen gevaren

De arbeid wordt zodanig georganiseerd, de arbeidsplaats wordt zodanig ingericht, een zodanige productie- en werkmethode wordt toegepast of zodanige hulpmiddelen en persoonlijke beschermingsmiddelen, worden gebruikt, dat de fysieke belasting geen gevaren met zich kan brengen voor de veiligheid en de gezondheid van de werknemer.

Tenzij dit redelijkerwijs niet kan worden geleverd worden werkplekken ingericht volgens de ergonomische beginselen.

De noodzaak van de werkgever (private partij) om werkplekken ergonomisch in te richten om de veiligheid en gezondheid niet te schaden geldt ook voor de iCentrale, tenzij dit tot redelijkerwijs niet mogelijk is.

#Housing

Artikel 5.9. Risico-inventarisatie en -evaluatie

In de risico-inventarisatie en -evaluatie, bedoeld in artikel 5 van de wet, wordt specifiek aandacht besteed aan de gevaren voor het gezichtsvermogen en die van de fysieke en psychische belasting als gevolg van arbeid aan een beeldscherm.

Beeldschermarbeid zal voor medewerkers van de iCentrale een essentieel onderdeel van de werkzaamheden zijn. De werkgever is verplicht hieraan in de eerder genoemde risico-inventarisatie en -evaluatie afdoende aandacht te besteden.

Artikel 5.10. Dagindeling van de arbeid

#iOrkestrator De arbeid aan een beeldscherm is zodanig georganiseerd dat deze arbeid telkens na ten hoogste twee achtereenvolgende uren wordt afgewisseld door andersoortige arbeid of door een rusttijd, zodanig dat de belasting van het verrichten van de arbeid aan een beeldscherm wordt verlicht.

De werkgever (DCO of private partij) is verplicht de arbeid zodanig te organiseren dat de werknemers ten hoogste twee achtereenvolgende uren beeldschermarbeid verrichten.

#Housing

Artikel 5.12. Voorschriften voor de inrichting van beeldschermwerkplekken

Onverminderd artikel 5.4 worden bij ministeriële regeling nadere regels gesteld met betrekking tot de beeldschermwerkplek en de wisselwerking tussen de gebruikte apparatuur en de werknemers.

#Housing Artikel 6.12I. Maatregelen ter voorkoming of beperking van de blootstelling

Er worden zodanige maatregelen genomen dat de risico's voor werknemers ten gevolge van elektromagnetische velden op de arbeidsplaats worden weggenomen dan wel tot een minimum beperkt, waarbij rekening wordt gehouden met de technische vooruitgang en de beschikbaarheid van maatregelen om het ontstaan van elektromagnetische velden aan de bron te beheersen.

#Housing

Artikel 7.13. Besturingssysteem en bedieningsorgaan

1. Een besturingssysteem van een arbeidsmiddel is veilig.
2. Een besturingssysteem levert ook bij onopzettelijke handelingen geen gevaar op voor de werknemers.
3. Bij de keuze van een besturingssysteem wordt rekening gehouden met defecten, storingen en belastingen die bij het gebruik van het besturingssysteem kunnen worden verwacht.
4. Een bedieningsorgaan is duidelijk zichtbaar en herkenbaar en is daartoe, waar nodig, op passende wijze van functionele aanduidingen voorzien.
5. Een bedieningsorgaan bevindt zich zoveel mogelijk buiten de gevaarlijke zone van het arbeidsmiddel.
6. De plaats van het bedieningsorgaan levert geen extra gevaren op voor de werknemers.
7. Indien een arbeidsmiddel in werking kan worden gesteld of kan worden gestopt op een plaats van waar dat arbeidsmiddel niet geheel kan worden gezien, wordt, om de betrokken werknemers te beschermen, telkens tijdig voor het inwerkingstellen of stoppen van dat

arbeidsmiddel een signaal gegeven dat voldoet aan het bij of krachtens afdeling 2 van hoofdstuk 8 bepaalde.

Besturingssystemen en bedieningsorganen dienen veilig te gebruiken te zijn door de medewerkers van de iCentrale. De werkgever (DCO of private partij) dient bovenstaande voorschriften daarom na te leven.

Bovenstaand kan van toepassing zijn op de werkplek (bureau) zelf binnen een iCentrale. De besturingssystemen en bedieningsorganen binnen het beheersgebied/domein zijn buiten scope.

Artikel 7.15. Stopzetten van arbeidsmiddelen

1. Een arbeidsmiddel kan op veilige wijze worden stopgezet met een daarvoor bestemd bedieningsorgaan. Een besturingssysteem stopt naar gelang het gevaar hetzij het gehele arbeidsmiddel hetzij onderdelen daarvan, zodanig dat het arbeidsmiddel in een veilige toestand is.

Zie verder in betreffende document.

Medewerkers van de iCentrale moeten alle op de arbeidsplaats gebruikte machines, installaties, apparaten en gereedschappen veilig kunnen stopzetten. De iCentrale is verplicht hiervoor te zorgen. Bij bediening op afstand van bijvoorbeeld sluizen, bruggen, tunnels, parkeervoorzieningen moeten ook deze veilig stilgezet kunnen worden.

Hierin wordt voorzien door de managementsystemen, welke het beheersgebied/domein bedienen, maar buiten scope zijn.

#iEmergency stop manager #iEmergency Stop #koppelvlakken presentation logic

Artikel 7.16. Noodstopvoorziening

Een arbeidsmiddel beschikt over een noodstopvoorziening, indien dit met het oog op de gevaren van dat arbeidsmiddel en de normale tijd die nodig is om dat arbeidsmiddel stop te zetten noodzakelijk is.

Gevaarlijke machines, installaties, apparaten en gereedschappen die niet direct tot stilstand komen moeten beschikken over een noodstopvoorziening. De iCentrale is verplicht hieraan te voldoen. Bij bediening op afstand van bijvoorbeeld sluizen, bruggen, tunnels, parkeervoorzieningen moeten ook deze met een noodstop stilgezet kunnen worden.

4.2.4 Arbeidsomstandighedenregeling

In de Arbeidsomstandighedenregeling zijn de bepalingen uit het Arbobesluit ('de wet') verder vormgegeven.

Artikel 5.1. Apparatuur en meubilair **#Housing**

Apparatuur en meubilair, in gebruik bij het verrichten van beeldschermwerk, voldoen in ieder geval aan de volgende voorschriften:

- a. de tekens op het beeldscherm zijn voldoende scherp, duidelijk van vorm en voldoende groot, met voldoende afstand tussen de tekens en de regels;
- b. het beeld op het beeldscherm is stabiel; **#Monitor**
- c. de luminantie van of het contrast tussen de tekens en de achtergrond is gemakkelijk door de gebruiker bij te stellen; **#Monitor**
- d. het beeldscherm is vrij te plaatsen en gemakkelijk verstelbaar en kantelbaar; **#Monitor**
- e. het beeldscherm is vrij van voor de gebruiker hinderlijke glans en spiegelingen; **#Monitor**
- f. het toetsenbord kan hellend worden geplaatst en vormt geen geheel met het beeldscherm; **#Keyboard&mouse**
- g. er is voor het toetsenbord voldoende ruimte voor handen en armen van de gebruiker;
- h. het toetsenbord heeft een mat oppervlak; **#Keyboard&mouse**
- i. de indeling van het toetsenbord en de vorm van de toetsen zijn gericht op vergemakkelijking van het gebruik; **#Keyboard&mouse**
- j. de symbolen op de toetsen zijn voldoende contrastrijk en vanuit een normale werkhouding voldoende leesbaar; **#Keyboard&mouse**

- k. de werktafel of het werkvlak maakt een comfortabele houding van de gebruiker mogelijk en heeft een reflectiearm oppervlak, is voldoende groot en maakt een flexibele opstelling van beeldscherm, toetsenbord, documenten en accessoires mogelijk;
- l. een voor het werk noodzakelijke documenthouder is stabiel en regelbaar en zodanig geplaatst dat oncomfortabele hoofd- en oogbewegingen tot een minimum zijn beperkt;
- m. de werkstoel is stabiel, heeft een in hoogte verstelbare zitting en een rugleuning, waarvan de hoogte en hellingshoek verstelbaar zijn en geeft de gebruiker bewegingsvrijheid en een comfortabele werkhouding;
- n. indien de gebruiker dat wenst wordt een voetensteun aangebracht.

Ten aanzien van beeldschermwerk op de iCentrale dient de werkgever (DCO of private partij) ervoor te zorgen dat apparatuur en meubilair voldoet aan bovengenoemde voorschriften.

Artikel 5.2. Inrichting van de beeldschermwerkplek **#Housing**

De omgeving waarin het beeldschermwerk wordt verricht en de inrichting van de beeldschermwerkplek voldoen in ieder geval aan de volgende voorschriften:

- a. de verlichting van de werkruimte of de beeldschermwerkplek zorgt voor voldoende licht en een passend contrast tussen beeldscherm en omgeving, rekening houdende met de aard van het werk en de visuele behoeften van de gebruiker;
- b. mogelijke verblinding en hinderlijke reflecties op het beeldscherm of op apparaten door kunstmatige lichtbronnen zijn vermeden;
- c. er treden door raam- en andere openingen, wanden en apparaten geen directe verblinding en hinderlijke reflecties op het beeldscherm op;
- d. de ramen zijn uitgerust met passende instelbare helderheidswering om de intensiteit van het licht dat op de beeldschermwerkplek valt te verminderen;
- e. het geluid dat de apparatuur voortbrengt veroorzaakt geen verstoring van de aandacht en het gesproken woord; **#Loudspeaker #Loudspeaker.knelpunt1 #iAudiomanager.knelpunt1**
- f. de apparatuur brengt geen voor de werknemers hinderlijke warmte voort; **#Hosting #Housing.knelpunt1**
- g. de vochtigheidsgraad is steeds toereikend.

Ten aanzien van de beeldschermwerkplekken op de iCentrale dient de werkgever (private partij) ervoor te zorgen dat voldaan is aan bovengenoemde voorschriften.

Artikel 5.3. Programmatuur

De programmatuur die wordt gebruikt bij het verrichten van beeldschermwerk voldoet in ieder geval aan de volgende voorschriften:

- a. de programmatuur is aangepast aan de te verrichten taak; **#iOrkestrator**
- b. de programmatuur is gemakkelijk te gebruiken en aan te passen aan het kennis- en ervaringsniveau van de gebruiker; **#iOrkestrator**
- c. er wordt zonder medeweten van de gebruiker geen gebruik gemaakt van een kwantitatief of kwalitatief controlemechanisme; **#iOrkestrator #iLogging**
- d. de systemen verschaffen de gebruiker gegevens over de werking ervan; **#Bedieninstructies**
- e. de systemen maken de informatie zichtbaar in een vorm en een tempo die zijn aangepast aan de gebruiker;
- f. bij de verwerking van informatie door de gebruiker worden de beginselen van de ergonomie toegepast.

Ten aanzien van de programmatuur voor beeldschermwerk op de iCentrale dient de werkgever (DCO of private partij) ervoor te zorgen dat voldaan is aan bovengenoemde voorschriften.

4.2.5 Overig

Geen

4.3 Knelpunteninventarisatie en Oplossingsrichtingen

1
Knelpunt Arbeidsveiligheid.#iOrkestrator.knelpunt.1
Monotone en tempo-gebonden arbeid moet zoveel mogelijk worden beperkt. Dit kan in conflict komen met de Business Logic waarin zoveel mogelijk wordt geautomatiseerd en de gebruiker een afhandelaar van triggers wordt.
Oplossingsrichting
Toets het Business Logic mechanisme op monotone en tempo-gebonden arbeid en stel het mechanisme zo nodig bij.
2
Knelpunt Arbeidsveiligheid.#Loudspeaker.knelpunt.1
Het geluid dat de apparatuur voortbrengt veroorzaakt geen verstoring van de aandacht en het gesproken woord; Bij het combineren van centrale bewaking en bediening van meerdere domeinen kunnen de operators gestoord worden door geluid wat niet voor hen bestemd is. Bijvoorbeeld marifooncommunicatie welke niet voor een tunneloperator bedoeld is.
Oplossingsrichting
Zorg voor een doordachte opstelling van de luidsprekers en maak zoveel mogelijk gebruik van (open) headsets. Akoestische maatregelen in het gebouw (vloerbedekking, geluidsabsorberende wanden en plafonds, gordijnen etc.
3
Knelpunt Arbeidsveiligheid.#iAudiomanager.knelpunt.1
Het geluid dat de apparatuur voortbrengt veroorzaakt geen verstoring van de aandacht en het gesproken woord; Bij het combineren van centrale bewaking en bediening van meerdere domeinen kunnen de operators gestoord worden door geluid dat niet voor hen is bedoeld.
Oplossingsrichting
Maak bij de verschillende domeinen onderscheid in verschillende attentiesignalen. Zorg dat de operators zoveel mogelijk individueel worden geïnformeerd en geattendeerd.
4
Knelpunt Arbeidsveiligheid.#Housing.knelpunt.1
De apparatuur brengt geen voor de werknemers hinderlijke warmte voort.
Oplossingsrichting
Plaats bij voorkeur de apparatuur in een technische ruimte.

5 Veiligheidsthema Verkeersveiligheid

5.1 Inventarisatie documenten

Niveau	Regelingen	Opmerking
EU Richtlijnen	RICHTLIJN 2008_96_EG - Beheer van de verkeersveiligheid van weginfrastructuur	
Wetten NL	Wegenwet Wegenverkeerswet Meerjarenprogramma Infrastructuur Rijksinfrastructuurfonds Wet beheer Rijkswaterstaatswerken	
Besluiten en Regelingen NL	Beleidsregels Incident Management Rijkswaterstaat Besluit Algemene Regels Ruimtelijke Ordening Structuurvisie Infrastructuur en Ruimte	
Normen en Visie	Ministerie van V&W - Strategie Verkeersveiligheid 2008-2020	
	Ministerie van V&W - Strategisch plan Verkeersveiligheid 2008-2020	
	RWS Richtlijn Wegwerkzaamheden 2012	
Landelijke beleid en Visie	Ministerie van Verkeer en Waterstaat - Strategie verkeersveiligheid 2008-2020	
	Ministerie van Verkeer en Waterstaat - Strategisch plan Verkeersveiligheid-2008-2020	
	Meerjarenprogramma Infrastructuur	
Provinciaal Beleid en Visie	Meerjarenprogramma Infrastructuur p-MIRT	
Lokaal Beleid en Visie		
Achtergrond kennis en Visie	Architectuur voor Verkeersbeheersing (AVB) - Verkeerskundige Architectuur (VA)	
Overig	ProMeV - Proactief Meten Verkeersveiligheid	

Tabel 2 Inventarisatie documenten Verkeersveiligheid

5.2 Uitwerking

Wegbeheerders

Nederland kent de volgende wegbeheerders:

- ›Het Rijk
- ›Provincies
- ›Waterschappen
- ›Gemeenten
- ›Overige (havenbedrijf, huiseigenaren, spoorwegbeheerder (ProRail) , etc.)

Beleid

Het verkeersbeleid wordt veelal onderverdeeld in de volgende drie onderwerpen:

- Bereikbaarheid;
- Veiligheid;
- Leefbaarheid.

Omdat dit project de veiligheidskaders behandelt, zullen we enkel het onderdeel veiligheid verder uitwerken.

De verkeersveiligheid kan toenemen door middel van het voeren van beleid.

De uitvoering van dit beleid is opgenomen in de structuurvisie infrastructuur en ruimte (SVIR).

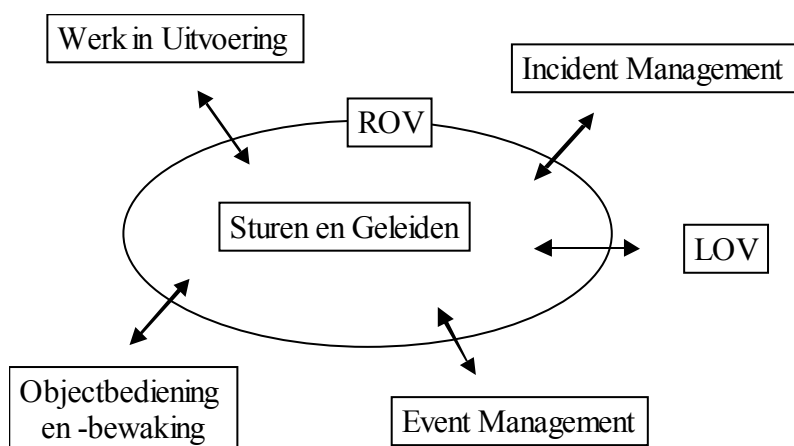
Regionaal verkeersmanagement

Regionaal verkeersmanagement of regionale operationele verkeersbeheersing kent een zestal hoofdtaken welke in de volgens de Architectuur voor Verkeersbeheersing (AVB) - Verkeerskundige Architectuur (VA) als volgt zijn samengevat:

- Sturen en Geleiden (S&G), d.i. inzetten van verkeersbeheersingmaatregelen gericht op het bevorderen van de doorstroming, veiligheid, comfort en leefbaarheid in het gehele wegennetwerk;
- Ondersteunen Werk in Uitvoering (WIU), d.i. inzetten van verkeersbeheersingmaatregelen ten behoeve van geplande wegwerkzaamheden;
- Ondersteunen Event Management (EM), d.i. inzetten van verkeersbeheersingmaatregelen ten behoeve van geplande of optredende evenementen;
- Ondersteunen Incident Management (IM), d.i. inzetten van verkeersbeheersingmaatregelen ten behoeve van optredende incidenten;
- Ondersteunen Object Bediening en Bewaking (OB), d.i. inzetten van verkeersbeheersingmaatregelen ten behoeve van het bedienen en bewaken van infrastructurele objecten;
- Ondersteunen Landelijke Operationele Verkeersbeheersing (LOV), d.i. inzetten van verkeersbeheersingmaatregelen uit het oogpunt van landelijke operationele verkeersbeheersing.

De hoofdtaken van regionale operationele verkeersbeheersing (ROV) zijn geschetst in Figuur 14.

N.B. De hoofdtak "ondersteunen Object Bediening en Bewaking (OB)" ligt in lijn met tunnelveiligheid en Veiligheid Beweegbare Objecten.



↔ = ondersteunende taak ROV i.r.t. andere deeldomeinen

Figuur 14. Hoofdtaken van regionale operationele verkeersbeheersing (ROV) (bron: AVB-VA)

De wijze van uitvoering van deze hoofdtaken is niet vastgelegd in richtlijnen. Omgekeerd kunnen deze hoofdtaken wel bewust worden ingezet vanuit een iCentrale ter ondersteuning van het generieke verkeersveiligheidsbeleid. Daarmee wordt vanuit verkeersbeheersing de link gelegd met de Richtlijn 2008/96/EG van het Europese Parlement en de raad van 19 november 2008 betreffende het beheer van de verkeersveiligheid van weginfrastructuur, welke overigens sec geldt voor het trans-Europese wegennet. Conform deze richtlijn heeft een wegbeheerder de verantwoordelijkheid voertuigbestuurders te waarschuwen **#Bedieninstructies** **#Bedienfilosofie** wanneer ze zich begeven op een gedeelte van een weg met een hoog aantal ongevallen, zodat ze hun gedrag kunnen aanpassen en de verkeersregels, en met name de snelheidsbeperkingen, nog beter kunnen naleven. Van oudsher gaat dat via bebording langs de kant van de weg. Verkeersbeheersing biedt de mogelijkheid dit dynamisch (d.i. afgestemd op de verkeersvraag, de toestand van de weg en het weer van dat moment) te doen vanuit een verkeerscentrale. In dit geval een iCentrale.

Hoewel de genoemde richtlijn geldt voor het trans-Europese wegennet en niet per definitie voor wegen onder beheer bij DCO's, sluit het gedachtegoed van de richtlijn één-op-één aan bij het Strategisch Plan Verkeersveiligheid 2008-2020 van het Ministerie van Infrastructuur en Waterstaat en bij de eigen insteek in meerjarenprogramma's infrastructuur van bijvoorbeeld provincies.

5.3 Knelpunteninventarisatie en Oplossingsrichtingen

1
Knelpunt Verkeersveiligheid. #iData Mapper.Knelpunt1
Zodra een iCentrale bewust inzet op het verbeteren van de verkeersveiligheid via dynamische informatie, waarschuwingen en adviezen aan weggebruikers, wordt omgekeerd de claim op de beschikbaarheid en correctheid van deze informatie, waarschuwingen en adviezen en daarmee de achterliggende iCentrale groter.
Oplossingsrichting
Implementeren van de eisen, wensen en aanbevelingen vanuit het project 4.3 Beschikbaarheid en Performance.

2
Knelpunt Verkeersveiligheid. #iEvent detector.Knelpunt1
Door het triggerbased werken kan de operator de momentane veiligheidsniveaus onvoldoende bewaken.
Oplossingsrichting
• Definiëren van de KPI's die uitdrukking geven aan het momentane veiligheidsniveau van een traject of route; • Per corridors of route definiëren van de drempelwaardes horende bij een acceptabel en onacceptabele veiligheidsniveau; • Definiëren van de wegverkeersdata, waarmee de actuele waarde van de KPI's kan worden vastgesteld.

3
Knelpunt Verkeersveiligheid. #iHMI.Knelpunt 1 Knelpunt Verkeersveiligheid.#iEvent detector.Knelpunt1 Knelpunt Verkeersveiligheid.#iData Mapper.Knelpunt2
Door het triggerbased werken kan de operator onvoldoende beeld opbouwen en bijhouden van het momentane veiligheidsniveau en hiernaar handelen wanneer dit veiligheidsniveau onacceptabel wordt.
Oplossingsrichting
In de iHMI uitdrukking geven aan het momentane veiligheidsniveau van de corridors in het beheergebied van de iCentrale, opdat hierop kan worden gestuurd. In de iEvent Generator triggers opnemen, die een drempelwaarde aangeven wat betreft het acceptabel en onacceptabele veiligheidsniveau van een corridor en route. In de iData Mapper de wegverkeersdata vergaren, waarmee de actuele waarde van de KPI's kan worden vastgesteld. Werkzaamheden welke langer aandacht nodig hebben, bijvoorbeeld voor beeldopbouw, voorzien van trigger en voldoende afhandeltijd.

6 Veiligheidsthema Nautische veiligheid

6.1 Inventarisatie documenten

Niveau	Regelingen	Opmerking
EU Richtlijnen		
Wetten NL	Scheepvaartverkeerswet	
Besluiten en Regelingen NL		
Normen en Visie	Binnenvaartpolitiereglement Regeling communicatie en afmetingen rijksbinnenwateren Richtlijnen Vaarwegen	
Provinciaal Beleid en Visie	-	
Lokaal Beleid en Visie	-	
Overig	Recommendation on Vessel Traffic Services in Inland Waters	
	RIS Guidelines	
	STIS (Scheepvaart Transport Informatie Systeem, later RIS-NL) - Referentiemodel voor de scheepvaart	
	COMPRIS - RIS Architecture	

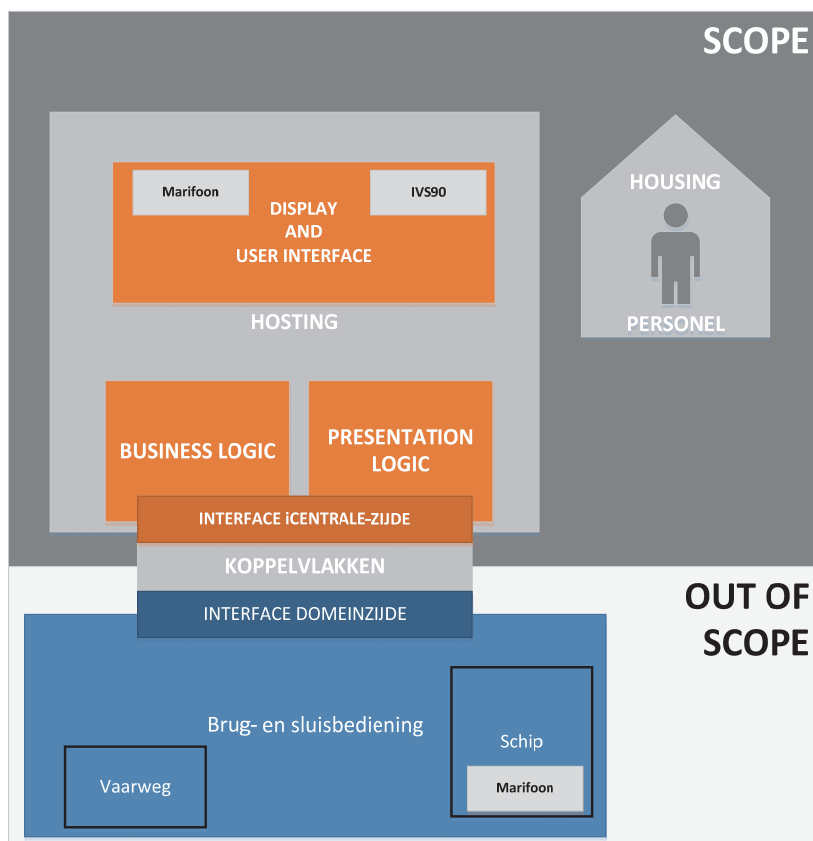
Tabel 3 Inventarisatie documenten Nautische veiligheid

6.2 Uitwerking

Nautische veiligheid komt met een drietal hoofdtaken, namelijk:

- Verkeersbegeleiding (in sommige gevallen in lijn met de richtlijnen voor Vessel Traffic Services – VTS)
- Brug-/sluisbeheer
- Ondersteunen bij incident- en calamiteitenbestrijding

De relatie tussen Nautische Veiligheid en iCentrale producten/diensten ligt vooral in het domein van Brug- en Sluisbediening. Dit domein heeft op zijn beurt weer een relatie met Veiligheid van Beweegbare Objecten. Zie hiervoor 8 Veiligheidsthema Veiligheid beweegbare objecten. Om scheepvaartverkeer veilige doorstroming langs de bruggen en sluizen te bieden, vereist een samenspel tussen mens en techniek. Alles wat gerelateerd is aan het schip en/of de bemanning wordt onder Nautische Veiligheid beschouwd. Eendachtig de scope zoals aangeduid in Figuur 2 Weergave reikwijdte veiligheid levert dit voor Nautische Veiligheid het volgende op.



Figuur 15 IVS90 en Marifoon in scope, schip en vaarweg buiten scope

6.2.1 Verkeersbegeleiding en brug- en sluisbeheer

Scheepvaart kent een drietal bedrijfsprocessen die in elkaars verlengde liggen, namelijk: verkeersbegeleiding, schutten van schepen bij sluisen en bedienen van bruggen om de scheepvaart door te laten.

In strikte zin richt verkeersbegeleiding zich op 'de verbetering van een veilige en vlotte afwikkeling van het verkeer over de vaarweg en de bijdrage aan de veiligheid van mens en milieu in relatie tot transport van goederen, personen en dieren over water'. Het schutten van sluisen en bedienen van bruggen sluit hierop aan.

Ten aanzien van nautische veiligheid kunnen drie niveaus worden onderscheiden voor de taakuitvoering, namelijk:

- Netwerkbrede informatievoorziening – netwerkbreed en proactief ondersteunen van de scheepvaart door gebundelde informatievoorziening (bijvoorbeeld gebundeld naar (hoofd)transportassen, of vaargebieden voor de recreatievaart). Deze informatie sluit aan bij de informatiebehoefte bij het opstellen en onderhouden van de reisplanning. Dit vraagt om samenwerking over de beheergrenzen heen en tussen verkeersbegeleiders in verkeersposten en de operators op sluisen en bruggen. Met proactief wordt bedoeld, waar mogelijk problemen zich gaan voordoen (zoals verwachte waterstanden, verwachte verkeersdrukte of geplande stremmingen);
- Strategische verkeersbegeleiding – rond een specifiek gebied begeleiden van de scheepvaart, door bijvoorbeeld mogelijke routes aan te duiden, of het scheepvaartverkeer pogen te spreiden in de tijd. Zo'n specifiek gebied kan zijn een kritisch knooppunt, traject, of bocht in de vaarweg, het gebied rond een sluis of sluisencomplex of een beweegbare brug;
- Tactische verkeersbegeleiding – binnen het specifieke gebied begeleiden van de scheepvaart.

Deze drie niveaus hangen samen met een geografische en tijdshorizon. Strategische taken zijn gekoppeld aan een groter beheergebied en kennen een langere tijdscope. Tactische taken zijn gekoppeld aan de directe omgeving en kennen een korte tijdscope.

Netwerkbrede informatievoorziening raakt aan de reisplanning van het schip of de boot. Vanuit verkeersmanagement oogpunt willen we:

- degenen, die de reisplanning verzorgen en bewaken, en de verkeersbegeleider(s) voorzien van nautische informatie:
 - de toestand van de vaarweg (zoals bevaarbare dieptes, c.q. ondieptes of stremmingen)
 - de actuele en verwachte waterstanden, weersomstandigheden en de invloed van de weersomstandigheden op de waterstanden (hydro- en meteo-informatie);
- degenen, die de reisplanning verzorgen en bewaken, en de verkeersbegeleider(s) voorzien van globale verkeersinformatie:
 - de actuele en verwachte verkeerssituatie op het vaarwegnetwerk, opdat de schepen eventueel hun route of reisplanning kunnen bijstellen;
 - de voorkeursroutes voor de verschillende doelgroepen op specifieke momenten in de tijd (bijvoorbeeld beroepsvaart en recreatievaart, gevaarlijke stoffen versus geen gevaarlijke stoffen);
- waar nuttig en nodig degenen, die de reisplanning verzorgen en bewaken, voorzien van sociale en bedrijfseconomische informatie:
 - mogelijkheden tot bunkeren en inslaan van proviand;
 - afgifte van afval
 - overzicht van ligplaatsen, wachtplaatsen, of plaatsen waar de auto van boord kan;
 - recreatiemogelijkheden;
- teneinde een beeld te krijgen van de verkeerssituatie, van degenen die de reisplanning verzorgen en bewaken, vernemen:
 - wat het vaarplan is en wanneer zij het beschouwde vaarwegnetwerk binnenvaren, respectievelijk weer uitvaren;
 - wat de intenties zijn ten aanzien van al dan niet opzoeken van een ligplaats;
 - wat het scheepstype en de lading is (met oog op informeren doelgroepen);

Via een dergelijke interactie en informatie-uitwisseling beoogt de verkeersbegeleider een actueel beeld te behouden van de verkeerssituatie op het vaarwegnetwerk.

Een strikte vorm van verkeersbegeleiding is het bieden van Vessel Traffic Services (VTS) conform de richtlijnen van IALA. VTS stelt strikte eisen aan de opleiding en certificering van verkeersbegeleiders en aan de wijze waarop een VTS-dekkingsgebied is uitgerust met radars en camera's om een sluitend beeld te hebben van de scheepvaart in het dekkingsgebied.

Het Informatie- en Volgsysteem voor de Scheepvaart (IVS90) draagt bij aan een vlotte en veilige doortocht van schepen. Door dit systeem zijn sluizen, verkeersposten en enkele bruggen op de meeste Nederlandse vaarwegen met elkaar verbonden. IVS90 is bestemd voor alle schepen die gebruikmaken van de Nederlandse hoofdvaarwegen, maar richt zich met name op de binnenvaart. Door middel van het systeem registreert een schipper zijn scheeps- en ladingsgegevens. Na aanmelding bij een IVS-post blijven de relevante gegevens langs de hele vaarroute beschikbaar. De gegevens van een schip hoeven niet telkens opnieuw te worden doorgegeven. Dit bevordert een snelle gang van zaken bij sluizen, bruggen en verkeersposten. Hierdoor kunnen schippers op schema varen en hun lading op tijd afleveren. IVS90 bevordert bovendien de hulpverlening bij calamiteiten op het water. Door het systeem is namelijk bekend waar een schip zich bevindt, hoeveel personen er aan boord zijn en wat de lading is. Daardoor kunnen hulpdiensten direct en doelgericht optreden. Op die manier kan persoonlijk leed worden voorkomen en kan ook de schade aan de lading en het milieu worden beperkt. De informatie uit IVS90 is bij calamiteiten dus onontbeerlijk, wat IVS90 tot een missie-kritieksysteem maakt.

Alle informatie die met IVS90 wordt verzameld geeft een duidelijk beeld van de totale scheepvaart op de hoofdvaarwegen in bepaalde periodes. De informatie uit IVS90 is niet alleen belangrijk voor Rijkswaterstaat maar ook voor regionale waterbeheerders en havens. Met de gegevens uit het systeem kunnen zij beter adviseren over transport op het water.

Bij deelname aan scheepvaartverkeer op scheepvaartwegen dient het schip communicatiemiddelen aan boord te hebben. De meest bekende is de marifoon. De marifoon (maritieme telefoon) is, anders dan zijn naam doet vermoeden, geen telefoon maar een zendontvanger. De marifoon is bedoeld voor gebruik in de maritieme communicatie en in het nautische berichtenverkeer over korte afstand. Het apparaat kan zenden en ontvangen in de VHF-band. De plaatsing en bediening van een marifoon is aan wettelijke regels gebonden. De marifoon is een belangrijk communicatiemiddel aan boord. Op de grote rivieren zoals: de Waal, de Rijn, de Noord enz. hebben grotere schepen de verplichting om minimaal twee marifoons aan boord te gebruiken: één voor het onderling verkeer en één voor het blokkanaal.

Steeds meer sluis- en brugwachters verwachten dat op de marifoon wordt uitgeluisterd. Ook bij het zoeken naar ligplaatsen in een (jacht)haven is de marifoon een handig hulpmiddel. De belangrijkste functie blijft echter de communicatie in het nood-, spoed- en veiligheidsverkeer.

Hieronder is een voorbeeld proces voor het schutten van een sluis uitgewerkt.

1. Opstellen schutplan

Bij het opstellen van een schutplan dient het personeel rekening te houden met de aankomstvolgorde, voorschriften met betrekking tot gevaarlijke lading weersomstandigheden, aanwezigheid recreatievaart en dergelijke. Voor drukke sluisen wordt het schutplan in de regel met een computer gegenereerd;

2. Verstrekken informatie

De informatie van het schutplan moet aan de schepen verstrekt worden. Meestal geschiedt dit per marifoon, maar het is ook mogelijk gebruik te maken van een luidsprekerinstallatie. Als sprake is van meer kolken, is het aan te bevelen met pijlen (verkeersteken D.3a) aan te geven bij welke kolk het schip is ingedeeld. Als er meer dan één voorhaven is, kan de toewijzing eveneens met pijlen geregeld worden. In de Richtlijnen Scheepvaarttekens zijn hiertoe bruikbare beeldweergavetechnieken beschreven. Een dynamisch informatiepaneel kan dienen voor het verstrekken van aanvullende informatie;

3. Aanwijzen opstelplaats

De opstelplaats is uitsluitend bedoeld voor het afmeren van schepen, die met de eerstvolgende schutting mee kunnen. Zicht op de opstelplaats is aan te bevelen, zeker bij grote sluisen. Met camerabeelden, radar of direct zicht of een combinatie daarvan kan zonodig ondersteuning worden gegeven;

4. Invaarvolgorde en ligplaats in sluis.

Voor het invaren begint, moet ieder schip weten wat de invaarvolgorde is en welke plaats in de kolk is aangewezen. Deze informatie is over te dragen door gebruik te maken van een marifoon- of omroepinstallatie en ter zijner tijd op digitale wijze;

5. Gereed maken voor invaren

Door het tonen van een rood/groen seinlicht weet de scheepvaart dat het invaren binnen korte tijd kan beginnen;

6. Openen invaardeuren

De invaardeuren mogen pas worden geopend nadat het sluispersoneel heeft vastgesteld, dat zich geen personen of voorwerpen op of in de nabijheid van bewegende delen bevinden. Tijdens het openen van de deuren houdt het personeel toezicht, zonodig met technische hulpmiddelen;

7. Invaren toegestaan

Voordat het groene invaarsein getoond wordt, dient het personeel zich ervan te vergewissen dat zich geen andere schepen meer in de kolk bevinden;

8. Aanwijzingen ten behoeve van invaren

Het personeel ziet, eventueel ondersteund door technische hulpmiddelen, toe op het vlot en veilig invaren van de schepen en geeft zonodig aanwijzingen met gebruikmaking van de hen ter beschikking staande communicatiesystemen;

9. Aanwijzingen tijdens afmeren

Deze kunnen betrekking hebben op het innemen van de juiste ligplaats, het voldoende aansluiten van schepen, het afzetten van de schroef, enzovoorts. Het personeel geeft zonodig aanwijzingen met gebruikmaking van de communicatiesystemen;

10. Invaren verboden

Als het laatste schip is ingevaren, wordt door een rood seinlicht aangegeven, dat de invaart voor volgende schepen verboden is.

Tabel 4 Schutproces

Gebruikershandleiding (#Bedieninstructies, #Personnel)

De operator heeft een grote verantwoordelijkheid voor het scheepvaartverkeer. Deze dient het schip veilig te geleiden langs de beweegbare objecten en eventuele voorzieningen om aan te meren, indien dit in de dienstverlening is opgenomen. Vooral het schutproces (zie Tabel 4 Schutproces) is daarvoor van belang.

Tevens dient kennis aanwezig te zijn voor het innemen van een ligplaats op een wachtplaats. Hiervoor dient indien van toepassing met de schipper gecommuniceerd te kunnen worden. De schipper zelf kan het verzoek tot bedienen van een sluis kenbaar maken. Er dient kennis te zijn om het de schutvolgorde van kleine en grote schepen te bepalen. Eveneens dient het schutten te worden gemonitord. Zowel ter bescherming van het schip als van de sluisdeuren of de beschermingsinrichtingen. Indien de operator optreedt als bevoegde autoriteit geldt het volgende. De bevoegde autoriteit kan, wanneer een schip zich in een sluis of op een wachtplaats daarvan bevindt, aan de schipper een verkeersaanwijzing geven.

Dit om de veiligheid of de goede orde van de scheepvaart, dan wel het zonder oponthoud doorvaren van de sluis en het doelmatig gebruik daarvan, te verzekeren

De schipper is verplicht aan deze verkeersaanwijzing gevolg te geven.

6.2.2 Beschouwing systeemfuncties brug- en sluisbeheer

Deze zijn geïnventariseerd in Figuur 13 Cross-reference systeemfuncties met configuratie-items en worden hieronder per systeemfunctie beschouwd. In de hiervoor aangegeven figuur is aangegeven welke configuratie-items hiertoe onder vallen.

Coördineren

De inrichting van iCentrale is volgens de huidige inzichten gebaseerd op flexibele bediening, dat wil zeggen: één bedienaar kan veilig, onder specifieke voorwaarden, meerdere bedieningsprocessen tegelijk of overlappend uitvoeren. het zogeheten ritsend bedienen (#iOrkestrator). De operators opereren in teams, waarbij de werklust gelijkmatig over de teamleden verdeeld wordt.

Ritsend bedienen betekent: het bedienen van meerdere objecten op een zodanige wijze, dat bedienstappen van de ene bedieningscyclus vallen in de momenten van de andere bedieningscyclus, waarin geen directe controle en sturing vereist is. Door het in elkaar schuiven van de processtappen is winst te behalen ten opzichte van zuiver volgtijdelijke bediening.

Observeren

De operator dient bij Beweegbare objecten direct zicht op de scheepvaart te hebben (#iPixel Space Manager).

Alvorens de deuren van een sluis te sluiten, dient het personeel zeker te stellen dat er zich geen schepen kort voor of tussen de sluishoofden bevinden (#iPixel Space Manager). Reeds afgemeerde schepen moeten binnen de stopstrepen liggen. Hierna kunnen de deuren gesloten worden. Tijdens het sluiten houdt de bedienaar toezicht en stopt het sluitproces indien een onveilige situatie ontstaat.

Bij het openen van de uitvaardeuren moet het sluispersoneel er op toezien, dat geen onveilige situatie kan ontstaan en stopt indien nodig het openingsproces. Het openen van de deuren kan ter bevordering van de vlotheid van het schutproces al beginnen als er nog enig, maar niet meer dan 20 cm verval aanwezig is en er geen kleine schepen in de kolk aanwezig zijn.

Richtlijn vaarwegen stelt in artikel 6.7.4 *Cameratoezicht*:

Cameratoezicht vanuit een verkeerspost of permanent bemande bedieningspost verdient overweging in verband met de bestrijding van criminaliteit en vandalisme.

Ingevolge het Privacyreglement Verkeersregistratiesystemen Rijkswaterstaat, voortvloeiende uit de Wet bescherming persoonsgegevens (Wbp), dat onder meer van toepassing is op videoregistraties, mogen de beelden alleen worden gebruikt voor het veilige gebruik van de faciliteiten en niet aan derden worden verstrekt. De bewaartermijn van beelden is niet langer dan 30 dagen, maar in de regel worden ze niet langer dan 24 uur bewaard. Dit geldt niet bij calamiteiten of het vermoeden van criminele activiteiten. **#iPixel Space Manager** **#iLogging**

Communiceren

Het is nodig de schipper terug te melden dat hij is gesignaleerd, het al dan niet in behandeling nemen van zijn verzoek tot bediening en de geschatte wachttijd (**#Loudspeaker**).

Nadat een sluitdeur is gesloten start het nivelleren dat met een akoestisch signaal wordt aangegeven. Het signaal, in de regel een sirene, heeft een sterkte van 112 dB. In de bebouwde kom is maximaal 85 dB toegestaan (**#koppelvlakken business logic**).

Personeel dient tijdens het nivelleren toe te zien op mogelijke problemen met het vieren of aanhalen van trossen. Recreatievaartuigen hebben hier soms problemen mee. Het personeel geeft zondig aanwijzingen met gebruikmaking van communicatiesystemen (**#Loudspeaker**).

Tijdens uitvaren zijn in de regel geen aanwijzingen nodig. Zonodig geeft het personeel aanwijzingen met gebruikmaking van de ter beschikking staande communicatiesystemen (**#Loudspeaker**).

Een schip kan aangeven dat het de brug wil passeren door middel van het geven van het voorgeschreven geluidsein (lang-kort-lang) of door melding via marifoon, telefoon, etc. (**#Loudspeaker**). Veelal heeft de bedienaar het schip reeds visueel waargenomen en daarop actie genomen.

Managen

De schipper levert tijdig gegevens aan de IVS-post die op de vaarroute het eerst zal worden gepasseerd. (**#Monitor**, **#iPixel Space Manager**). Indien de gegevens tijdens de vaart wijzigen, wordt dit door de schipper of de kapitein van een schip onmiddellijk aan de dichtstbijzijnde IVS-post medegedeeld.

Volgens het Rijks-ambtenarenreglement heeft een medewerker Operationeel Verkeersmanagement VTS-operator een substantieel bezwarende functie. Dit betekent dat er specifieke arbeidsvoorwaarden gelden voor dergelijk personeel. Mogelijk dat er op provinciaal of gemeentelijk niveau ook zulke functies bestaan. Het is aan te bevelen dit na te gaan om te komen tot een degelijke personeelsselectie. **#Personnel**

6.2.3 Ondersteunen bij incident- en calamiteitenbestrijding

Een incident is een onvoorziene gebeurtenis, waardoor in het beheergebied of in de omliggende beheergebieden plotsklaps een situatie ontstaat van waterverontreiniging, wateroverlast, of onveilige situaties op de vaarwegen, dan wel een situatie waarbij waterstaatswerken zijn/kunnen worden beschadigd. Een incident wordt een calamiteit, wanneer door de onvoorziene gebeurtenis een ernstige verstoring van de algemene veiligheid is ontstaan, waarbij het leven en de gezondheid van vele personen, dan wel grote materiële belangen, in ernstige mate bedreigd worden en waarbij een gecoördineerde inzet van diensten en organisaties van verschillende disciplines vereist is.

Komt een incidentmelding binnen bij de iCentrale dan kan dez worden doorgezet naar de betreffende nooddienst (politie of brandweer) in het gebied waar het incident heeft plaatsgevonden. De iCentrale kan vervolgens ondersteuning verlenen bij de bestrijding van het incident of de calamiteit bieden in de vorm van:

1. Informeren van schepen welke in hun reis hinder kunnen ondervinden van de calamiteit en zo nodig omleiden van deze schepen.
2. Informeren van beheerders van aanpalende vaarwegen over de stremming van de vaarweg en de bijbehorende iCentrale;
3. Informeren van havenautoriteiten in het bewuste gebied over de stremming van de vaarweg. Naarmate de calamiteitenafhandeling verder wordt opgeschaald worden het geografisch gebied waarin partijen worden geïnformeerd groter;
4. Voorzien van politie en brandweer van alle benodigde informatie die kan helpen bij de bestrijding van het incident of de calamiteit

De volgende informatie is onder meer benodigd voor het succesvol kunnen afhandelen van een calamiteit:

- Informatie over de plaats, aard en kilometerraai-aanduiding van het scheepsongeval;
- Informatie over de hoeveelheid en aard van de vervoerde goederen en de locatie van deze goederen in het schip;
- Informatie over de eventueel bij het incident betrokken gevaarlijke stoffen;
- Informatie over het schip;
- Informatie over de bemanning (aantal, huisarts, naaste familie, locatie op het schip);
- Informatie over de passagiers (hoe ver willen (nog afgezien van het kunnen) we gaan);
- Informatie over restcapaciteit in het netwerk om lading dan wel mensen over te nemen.

6.3 Knelpunteninventarisatie en Oplossingsrichtingen

1
Knelpunt Nautische Veiligheid.#iOrkestrator.Knelpunt1
Trigger based werken sluit niet aan op de door VTS gevraagde 24/7 verkeersbegeleiding in het VTS-dekkingsgebied.
Oplossingsrichting
Capaciteitsclaim VTS opnemen in de iOrkestrator zodat er 24/7 begeleid kan worden.

2
Knelpunt Nautische Veiligheid.#iData Mapper.Knelpunt1
Er is onvoldoende data/informatie voorhanden op decentraal niveau voor het automatisch vergaren, bewerken en distribueren van netwerkbrede (vaarwegen, sluizen, bruggen, stuwen, etcetera) informatie. Hiervoor is een informatiedienst nodig. Binnen de RIS Guidelines wordt hiervoor gesproken over een zogeheten Fairways Information Service (FIS) en Traffic Information Service (TIS).
Oplossingsrichting
De iCentrale zoekt aansluiting bij de vaarweg- en scheepvaartverkeerinformatiedienstverlening vanuit RWS en breidt deze uit naar de vaarwegen van DCO's waar dat nog niet is gebeurd.

7 Veiligheidsthema Externe veiligheid

7.1 Inventarisatie documenten

Niveau	Regelingen	Opmerking
EU Richtlijnen	-	
Wetten NL	Wet veiligheidsregio Wet vervoer gevaarlijke stoffen	
Besluiten en Regelingen NL	-	
Normen en Visie	-	
Provinciaal Beleid en Visie	-	
Lokaal Beleid en Visie	-	

Tabel 5 Inventarisatie documenten externe veiligheid

7.2 Uitwerking

7.2.1 Wet veiligheidsregio's

De wet veiligheidsregio's bepaalt welke organisaties belast zijn met rampenbestrijding en crisisbeheersing en arbeidsomstandigheden en aan welke minimeisen zij daarbij moeten voldoen. Als zodanig raakt de wet slechts indirect aan thema's die relevant kunnen zijn voor de iCentrale. In het onderstaande artikel wordt een verplichting genoemd die voor eenieder geldt en daarom ook voor (personeel van) de iCentrale.

Artikel 48 lid 1 **#Personnel**

Eenieder die beschikt over relevante veiligheidstechnische gegevens, verschaft het bestuur van de veiligheidsregio de informatie die nodig is voor een adequate voorbereiding van de rampenbestrijding en de crisisbeheersing. Dit geldt niet voor zover deze informatie reeds op grond van andere voorschriften is verschaft of kan worden verkregen.

Dit artikel zou betrekking kunnen hebben op informatie die bij de verkeerscentrale bekend is, zoals data met betrekking tot verkeersbewegingen, en relevant is voor bijvoorbeeld een effectieve bestrijding van incidenten of rampen.

7.2.2 Wet vervoer gevaarlijke stoffen

De Wet vervoer gevaarlijke stoffen stelt regels aan het transport van gevaarlijke (giftige, explosieve) stoffen met een vervoermiddel over auto-, water- of spoorwegen. Als zodanig is zij slechts zijdelings relevant voor het werkveld waarin verkeerscentrales zich bevinden. Hoewel de wet verkeerscentrales niet specifiek adresseert is het wel van belang te realiseren dat de objecten binnen het werkveld van verkeerscentrales gebonden zijn aan regels over transport van gevaarlijke stoffen. Dit betreft dan bijvoorbeeld tunnels op bepaalde wegen, die worden aangewezen of (tijdelijk) uitgesloten als route voor gevaarlijke stoffen. De volgende artikelen zijn in dit opzicht noemenswaardig.

Artikel 20 **#Bedieninstructies** **#Bedienfilosofie**

1 Onze Minister kan besluiten in het belang van de openbare veiligheid een weg, binnenwater of hoofdspoorweg aan te wijzen waarover het wegvervoer, het binnenwatervervoer onderscheidenlijk het spoorvervoer van bij dat besluit te bepalen gevaarlijke stoffen niet is toegestaan.

2 Bij een besluit als bedoeld in het eerste lid kan Onze Minister bepalen dat het verbod uitsluitend geldt voor een bij dat besluit te bepalen periode van het jaar of van de dag.

Het belang van dit artikel schuilt in het besef dat wegen op land, water of spoor al dan niet gebruikt kunnen worden voor het vervoer van gevaarlijke stoffen. Dit is bij bediening op afstand een aandachtspunt voor de (medewerkers van de) iCentrale, aangezien de (bestrijding van de) gevolgen van ongevallen met gevaarlijke stoffen bijzondere inzet vereist die bijvoorbeeld in geval van tunnels in calamiteitenplannen zullen moeten worden vastgelegd.

Artikel 23 **#Bedieninstructies** **#Bedienfilosofie**

1 Provinciale Staten wijzen ten behoeve van het doorgaande vervoer van gevaarlijke stoffen een netwerk aan dat bestaat uit bij de provincie of bij waterschappen in beheer zijnde wegen of weggedeelten, niet zijnde de krachtens artikel 13, eerste lid, vastgestelde wegen.

In aanvulling op het punt hiervoor kunnen Provinciale Staten een netwerk aanwijzen waarover gevaarlijke stoffen vervoerd moeten worden.

Artikel 24 **#Bedieninstructies** **#Bedienfilosofie**

2 De gemeenteraad kan met betrekking tot het vervoer van gevaarlijke stoffen op zijn grondgebied gelegen wegen aanwijzen waarover de krachtens het eerste lid aangewezen gevaarlijke stoffen uitsluitend mogen worden vervoerd.

In aanvulling op de punten hiervoor kan de gemeenteraad specifieke wegen aanwijzen voor het vervoer van gevaarlijke stoffen.

7.3 Knelpunteninventarisatie en Oplossingsrichtingen

1
Knelpunt Externe Veiligheid.#Bedieninstructies.Knelpunt1
Bij calamiteiten hebben medewerkers geen routine hebben in de operationele uitvoering, doordat calamiteiten in het algemeen weinig voorkomen.
Oplossingsrichting
Training van calamiteitenscenario's.

8 Veiligheidsthema Veiligheid beweegbare objecten

8.1 Inventarisatie documenten

Niveau	Regelingen	Opmerking
EU Richtlijnen	Machinerichtlijn	
Wetten NL		
Besluiten en Regelingen NL		
Normen en Visie	NEN-EN-IEC 60204-1 NEN-EN-IEC 62061 NEN-EN-ISO 13850 NEN 6786 NEN 6787 NEN-EN-IEC 61508-1 - 2010 en LBS - Gebruikershandleiding Natte Beweegbare Objecten LBS – Veiligheidsfuncties LBS – Faaldefinities LBS – Basisbeschrijving LBS Bedienplek nautische Objecten LBS Noodbediening	
Provinciaal Beleid en Visie	-	
Lokaal Beleid en Visie	-	

Tabel 6 Inventarisatie documenten Veiligheid beweegbare objecten

De Machinerichtlijn is van toepassing op machines, waarbij een machine in deze richtlijn diverse definities kent. De meest van toepassing zijnde voor dit document is de volgende definitie: “Een samenstel, voorzien van of bestemd om te worden voorzien van een aandrijfsysteem — maar niet op basis van rechtstreeks gebruikte menselijke of dierlijke spierkracht van onderling verbonden onderdelen of componenten waarvan er ten minste één kan bewegen, en die samengevoegd worden voor een bepaalde toepassing”.

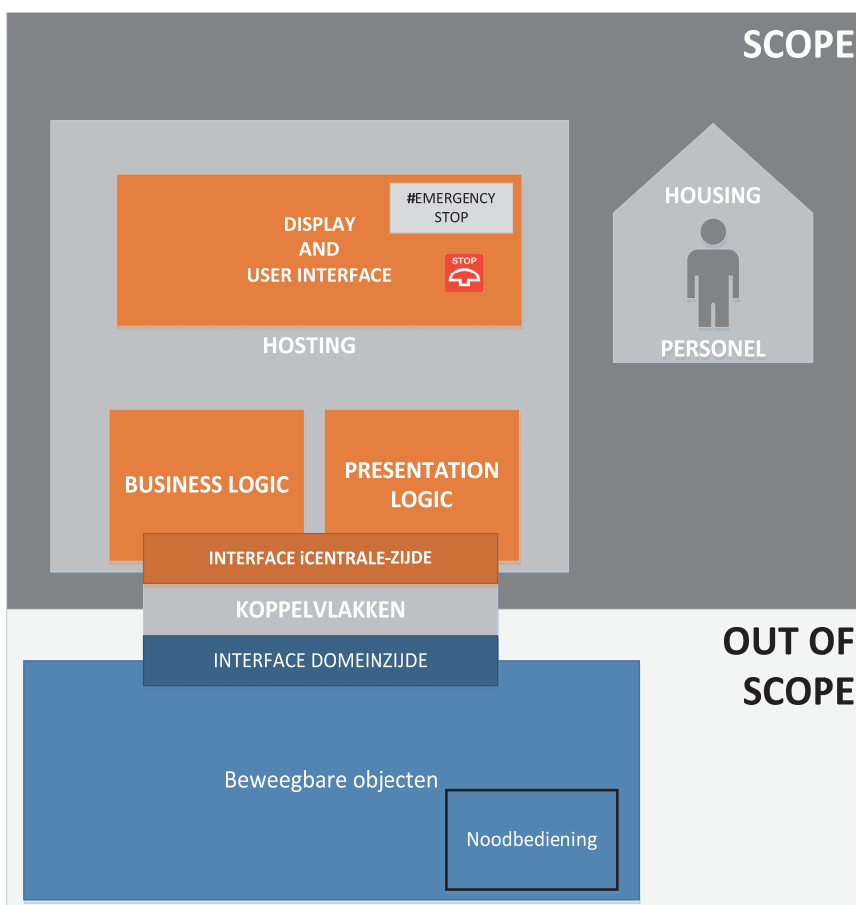
Veel van de gebruikte normen handelen over de veiligheid van deze apparaten (machines), terwijl de LBS (Landelijke Brug- en Sluisstandaard) juist meer de proceskant benadert.

Beide gezichtspunten zijn van belang voor de totale veiligheidsketen.

8.2 Uitwerking

Een beweegbaar object is in die zin een machine, omdat er bewegende onderdelen zijn, die vanuit de iCentrale en/of plaatselijk gecontroleerd in beweging kunnen worden gezet en indien noodzakelijk geforceerd tot stoppen kunnen worden gebracht.

Hierbij komen aspecten als Noodbediening en Noodstop naar voren. Noodbediening is een functie die gebruikt wordt indien de reguliere bediening niet of onjuist functioneert. Noodbediening is er vooral voor om het proces zoveel als mogelijk te borgen en is te zien als een uitwijkfunctie. De Noodstop daarentegen is puur een veiligheidsfunctie om beknelling, aanrijgevaar, aanvaargevaar etc. te voorkomen. De Noodbediening valt dan ook meer in de categorie 'Beschikbaarheid', terwijl Noodstop puur 'Veiligheid' betreft. De Noodbediening valt in het domein / beheersgebied zelf en is conform Figuur 2 Weergave reikwijdte veiligheid 'out of scope'. De Noodstop (**#Emergency Stop**) valt wel degelijk binnen de scope.



Figuur 16 Noodbediening (out of scope) vs Noodstop (scope)

Het kan voorkomen dat een brug / sluis ook lokaal bediend moet kunnen worden, vergelijkbaar met tunnelobjecten. Er dient voorkomen te worden dat bewaking en zeker bediening van een object vanuit meerdere bedienlocaties tegelijkertijd mogelijk is, om tegenstrijdige bedieningen te voorkomen. Deze functionaliteit dient in het domein zelf geïmplementeerd te worden. Alleen het object zelf kan 'zien' dat deze wordt bediend.

Veiligheid is niet alleen een technische aangelegenheid. Ook goede procedures en adequaat opgeleid personeel beïnvloeden positief de veiligheid. Om dit in een context te plaatsen is hieronder als voorbeeld het bedienproces van een beweegbare brug uitgewerkt.

Reguliere bediening beweegbare brug
1. Brug sluiten voor landverkeer (voorafgaand schouwen);
2. Brug openen (inclusief schouwen);
3. Doorvaart vrijgeven voor scheepvaartverkeer;
4. Doorvaart sluiten voor scheepvaartverkeer;
5. Brug sluiten (inclusief schouwen);
6. Brug vrijgeven voor landverkeer.

Tabel 7 Stappenplan beweegbare brug

De bediening van een beweegbare brug is een intensieve taak, die nauwgezet moet worden uitgevoerd. Er wordt hier veel geschouwd en indien nodig gecommuniceerd via omroep. De brugbeweging, en dus ook elk deelproces na het geven van een startopdracht, moet altijd door een stop of een noodstop kunnen worden onderbroken om de brug in een veilige toestand te brengen. Daarna kan door een hernieuwde startopdracht het onderbroken of het omgekeerde deelproces worden geactiveerd.

Eisen beweegbare brug
11. Bediening dient mogelijk te zijn met reguliere bediening;
12. Onderhoudsbediening en noodbediening dienen niet meegenomen te worden als back-up voor het bieden van de functionaliteit;
13. Er moet éénrichting communicatie mogelijk zijn met het landverkeer;
14. Er moet zicht zijn bij bediening van beweegbare bruggen en schutsluizen;
15. Het landverkeer moet veilig gestopt kunnen worden;
16. Er mogen geen veiligheidsfuncties overbrugd zijn (tijdens bediening).

Tabel 8 Eisen beweegbare brug

Overbruggingen

Deze dienen alleen geactiveerd te kunnen worden door middel van een sleutelschakelaar of het invoeren van een wachtwoord. Het actief zijn van een overbruggingsschakelaar moet duidelijk herkenbaar zijn (**#koppelvlakken presentation logic**). Deze mag hierop de brug niet bedienen (**#Bedieninstructies**).

Bedienbaarheid (**#iNotification panel**)

De informatie die nodig is voor het bedienen van een machine (in dit geval een brug/sluis), moet in een ondubbelzinnige en gemakkelijk te begrijpen vorm worden verstrekt. Zij mag niet zo uitgebreid zijn dat te hoge eisen aan de bediener worden gesteld. Dit heeft voor de iCentrale effect op beeldschermen en communicatiemiddelen. Er dient vooral aandacht aan ontwerp van de displays te worden. Voor bedieningsmiddelen wordt verwezen naar NEN-EN 894-3. Gebruik van drukknoppen wordt aanbevolen, deze zijn minder gevoelig voor onbedoeld gebruik of misbruik.

Bedienruimte

Bij lokale bediening van bruggen en sluizen wordt gebruik gemaakt van de NEN 6787 voor de inrichting van bedienruimtes. In die norm wordt aandacht besteed aan de plaats van de bedienlocatie (zicht) en het goed afleesbaar zijn van bedieningspanelen en signaleringspanelen (lichtinval). Hoewel dit voor de iCentrale zaken zijn die ook onder arbeidsveiligheid kunnen vallen, dient vooral aandacht aan zicht te worden besteed. Hierbij wordt verwezen naar de systeemketen 'Observeren'.

Gebruikershandleiding (#Bedieninstructies, #Personnel)

Er moet een gebruikershandleiding worden opgesteld volgens hoofdstuk 5 van NEN-EN 292-2:1996 in de taal van het land waar de brug wordt gebruikt. Voor het opstellen van de gebruikershandleiding wordt verwezen naar eisen uit NEN 5509, NEN-EN-IEC 60204-1 en NEN-EN 982. De gebruikershandleiding moet de gebruiker alle informatie verschaffen om de brug veilig te gebruiken. De bedieningshandleiding moet aan de gebruiker aangeven wat de minimeisen zijn die aan de vaardigheden van bedienend personeel worden gesteld.

De operator heeft een grote verantwoordelijkheid. Ten eerste is de operator is door middel van art. 450 Wetboek van Strafrecht verplicht om iemand in levensgevaar te helpen (mits je jezelf niet in gevaar brengt). Vanuit iCentrale heeft hij hiertoe diverse communicatiemiddelen ter beschikking. In geval van incidenten heeft de operator een ondersteunende en regelende taak. Hij is verantwoordelijk voor het zo snel mogelijk contacteren van hulpdiensten (via 112) en het informeren van anderen (ter plaatse).

Eveneens moet de operator – in de rol van waarnemer storing – bij een storing, in overeenstemming met de afgesproken werkwijze deze melden, de storing registreren en zorgen voor een goede (administratieve) afhandeling volgens het calamiteitenplan.

De operator is vervolgens verantwoordelijk voor de veiligheid van het scheepvaartverkeer en het landverkeer in, op en nabij het object tijdens het bedienproces. Het gaat daarbij om de veiligheid van scheepvaartverkeer en landverkeer voor zover de operator deze in relatie tot het bedienproces kan beïnvloeden. De schipper en automobilist zijn en blijven verantwoordelijk voor hun veilig varen/rijden. De operator heeft daarbij de verantwoordelijkheid op basis van het bedienprotocol/handboek te handelen. Bij calamiteiten moet het calamiteitenplan/draaiboek de bedienaar aangeven hoe te handelen en op te schalen. Wanneer het bedienprotocol/handboek en calamiteitenplan/draaiboek geen uitkomst bieden of twijfel ontstaat, zal de operator zodanig moeten handelen dat de veiligheid gewaarborgd wordt. Wanneer mogelijk, dient de operator te overleggen met zijn direct leidinggevende (teamleider). Het optreden van bijzondere situaties moet altijd worden gemeld bij de direct leidinggevende (teamleider). Bovendien moet de optreden van bijzondere situaties registreren.

Het gebruik van de noodstop dient geregistreerd te worden, net als de bijbehorende oorzaak en de daarna genomen vervolgstappen.

Bij afwijkende weersomstandigheden en donkerte kunnen andere eisen van toepassing zijn. Er moeten duidelijke instructies komen onder welke omstandigheden een operator moet besluiten om te stoppen met bedienen (bv falende functionele zicht of audiocommunicatie-eisen)

Er dienen specifieke bedieninstructies te worden gemaakt indien de operator geacht wordt te werken met IVS90. Dit ligt op het snijvlak met Nautische veiligheid. In IVS90 is de operator in de rol van planner actief om bij bruggen tijdstippen van de brugopening en bij sluizen de toerbeurtnummers, kolkindeling en schutbrief vast te leggen.

Indien de operator actief is voor taken als waarnemer ongeval of waarnemer technische storingen of zelfs nautisch beheerder dient deze zaken te registreren in de daarvoor afgesproken systemen. Dit vereist instructie.

8.2.1 Beschouwing systeemfuncties

Deze zijn geïnventariseerd in Figuur 13 Cross-reference systeemfuncties met configuratie-items en worden hieronder per systeemfunctie beschouwd. In de hiervoor aangegeven figuur is aangegeven welke configuratie-items hiertoe onder vallen.

Coördineren

Het bedienen van meer dan één brug gelijktijdig vanaf één bedieningsstation mag niet mogelijk zijn. Ongeacht het aantal bedieningsstations moet de geselecteerde brug voor het bedienen duidelijk zijn aangegeven op het desbetreffende bedieningsstation. (#iOrkestrator)

Observeren

De mate waarin gemonitord moet worden tijdens de uitvoering van bedienactiviteiten is afhankelijk van de lopende activiteit en de specifieke situatie. In veel stappen bij de bediening dient er te worden geschouwd (zie Tabel 8 Eisen beweegbare brug). De grootte van het risico bepaalt de mate waarin gemonitord dient te worden. Neerlaten van aanrij- en afrijbomen geschiedt met behulp van camera's. De bedienaar dient te kunnen zien dat het gebied tussen de witte kruisvlakken (inclusief kruisvlakken) vrij is van onbevoegd verkeer en personen. Pas daarna zal hij de afsluitbomen laten dalen. Ook zal de bedienaar in de gaten houden of het landverkeer het gebied tussen de witte kruisvlakken verlaat en er geen ongevallen plaatsvinden. Dit als voorschot op het schouwen van het brugdek voor sluiten van de afsluitbomen in de afrijrichting. In geval van incidenten dient de bedienaar volgens het calamiteitenplan te handelen. Daarnaast dient de verkeersregelaar scheepvaart zich ervan te vergewissen dat de uitvaart vlot en veilig kan plaatsvinden. Vanuit veilig betekent dit dat hij schepen moet kunnen waarnemen in de uitvaart fuik en dat hij vanuit vlot inzicht moet hebben in de scheepvaart in het verdere uitvaartgebied. Bij bijzondere omstandigheden als mist of harde wind is meer aandacht vereist.

Tijdens de bediening moet de operator zicht worden verschaft op en/of visuele informatie krijgen over:

1. de stand van de brug;
2. het correct functioneren van de veiligheidsvoorzieningen;
3. het passerend scheepvaartverkeer;
4. het landverkeer;
5. overige gebruikers van de brug.

Bij sluizen geldt dat de operator de sluisdeur(en) en de directe omgeving dient te schouwen op gevaarlijke situaties. Daarbij dient hij zeker te stellen dat er geen onbevoegde personen zich op de sluisdeur(en) of in de buurt daarvan bevinden. De operator dient stilstaande en zich bewegende personen en voorwerpen op de sluisdeur(en) waar te kunnen nemen. Ook gehurkte en liggende personen dienen gedetecteerd te kunnen worden. De veiligheidsruimte van de sluisdeur(en) dient op waterniveau zodanig zichtbaar te zijn dat kleine bootjes waar mensen in kunnen zitten en grote drijvende voorwerpen herkend kunnen worden.

Communiceren

Indien hulpdiensten (ambulance, politie, brandweer) willen passeren, dan dient dit door de betreffende hulpdienst aan de bedienaar te worden gemeld voordat de hulpdiensten daadwerkelijk passeren. De bedienaar moet auditief kunnen communiceren met hulpverleningsdiensten, wanneer er vanwege een melding van hulpverleningsdiensten is bepaald dat de brug nog niet geopend mag worden zolang zij nog niet gepasseerd zijn. Zonder voorafgaande melding hoeft de operator het lopende brugproces niet te onderbreken indien dit tot onveilige situaties op de vaarweg leidt.

Er moet eenrichting communicatie mogelijk zijn met het landverkeer (indien landverkeer over de sluisdeuren rijdt). Er moet tweerichting communicatie mogelijk zijn met het scheepvaartverkeer.

Als de communicatie verbinding tussen bediening op afstand en brug verbroken wordt moet een op afstand bediende brug automatisch tot stilstand komen. Deze functionaliteit dient in het domein geïmplementeerd te worden en is voor dit document 'out of scope'.

Veilig ingrijpen

Op één of meer plaatsen, vanwaar bediend wordt en zicht is op gevaarlijke situaties moet een noodstopchakelaar zijn aangebracht waarmee bewegingen onmiddellijk tot stilstand kunnen worden gebracht.

Het doel van de noodstopfunctie is bewegingen te stoppen die leiden tot opkomende staande schade aan een beweegbare brug of schutsluis af te wenden respectievelijk te beperken. Een noodstop is een door een persoon geïnitieerde actie om bedienobjecten zo snel mogelijk op een gecontroleerde manier tot stilstand te brengen. Een noodstop leidt niet tot het deactiveren van de betreffende bedienvorm en is altijd een secundaire veiligheidsfunctie en geen alternatief voor veiligheidsfuncties of andere beveiligingen.

De operator moet zich er vanaf iedere bedieningspost van kunnen vergewissen dat er zich geen personen in de gevarenczones bevinden of het bedieningssysteem moet zodanig zijn ontworpen en uitgevoerd dat het inschakelen van de machine wordt verhinderd zolang er zich iemand in de gevarenczone bevindt.

Enkele voorbeelden van situaties waarbij een bedienaar de noodstopfunctie MOET gebruiken:

1. Het besturingssysteem reageert niet op een STOP opdracht waardoor een gevaarlijke situatie voor een gebruiker ontstaat, zoals knelgevaar;
2. Bij een openende of sluitende sluisdeur dreigt beknelling van scheepvaart of een persoon.
NB Als uitzondering op het doel van de noodstopfunctie is hierbij de noodstopfunctie een primaire veiligheidsmaatregel;
3. Het val van een brug sluit zonder dat er een bedienopdracht sluiten gegeven is;
4. Een persoon of voertuig blijft stil staan onder een van de omlaag komende afsluitbomen en is daarbij/daarvoor niet door het rode bruglicht gekomen.

Benevens de noodstop is er altijd een processtop mogelijkheid om het proces te stoppen, indien hiermee niet de veiligheid in het geding komt.

Nadat de noodstop is ingeschakeld, moet het gevaar weggenomen worden. Indien dit onmogelijk is zonder nieuwe machine gerelateerde bewegingen te starten, dan moet alsnog de noodstopfunctie eerst gereset worden. Een operator mag niet zomaar een bediende noodstop ontgrendelen. Eerst moet de operator zich overtuigen of het ontgrendelen van de noodstopstoel niet tot herhaalde of aanvullende gevarensituaties kan leiden. Het is dus van belang dat de operator op een zo eenvoudig mogelijke manier een besluit kan nemen of hij de geactiveerde noodstopfunctie mag ontgrendelen en eventueel het object verder te kunnen bedienen.

Er moet een beproeving worden gedaan van elke bedieningsplaats en/of positie waar de noodstopinrichting kan worden bekrachtigd.

8.2.2 Aandachtspunten bij migratie naar centrale bediening

Indien de lokale bediening overgenomen wordt in iCentrale producten/diensten, verandert daarmee de veiligheidsketen. Hiervoor zijn specifieke zaken van toepassing, afhankelijk van het opgelegde veiligheidsniveau (SIL-niveau). Dit vereist ook speciale aandacht voor testen en validatie.

Voor het veiligheidsniveau geldt het volgende (**#iEvent detector**, **#koppelvlakken business logic**, **#koppelvlakken presentation logic**): Het SIL-niveau is ingekaderd in de IEC 61508. Hierbij worden eisen gesteld aan de veiligheid gerelateerde betrouwbaarheid aan het systeem en de delen daarvan. Hier wordt vooral gekeken naar de betrouwbaarheid van de software. De IEC 61508-03 geeft handvatten om softwaremodules (daar SCRECS geheten) gestructureerd te ontwerpen, te ontwikkelen en te implementeren. Het resultaat van de verrichte activiteiten gedurende ontwerp, ontwikkeling en toepassing van een SCRECS moet voor elke relevante fase worden geverifieerd.

Een SCREC dient ontworpen te worden met inbegrip van de diagnostische functies en functies voor de respons op fouten reageren. De documentatie van de SCRECS dient:

1. accuraat, compleet en bondig zijn;
2. geschikt zijn voor de bedoelde toepassing;
3. toegankelijk en onderhoudsvriendelijk zijn;
4. de versie ervan moet verifieerbaar zijn.

Voor testen en validatie geldt het volgende (**#iNotification panel**, **#iEvent detector**, **#Emergency stop**, **#iEmergency stop manager**, **#iWorkspace manager**, **#koppelvlakken business logic**, **#koppelvlakken presentation logic**): De gehele keten moet worden beproefd op juiste en veilige werking voor zowel de reguliere bedieningen als voor de processtop en noodstop. Het moge duidelijk zijn dat de diverse faalwijzes en veilige toestand onder deze testen vallen.

8.3 Knelpunteninventarisatie en Oplossingsrichtingen

1
Knelpunt Veiligheid Beweegbare Objecten.#iEvent detector.1
Er dient zeker gesteld te worden dat lokale bediening en centrale bediening niet tegelijkertijd in staat zijn om commando's uit te laten voeren. Aangezien iCentrale niet de regie voert over de lokale bediening kan deze daar niet over waken.
Oplossingsrichting
Het beweegbare object bewaakt zelf of deze lokaal dan wel centraal bediend wordt. Via iEvent detector wordt lokale bediening aan de Centrale Bediening gemeld, waarmee het beweegbare object borgt dat er niet vanuit iCentrale bediend kan worden.

2
Knelpunt Veiligheid Beweegbare Objecten.#iNotification panel.1
Gebruik van drukknoppen wordt aanbevolen, deze zijn minder gevoelig voor onbedoeld gebruik of misbruik. De iCentrale kent echter geen drukknoppen.
Oplossingsrichting
Om onbedoeld gebruik te voorkomen kan als mitigerende maatregel worden opgenomen dat bij bepaalde commando's de bevestiging 'enkele seconden' ingedrukt dient te worden. Dit voorkomt onbedoeld gebruik.

3
Knelpunt Veiligheid Beweegbare Objecten.#iOrkestrator.1
Men wordt tijdens het bedienen van objecten afgeleid door communicatie.
Oplossingsrichting
Houdt binnen de iOrkestrator extra rekening met mogelijk conflicterende parallele activiteiten.

9 Veiligheidsthema Tunnelveiligheid

9.1 Inventarisatie documenten

Niveau	Regelingen	Opmerking
EU Richtlijnen	Minimumveiligheidseisen Tunnels	
Wetten NL	WARVW	
Besluiten en Regelingen NL	RARVW Bouwbesluit	
Normen en Visie	-	
Provinciaal Beleid en Visie	-	
Lokaal Beleid en Visie	-	

Tabel 9 Inventarisatie documenten Tunnelveiligheid

Hoewel er een Landelijke Tunnel Standaard (LTS) is opgesteld door Rijkswaterstaat is deze niet meegenomen in bovenstaande inventarisatie. Voor zover dit effect heeft op veiligheid van andere tunnels is dit inmiddels verankerd in de WARVW en de RARVW.

Vanuit Europese Wetgeving is gesteld dat tunnels met een lengte van meer dan 3000 meter en een verkeersintensiteit van meer dan 2000 voertuigen per rijstrook bediend moeten worden. Vanuit de RARVW is dit gesteld op tunnels met een lengte van meer dan 500 meter. Bouwbesluit geeft aan dat iedere tunnel met een tunnallengte van meer dan 500m moet worden bediend.

Omdat de scope van de veiligheidskaders zich beperkt tot hetgeen in Figuur 2 Weergave reikwijdte veiligheid is afgebeeld, is Bouwbesluit in deze minder relevant voor de uitwerking dan de RARVW. Daar wordt immers het bedienaspect en de bijbehorende functies dieper uitgewerkt.

In de RARVW wordt de term tunneloperator benoemd. In dit document wordt dit als operator aangeduid.

9.2 Uitwerking

Bij tunnelveiligheid dient in eerste instantie incidenten zoveel als mogelijk voorkomen te worden (preventie) en als ze optreden zo snel als mogelijk hiertoe maatregelen te treffen (mitigatie) om een calamiteit (escalatie) te voorkomen. Indien dit toch escaleert dient zelfredding ondersteund te worden en hulpverlening mogelijk te worden gemaakt.

Het kan voorkomen dat tunnelobjecten ook lokaal bediend kunnen worden, vergelijkbaar met bruggen en sluizen. Er dient voorkomen te worden dat bewaking en zeker bediening van een object vanuit meerdere bedienlocaties tegelijkertijd mogelijk is, om tegenstrijdige bedieningen te voorkomen. Deze functionaliteit dient in het domein zelf geïmplementeerd te worden. Alleen het object zelf kan 'zien' dat deze wordt bediend.

#Personnel

In de gehele veiligheidsketen 'van lus tot lessenaar' bij Tunnelveiligheid speelt de bedienaar een dominante rol. Enerzijds moet deze voldoende onderricht zijn om zijn/haar taak te kunnen vervullen en aan de andere kant moet deze een goede inschatting van de veiligheidssituatie kunnen maken om de juiste initiële maatregelen en eventuele verdere opschaling van incident naar calamiteit te kunnen faciliteren. Een voorbeeld standaard stappenplan is weergegeven in Tabel 10 Stappenplan Afhandeling Incidenten en calamiteiten.

Stappenplan afhandeling incidenten en calamiteiten
Hierbij worden de volgende stappen doorlopen
17. Vaststellen aard van het voorval;
18. Bepalen afhandelingsstrategie;
19. Instellen initiële maatregelen;
20. Informeren en oproepen;
21. Instellen additionele maatregelen;
22. Herstellen en normaliseren;
23. Loggen en registreren;

Tabel 10 Stappenplan Afhandeling Incidenten en calamiteiten

Er zijn diverse soorten incidenten en calamiteiten die conform bovenstaand stappenplan afgehandeld dienen te worden. Deze zijn weergegeven in Tabel 11 Soorten Incidenten en calamiteiten

Soorten incidenten en calamiteiten
De volgende incidenten dienen minimaal afgehandeld te kunnen worden
1. stilstaande voertuigen;
2. aanrijdingen;
3. verloren lading;
4. voorvallen met verdwaalde personen.
De volgende calamiteiten dienen afgehandeld te kunnen worden:
1. een ernstige aanrijding of een kettingbotsing;
2. een brand of het vermoeden daarvan;
3. het vrijkomen van gevaarlijke stoffen of een vermoeden daarvan;
4. een brand in de verkeerscentrale;
5. een bommelding.
De aanwezigheid van hoogtedetectie is afhankelijk van het doorrijprofiel van de verkeersbuis.

Tabel 11 Soorten Incidenten en calamiteiten

Dit leidt niet alleen tot een omlijning van het takenpakket en daarmee vaardigheden van de operator, maar stelt ook eisen aan de bedieninstructies om dit takenpakket uit te kunnen voeren.

Tot de taken en vaardigheden van de operator behoort:

1. Bij tunnelafsluitingen (van lange of korte duur) de gebruikers door middel van makkelijk toegankelijke informatiesystemen informeren over de beste alternatieve rijroutes;
2. Bij slecht weer situaties weggebruikers advies geven over passende snelheden en afstanden tussen voertuigen;

3. Meewerken aan periodieke oefeningen;
4. In staat zijn om voorvallen te detecteren, installaties te bedienen en met hulpverleningsdiensten, wegininspecteurs, de officier van dienst van de tunnelbeheerder en weggebruikers te communiceren;
5. Voor het communiceren met weggebruikers dient men Nederlands en Engels te kunnen spreken;
6. Herkennen van personen in het tunneltracé, de stand van het verkeerslicht, de situatie bij hulpposten en vluchtdeuren, en het identificeren van voertuigen in het tunneltracé op basis van camerabeelden.

#Bedieninstructies- #Bedienfilosofie

Voor de bedieninstructies geldt het volgende:

1. Deze beschrijven hoe welke soort voorvallen gedetecteerd kunnen worden en hoe installaties te bedienen om hiervan de gevolgen te beperken;
2. Beschrijft de wijze en de hulpmiddelen waarmee gecommuniceerd wordt met hulpverleningsdiensten;
3. Beschrijft de wijze en de hulpmiddelen waarmee gecommuniceerd wordt met weggebruikers; Met de noodbediening een tunnel afsluiten indien de reguliere bediening en besturing niet functioneert;
4. Een tunnelbuis te sluiten indien de hoogtedetectie wordt genegeerd;
5. Bij een waargenomen voorval met kenmerken van brand, gevaarlijke stoffen, een ernstige aanrijding of een kettingbotsing of een vermoeden daarvan plaatst de operator de tunnel onmiddellijk in calamiteitenbedrijf;
6. Bij brand of vrijkomende gevaarlijke stoffen of een vermoeden daarvan plaatst de operator in aanvulling op het tweede en derde lid de tunnel onmiddellijk in evacuatiebedrijf;
7. Een procedure (bij voorkeur per tunnel i.v.m. verschillen per tunnel) hoe moet worden omgegaan met brand in de iCentrale;
8. Een procedure hoe de gemeenschappelijke meldkamer van de hulpverleningsdiensten wordt geïnformeerd over de volgende incidenten:
 - a. aanrijding met letsel of een vermoeden van letsel;
 - b. stilstaand voertuig met onwelwording of een vermoeden van onwelwording;
 - c. een betoging;
 - d. vandalisme;
 - e. aanwezigheid van voetgangers, fietsers of dieren, en
 - f. spookrijder.
9. Een gemeenschappelijk uitvraagprotocol om uitwisseling van informatie tussen de operator, de wegininspecteur, de officier van dienst van de tunnelbeheerder en de gemeenschappelijke meldkamer van de hulpverleningsdiensten geschiedt met een gemeenschappelijk uitvraagprotocol met als onderdelen:
 - a. exacte locatie;
 - b. aard van het voorval;
 - c. getroffen initiële maatregelen;
 - d. aantal dodelijke en gewonde slachtoffers;
 - e. aantal mensen in het incidentvoertuig achtergebleven en aantal immobiele slachtoffers;
 - f. aantal betrokken voertuigen;
 - g. eventueel in de tunnel aanwezig vervoer van gevaarlijke stoffen;
 - h. eventuele lekkage van vloeistoffen;
 - i. gewenste inzet van hulpverleningsdiensten, en
 - j. beste aanrijdroute.
10. Afspraken om bij calamiteiten toegang aan de bevelvoerder van de hulpverleningsdiensten te geven na briefing over de toestand in de calamiteitenbuis.

9.2.1 Beschouwing systeemfuncties

Deze zijn geïnventariseerd in Figuur 13 Cross-reference systeemfuncties met configuratie-items en worden hieronder per systeemfunctie beschouwd. In de hiervoor aangegeven figuur is aangegeven welke configuratie-items hiertoe onder vallen.

Coördineren

De **#iAuthenticator** dient te borgen dat alleen geautoriseerde operators van de iCentrale als tunneloperator kunnen functioneren.

Attenderen

Snel attenderen op (mogelijke) incidenten is cruciaal om snel mitigerende maatregelen te kunnen nemen en om escalatie te voorkomen. Dit stelt eisen aan:

1. **#iOrkestrator** om taken en meldingen te prioriteren aan operators
2. De duidelijkheid van informatie op **#iNotification panel**;
3. Betrouwbare en snelle detectie van de **#iEvent detector**;
4. Aangezien incidenten meestal meerdere 'triggers' hebben (bv meerdere SOS-meldingen, rookdetectie e.d.) dient de **#iState Estimator** and **#iPredictor** hiermee rekening te houden;
5. De operator dient door de **#iNotification panel** duidelijk geattendeerd te worden.

Bij Tunnelveiligheid is er geen sprake van een Noodstop in termen van machineveiligheid, een processtop in de GUI om de beweging van een afsluitboom of CADO te stoppen. De **#Emergency stop** en de **#iEmergency stop manager** spelen diensgevolge geen rol.

Het verloop van incident dient gelogd te kunnen worden door de operator (**#keyboard&mouse**). Dit is benevens het logging-systeem die bedieningshandelingen logt. Met het verloop worden vooral aanleiding en escalatie van het incident, en momenten en handelingen / gedragingen van weggebruikers en hulpdiensten.

Observeren

Bij (mogelijke) incidenten dient de operator goed zicht te hebben op de situatie om de aard en eerst ervan te kunnen beoordelen. Door middel van CCTV kan op iedere locatie in de verkeersbuis elk mogelijk incident geobserveerd worden en kan in de hele verkeersbuis de verkeerssituatie herkend worden en worden alle voertuigen geïdentificeerd, personen herkend en de standen van het verkeerslicht herkend. Hiertoe worden pan tilt zoom CCTV camera's gebruikt (**#joystick**).

Camerabeelden ten behoeve van het herkennen van personen in het tunneltracé, de stand van het verkeerslicht, de situatie bij hulpposten en vluchtdeuren, en het identificeren van voertuigen in het tunneltracé zijn op aanvraag beschikbaar voor de operator (**#koppelvlakken presentation logic**, **#Monitor**, **#iPixel Space Manager**).

Dit geldt eveneens voor de hoogtedetectie indien dit van toepassing is.

Communiceren

Voor communiceren met hulpdiensten en wegininspecteurs wordt uitgegaan van het openbare telefoonnet. Hiertoe zijn geen specifieke voorzieningen vereist. Voor communiceren met (vluchtende) weggebruikers zijn hiervoor wel specifieke voorzieningen vereist. Dit zijn:

1. HF-voorziening om radio-uitzendingen te onderbreken om dringende mededelingen te doen;
2. De omroepinstallatie om zowel vooraf opgenomen boodschappen als een rechtstreeks ingesproken boodschap afspelen in een, meerdere, of alle secties;
3. De noodtelefoon om een gelijktijdige spreek- en luisterverbinding met de actieve bediening indien de noodtelefoon in de gesprekstand staat. Deze functionaliteit is verplicht voor tunnels>250m ook al zijn ze niet bediend.

Voor noodtelefoon gelden specifieke prestatie-eisen:

1. De noodtelefoon in tunnels langer dan 500 meter voldoet voor zowel spreken als luisteren, zowel bij de hulppost als in de verkeerscentrale, aan het gestelde criterium voor STI in gebruikssituaties met rijdend verkeer met een snelheid van 70km/h in combinatie met 87dB(A) ventilatorlawaai in de verkeersbuis en normaal omgevingsgeluid in de verkeerscentrale;
2. De noodtelefoon in tunnels langer dan 250 meter en ten hoogste 500 meter voldoet voor zowel spreken als luisteren, zowel bij de hulppost als in de meldkamer, aan het gestelde criterium voor STI in gebruikssituaties met rijdend verkeer met een snelheid van 70km/h in de verkeersbuis en normaal omgevingsgeluid in de meldkamer.

Deze functionaliteit raakt **#Headset**, **#Horn** en **#Loudspeaker**

Managen

De stappen in Tabel 10 Stappenplan Afhandeling Incidenten en calamiteiten voor de incidenten / calamiteiten in Tabel 11 Soorten Incidenten en calamiteiten dienen door **#iNotification panel** gefaciliteerd te worden.

De uitleesmogelijkheid dien geïmplementeerd te worden. Hierbij dient te worden beschouwd of de operator of een andere functionaris hiertoe leesrechten moet krijgen.

Eveneens wordt als uitgangspunt gehanteerd dat de beeldvoorziening voor de meldkamer vanuit het tunnelobject wordt opgebouwd en dat daar ook de authenticatie plaatsvindt.

9.3 Knelpunteninventarisatie en Oplossingsrichtingen

1
Knelpunt Tunnelveiligheid.#iEvent detector.1
Er dient zeker gesteld te worden dat lokale bediening en centrale bediening niet tegelijkertijd in staat zijn om commando's uit te laten voeren. Aangezien iCentrale niet de regie voert over de lokale bediening kan deze daar niet over waken.
Oplossingsrichting
Het tunnelobject bewaakt zelf of deze lokaal dan wel centraal bediend wordt. Via iEvent detector wordt lokale bediening aan de Centrale Bediening gemeld, waarmee het tunnelobject borgt dat er niet vanuit iCentrale bediend kan worden.

2
Knelpunt Tunnelveiligheid.#Personnel.1
Bij brand in de iCentrale zelf dient de tunnel te worden gesloten en indien mogelijk lokaal te worden bediend. Een mogelijk knelpunt is dat de iCentrale of op grote afstand van de lokale bediening staat en/of er onvoldoende personeel beschikbaar is om lokaal te bedienen.
Oplossingsrichting
Aparte afspraken in de dienstverlening hierover maken.

3 Knelpunt Tunnelveiligheid.#Bedieninstructies.1
Knelpunt
Toegesproken berichten dienen vooraf te worden gegaan door een ding-dong. Nadat een operator een aanvraag tot toespreken heeft gedaan, moeten de geselecteerde secties in de verkeersbuis in een toestand worden gebracht opdat de boodschap overal hetzelfde klinkt. Daar moet de operator terugkoppeling van krijgen opdat deze weet dat deze kan toespreken. Of het ding-dong signaal vanuit iCentrale-systeem of vanuit de Omroepinstallatie moet worden geïnitieerd is een keuzemogelijkheid.
Oplossingsrichting
Als het ding-dong signaal vanuit iCentrale wordt geïnitieerd, krijgt de operator daar een terugkoppeling van. Als de Omroepinstallatie dat doet, moet er een andere voorziening komen die deze terugkoppeling geeft.

4 Knelpunt Tunnelveiligheid.#Bedienfilosofie.1
Knelpunt
Indien een bestaande bediende tunnel bediend gaat worden vanuit de iCentrale kan ervoor gekozen worden om het huidige bedienconcept te behouden, om bv zo min mogelijk ingrepen te doen in bestaande concepten. Een mogelijke oplossing is om de huidige bedienapplicatie (GUI) remote over te zetten naar iCentrale via een zogeheten RGUI-implementatie (Remote GUI). De huidige applicatie wordt als het ware overgezet. Dan blijven de huidige mechanismes (events) ook intact. Dit is niet in lijn met het iCentrale concept.
Oplossingsrichting
Hiermee met de taakbelasting rekening mee houden. Eveneens dient geborgd te worden dat de tunnel bediend wordt en dat het tunnelsysteem (TTI) vindt dat deze wordt bediend. M.a.w. de Remote-verbinding dient bewaakt te worden. Met Universeel Koppelvlak Verkeerscentrale van RWS (UKVC) is hiervoor een apart 'alive-sigitaal' beschikbaar.

5 Knelpunt Tunnelveiligheid.#iOrkestrator
Knelpunt
In een tunnelsysteem dienen bedieningen te worden gelogd en de mogelijkheid te worden geboden om uit te lezen. Voor dit uitlezen zijn speciale autorisaties nodig. Het is de keuze of deze logging (en ook de uitleesmogelijkheid) of op het tunnelobject of in de iCentrale te realiseren.
Oplossingsrichting
Geadviseerd wordt om deze logging in het tunnelobject te realiseren. Daar worden sowieso alle storingen en alarmen gelogd en om incidenten te kunnen analyseren lijkt het de meest voor de hand liggend om daar een aparte voorziening te creëren die geen onderdeel is van de iCentrale.

10 Veiligheidsthema Integrale beveiliging

10.1 Inventarisatie documenten

Niveau	Regelingen	Opmerking
EU Richtlijnen	2016/1148 beveiliging van netwerk- en informatiesystemen 95/45/EG Bescherming Persoonsgegevens	
Wetten NL	Telecommunicatiewet Wet bescherming persoonsgegevens	
Besluiten en Regelingen NL	Beleidsregels cameratoezicht	Camera's
Normen en Visie	NEN-ISO/IEC 27001:2005	
Landelijke beleid en Visie	Baseline Informatiebeveiliging Rijksdienst (BIR)	
	NTSC richtlijnen en aanbevelingen	
Rijkswaterstaat Beleid en Visie	Cybersecurity richtlijn Cybersecurity implementatierichtlijn RWS CS R06 - Richtlijn registratie CI items in een configuration management database (bijlage bij Richtlijnen Cybersecurity, 10 november 2015)	
	RWSCS R03 - Richtlijn voor handelwijze bij een hack, malwarebesmetting en verhoogde dreiging (bijlage bij Richtlijnen Cybersecurity, 10 november 2015)	
	CS R05 - Richtlijn camera's en omgang met camerabeelden van de verkeersregistratiesystemen	Camera's
Provinciaal Beleid en Visie	Interprovinciale Baseline Informatieveiligheid (IBI) Cybersecurity Implementatie Richtlijn PNH Richtlijnen Cybersecurity PNH	
Waterschappen	Baseline Informatiebeveiliging Waterschappen (BIWA)	
Lokaal Beleid en Visie	Strategische en Tactische Baseline Informatiebeveiliging Gemeenten (BIG)	
Achtergrond kennis en Visie	ICS/SCADA operationeel product (BID)	

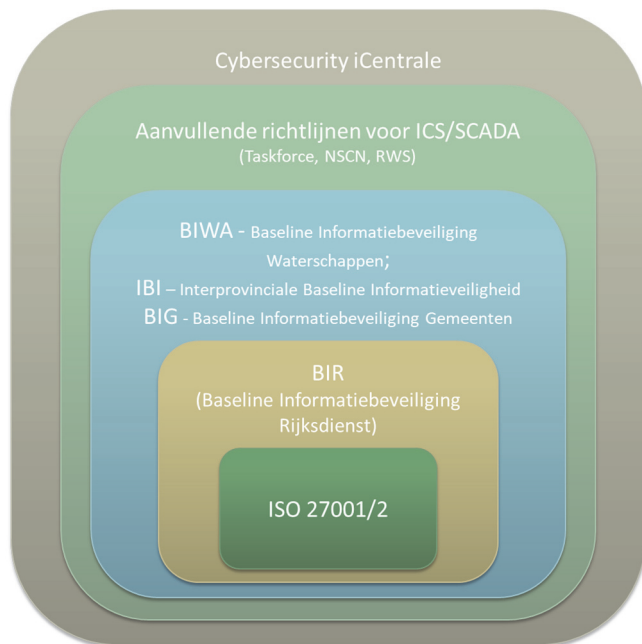
10.2 Uitwerking

De uitwerking is opgesplitst in 2 delen.

1. Cybersecurity
2. Cameratoezicht

10.2.1 Cybersecurity

Nederland kent een hiërarchie van baselines en richtlijnen waar de iCentrale rekening mee moet houden.



Figuur 17 - Hiërarchie van baselines en richtlijnen informatiebeveiliging

ISO27001

ISO 27001 is een ISO standaard voor informatiebeveiliging. De standaard bestaat feitelijk uit Deel 2 van de BS 7799, de standaard waarin wordt beschreven hoe Informatiebeveiliging procesmatig ingericht zou kunnen worden, om de beveiligingsmaatregelen uit ISO/IEC 17799 te effectueren. In Nederland is het vastgesteld als NEN norm NEN-ISO/IEC 27001:2005 en vertaald naar het Nederlands en verplicht gesteld voor Nederlandse overheden door het College standaardisatie.

De norm specificeert eisen voor het vaststellen, implementeren, uitvoeren, controleren, beoordelen, bijhouden en verbeteren van een gedocumenteerd Information Security Management System (ISMS) in het kader van de algemene bedrijfsrisico's voor de organisatie.

De norm specificeert verder eisen voor de implementatie van beveiligingsmaatregelen die zijn aangepast aan de behoeften van afzonderlijke organisaties of delen daarvan (bron: Wikipedia).

Baseline Informatiebeveiliging (BIR, BIWA, IRI, BIG)

De baseline informatiebeveiliging schrijft het basisniveau voor informatiebeveiliging bij de Rijksoverheid voor uitgaande van de ISO 27001/2 norm. De baseline biedt één normenkader voor de beveiliging van de Informatievoorziening (IV). Dit maakt het mogelijk om veilig samen te werken en onderling gegevens uit te wisselen.

Nederland kent een viertal baselines, namelijk:

- BIR - Baseline Informatiebeveiliging Rijksdienst en de nadere uitwerkingen daarvan in;
- BIWA - Baseline Informatiebeveiliging Waterschappen;
- IBI – Interprovinciale Baseline Informatieveiligheid;
- BIG - Baseline Informatiebeveiliging Gemeenten.

Aanvullende richtlijnen voor ICS/SCADA

De iCentrale gaat verder dan sec Informatievoorziening. De iCentrale is immers nadrukkelijk gepositioneerd in de wereld van ICS/SCADA-systemen (Industrial Control Systems/Supervisory Control And Data Acquisition) toegepast voor de bewaking en besturing van objecten, openbare ruimte en het managen van scheepvaart- en wegverkeer.

Met toename van dergelijke systemen met name ook bediening en besturing op afstand blijft het aantal kwetsbaarheden toenemen. Immers ook bediening en besturing op afstand **#iPixel Space Manager** vanuit een iCentrale vraagt veel van de beveiliging van de de ICS/SCADA systemen en de verbindingen met een iCentrale. **#Communication Logic<-> domein**

Niet alleen van nieuwe ICS/SCADA systemen, maar ook van bestaande systemen.

Systemen die, in tegenstelling tot bijvoorbeeld administratieve systemen, een lange levensduur van 15 tot 20 jaar hebben.

Dit verhoogt het risico op veiligheidsincidenten, bijvoorbeeld omdat er mogelijk via internet toegang **#Communication Logic<-> domein** kan worden verkregen tot systemen, waarbij met name de oude(re) systemen of embedded devices niet zijn gebouwd volgens het principe van security-by-design (waarmee wordt bedoeld dat beveiliging niet als kernbestanddeel in het ontwerp is meegenomen).

Een tweede verschil met reguliere systemen voor informatievoorziening is dat de gevolgen van falen van de beveiliging vrijwel direct voelbaar zijn voor burgers. Reputatieschade door negatieve publiciteit is een logisch gevolg. Dit is minstens zo belangrijk als de feitelijke gevolgen van een cyberaanval, aangezien het vertrouwen van burgers in overheidsorganisaties een hoge verantwoordelijkheid met zich brengt mee ten aanzien van de kwaliteit en de veiligheid die organisaties moeten bieden.

De baselines voor informatiebeveiliging voor waterschappen (BIWA), gemeenten (BIG), provincies (IBI) en Rijksoverheidsorganisaties (BIR) zijn, net als de richtlijnen van de ISO voor informatiebeveiliging, gebaseerd op drie aspecten van informatiebeveiliging, namelijk:

- Beschikbaarheid (B): het zorg dragen voor het beschikbaar zijn van informatie en informatie verwerkende bedrijfsmiddelen op de juiste tijd en plaats voor de gebruikers;
- Integriteit (I): het waarborgen van de correctheid, volledigheid, tijdigheid en controleerbaarheid van informatie en informatieverwerking;
- Vertrouwelijkheid (V): het beschermen van informatie tegen kennisname en mutatie door onbevoegden. Informatie is alleen toegankelijk voor degenen die hiertoe geautoriseerd zijn.

Voor ICS/SCADA ligt de prioriteit bij integriteit en beschikbaarheid. Integriteit betreft de juistheid van de output van sensoren en metingen, waarop de sturing van processen wordt gebaseerd. Als die begintdata niet overeenkomt met de werkelijkheid, dan kunnen fysieke verstoringen in het proces worden veroorzaakt. De beschikbaarheid van ICS/SCADA is tevens essentieel voor het kunnen uitvoeren van belangrijke bedrijfsprocessen. Het niet beschikbaar zijn van processen (zoals het sluiten van sluizen of het aansturen van gemalen) kan leiden tot fysieke schade of veiligheidsrisico's. Verstoringen, door bijvoorbeeld patch management, moeten derhalve ruim van tevoren worden ingepland. **#Housing**

Ten aanzien van het personeel **#Personnel** dat de systemen configureert, bedient en beheert is vertrouwelijkheid van gegevens en dan met name bedrijfsgegevens of persoonsgegevens van belang.

Door de Taskforce Bestuur en Informatieveiligheid Dienstverlening (Taskforce BID) zijn nadere aanbevelingen gedaan voor de beveiliging van ICS/SCADA. Rijkswaterstaat heeft zelf een cybersecurity implementatierichtlijn voor Objecten opgesteld.

10.2.2 Cameratoezicht

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. **#iLogging** Beelden kunnen persoonsgegevens bevatten.

Een voorbeeld van een persoonsgegeven is een videobeeld waarop een persoon zichtbaar is of gegevens staan die herleidbaar zijn tot een natuurlijk persoon. Persoonsgegevens moeten conform de Wet Bescherming Persoonsgegevens (Wbp) beveiligd worden.

In deze wet en de daarop berustende bepalingen wordt verstaan onder:

- persoonsgegeven:
elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon.
- verwerking van persoonsgegevens:
elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens;
- bestand:
elk gestructureerd geheel van persoonsgegevens, ongeacht of dit geheel van gegevens gecentraliseerd is of verspreid is op een functioneel of geografisch bepaalde wijze, dat volgens bepaalde criteria toegankelijk is en betrekking heeft op verschillende personen;
- verantwoordelijke:
de natuurlijke persoon, rechtspersoon of ieder ander die of het bestuursorgaan dat, alleen of tezamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt;

De beleidsregels voor de toepassing van bepalingen uit de Wet bescherming persoonsgegevens en de Wet politiegegevens vormen een verdere uitwerking van bepalingen uit de Wet bescherming persoonsgegevens en de Wet politiegegevens, die relevant zijn voor cameratoezicht door private of publieke organisaties, beveiliging van personen en goederen en door gemeenten ter handhaving van de openbare orde.

10.3 Knelpunteninventarisatie en Oplossingsrichtingen

10.3.1 Knelpunten Cybersecurity

1

Knelpunt **Integrale Beveiliging.#Hosting.Knelpunt 1**

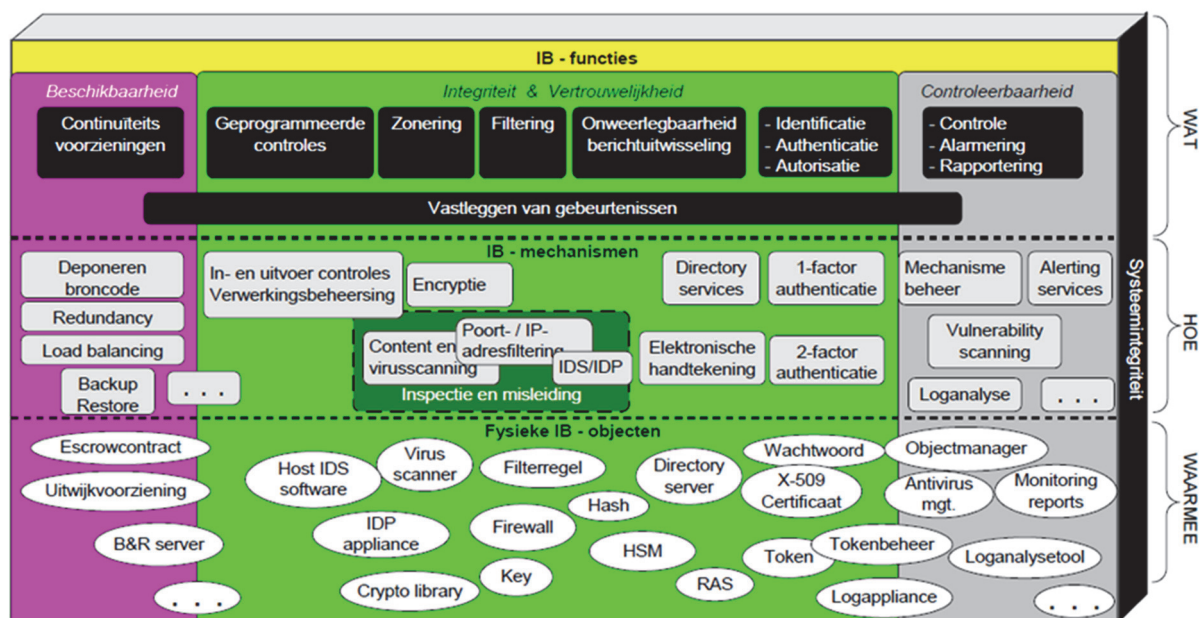
De iCentrale zelf is een object dat moet worden beveiligd tegen mogelijke cyberaanvallen. Zeker met het combineren van domeinen en beheergebieden wordt het steeds interessanter een cyberaanval uit te voeren.

Oplossingsrichting

Onderken – in termen van de BIR – de patronen horende bij een iCentrale, te weten:

- generieke netwerkconfiguratie;
- koppelvlakken (met vertrouwde en onvertrouwde netwerken);
- servers en werkplekken;
- generieke applicatieconfiguratie;
- multifunctional configuratie;
- identificatie, authenticatie en autorisatie;
- Public Key Infrastructure (PKI);
- draadloze netwerken;
- Demilitarised Zone;
- logging & monitoring;
- data recovery;

en richt deze patronen in conform de BIR en naar de specifieke karakteristieken van die iCentrale. Daarbij gaat het om het vaststellen wat moet worden gedaan aan beveiliging, hoe dat moet worden gedaan en waarmee.



NORA- model IB-functies (als doorontwikkeling van ISO-NEN 7498-21)

Besteed vervolgens speciale aandacht aan de ICS/SCADA door:

1. Vast te stellen voor welke organisatorische processen ICS/SCADA is toegepast. Belangrijk is hierbij te kijken naar de functie van het proces, de betekenis van het proces voor de doelen van de organisatie en de fysieke locatie en netwerklocaties (asset management) van de ICS/SCADA.

2. Vaststellen wie verantwoordelijk is voor de ICS/SCADA-toepassing. Bij het onderzoeken van de (verdeling van) verantwoordelijkheden voor een bepaalde ICS/SCADA moet in ieder geval onderscheid worden gemaakt in de proceseigenaar, de beheerder (bv. IT of facilitair) en de verantwoordelijke voor de fysieke locatie. 3. Ontwikkelen van organisatiebeleid ten aanzien van ICS/SCADA. Door het verantwoordelijke management moeten algemeen geldende richtlijnen en maatregelen voor de omgang met ICS/SCADA worden beschreven. Beleid legt de basis voor een veilige en professionele omgang met ICS/SCADA in de organisatie. 4. Het vastleggen van verantwoordelijkheid, en eenduidige en gedragen processen van beheer, onderhoud en inkoop voor ICS/SCADA is noodzakelijk in elke organisatie. 5. Uitvoeren van pentesten op de ICS/SCADA-omgeving. Om de zwakste plekken te identificeren en deze direct te kunnen verbeteren, is het belangrijk om penetratietesten uit te voeren op de ICS/SCADA. Aanvallen van buiten kunnen op deze manier worden voorkomen. 6. Blijvend monitoren van de ICS/SCADA-omgeving. Door voortdurende monitoring van de netwerkomgeving door netwerk managementtools en Intrusion Detection Systems (IDS) of Security Information and Event Management (SIEM) ontstaat een beter en steeds actueel beeld van de veiligheid van ICS/SCADA in de organisatie. Hierdoor worden voorheen nog onbekende kwetsbaarheden inzichtelijk en is verbetering mogelijk.

2
Knelpunt Integrale Beveiliging.#Hosting.Knelpunt 2
Een actuele “configuratie management” database maakt het de iCentrale en de opdrachtgever aan de iCentrale mogelijk om proactief cybersecurity kwetsbaarheidsanalyses uit te kunnen voeren en de beheerders te adviseren over maatregelen alsmede het kunnen analyseren van security incidenten of storingen. Derhalve moet de opdrachtgever vanuit een informatievoorzieningsketen benadering kunnen leunen op de kwaliteit van de afzonderlijke “configuratie management” databases die door de afzonderlijke managementsystemen en de systemen binnen de iCentrale worden opgezet en bijgehouden.
Oplossingsrichting
Richt een “configuratie management” database in van alle management systemen bediend vanuit de iCentrale en de systemen binnen de iCentrale zelf. Voer vervolgens proactief cybersecurity kwetsbaarheidsanalyses uit aan de hand van de gegevens uit deze database, te weten: 1. Type en merk ICT en/of ICS/SCADA apparatuur; 2. Producent en Leverancier; 3. Versie nummer van ICT en/of ICS/SCADA; 4. Type object en locatiegegevens; 5. Ingezette software en hardware componenten inclusief hun samenhang en configuratie; 6. Informatie over de backup voorziening; 7. Datum laatste back-up en locatie van de back-up; 8. OS (Operation System), versie OS en Firmware; 9. Ingezette netwerk en applicatieprotocollen; 10. licentie informatie en verloopdatum licentie; 11. Escrow documentatie; 12. Welke antimalware applicatie en versie; 13. Netwerkoverzichten fysieke en logisch en IP-plan; 14. IP- en MAC-adres, DNS en hostnaam; 15. Documentatie patch procedure;

16. Datum laatste patch en versie;
17. Vervangingsinstructie en/of -procedure voor apparaat;
18. Identificatie en verwijzing naar vindplaats gebruikers, beheer en onderhoudsdocumentatie;
19. Datum laatst gewijzigd en door wie.

Bij het opzetten van de database moet nadrukkelijk rekening worden gehouden met de verschillen tussen systemen voor informatievoorziening en ICS/SCADA systemen. De laatste vragen om systeemeigen beveiligingsvoorzieningen, het zijn veelal Mission Critical systemen.

Zo moet "patch management" ook worden ingericht voor ICS/SCADA, maar volgens een andere werkwijze dan bij reguliere systemen voor informatievoorziening. Hetzelfde geldt voor het inrichten van toegangsbeveiliging van een iCentrale of objectgebouw, firewalls, de architectuur, en alle andere aspecten van ICS/SCADA.

Om de beveiliging van ICS/SCADA te borgen in de organisatie en blijvend te verbeteren zijn de volgende stappen aan te bevelen:

1. Maatregelen uit analyses implementeren. De geïdentificeerde maatregelen uit de GAP-analyse (Zelfevaluatie voor provincies) en mogelijke additioneel uitgevoerde risicoanalyse moeten worden geïmplementeerd;
2. Ontkoppelen. Dataverkeer tussen ICS/SCADA enerzijds en kantoorautomatisering en internet anderzijds, moet zoveel als mogelijk worden beperkt. Waar nodig moet ICS/SCADA worden ontkoppeld als niet-noodzakelijke verbindingen met kantoorautomatisering of internet bestaan. Als het niet anders kan, moet netwerkverkeer slechts unidirectionaal worden toegestaan;
3. Remote access verbeteren. Als toegang op afstand noodzakelijk is voor bepaalde ICS/SCADA dan moet deze verbinding goed beveiligd zijn met VPN, netwerkmonitoring en firewalls;
4. Fuzz testen. In een fuzz test worden systemen blootgesteld aan onjuiste of onverwachte data input. Vervolgens worden de gevolgen op het systeem gemonitord. Fuzz testen kan onverwachte systeem crashes of geheugen lekken onthullen die de beschikbaarheid of integriteit van ICS/SCADA kunnen ondermijnen.

3

Knelpunt **Integrale Beveiliging.#Hosting.Knelpunt 3**

Indien zich een cyberaanval voordoet of dreigt voor te doen gaat er erom tijdig te acteren (bij dreiging) of reageren (bij een concrete aanval). Scenario's helpen daarbij.

Oplossingsrichting

Een iCentrale dient over drie volledig uitgewerkte scenario's te beschikken:

1. Hack: één of meer IA systemen zijn of worden gehacked;
2. Malware besmetting: één of meer IA systemen zijn besmet met malware;
3. Verhoogde dreiging: er is een verhoogde dreiging op een hackaanval op managementsystemen bediend vanuit de iCentrale of systemen binnen de iCentrale zelf.

Hack

Als het object in beweging is gebracht, zonder dat de bedienaar hier bewust opdracht toe heeft gegeven via het ICS/SCADA systeem, dan is er mogelijk sprake van een cyberaanval op het object. De opdrachtnemer wordt via een storingsmelding van de bedienaar (buiten het systeem om) opgeroepen om ter plaatse te komen.

De monteur van de opdrachtnemer neemt de volgende stappen:

1. Vraag aan de bedienaar wat er precies aan de hand is (indien het object onverwachte en 'onbeheersbare' acties blijft vertonen dan zal de bedienaar het object veiligstellen);
2. Controleer mogelijke storingsmeldingen aan het IA-systeem op de gebruikelijke manier;
3. Onderzoek, indien aanwezig, de logs van het betreffende IA systeem dat het object bedient op onregelmatigheden;

4. Stel, zo mogelijk, vast dat het niet om een technische storing gaat;
5. Rapporteer via het storingsproces de bevindingen terug naar de opdrachtgever;
6. Afhankelijk van de door de monteur gerapporteerde bevindingen kunnen nadere instructies vanuit opdrachtgever volgen die door de monteur opgevolgd moeten worden om er zeker van te zijn dat het om een hack(poging) gaat;
7. Als er daadwerkelijk sprake is van een hack(poging) informeer dan de betrokkenen van de regio (bedienaars, Officier van Dienst etc).

Scenario bij Malware besmetting

Als (bijvoorbeeld tijdens een reguliere onderhoudsbeurt) er een (vermoeden van een) malware besmetting op het object is, dienen de volgende acties te worden genomen:

1. Meld een mogelijke malware besmetting op de reguliere manier als het melden van storingen onder vermelding van mogelijk risico op malwarebesmetting en geef alle bevindingen door;
2. Het oplosteam zal contact zoeken met de monteur voor afstemming van de uit te voeren acties;
3. Wijzig niets aan het systeem als dat voor een veilige werking van het object niet strikt noodzakelijk is;
4. Maak, indien daarom wordt gevraagd, een volledige image van de (systeem)software van het betreffende IA systeem / -onderdeel;
5. Stel deze image van de (systeem)software ter beschikking voor nader onderzoek;
6. Wees alert op onverwachte bewegingen / storingen van het object en informeer de bedienaar om hier ook alert op te zijn;
7. Indien er sprake blijkt te zijn van malware besmetting, controleer dan of de back-up ook is besmet;
8. Indien er sprake is van een malwarebesmetting en de back-up blijkt niet geïnfecteerd, zet dan de back-up terug op het systeem;
9. Als ook de back-up besmet is, zorg er dan voor dat de besmette image 'geschoond' wordt en zet de geschoonde versie terug.
10. Let op dat de juiste parameters zijn ingesteld;
11. Meld de storing op de reguliere manier af.

Scenario bij Verhoogde Cyberdreiging

Er is sprake van verhoogde cyberdreiging als blijkt dat er een mogelijke aanval op objecten aangesloten op de iCentrale op handen is. 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 o.a. Rijkswaterstaat zijn aangesloten op het proces en *Alerteringssysteem Terrorismebestrijding* (ATb) van het ministerie van Veiligheid en Justitie.

Indien er sprake is van een verhoogde cyberdreiging dan meldt het Departementaal Coördinatiecentrum Crisisbeheersing (DCC) van het ministerie van Infrastructuur en Milieu dit aan het lijnmanagement van de betreffende wegbeheerder als de dreiging op een specifiek object is gericht.

De beheerder van de iCentrale moet vervolgens via het storingsmeldingsproces op de hoogte

Worden gebracht van de verhoogde dreiging. De beheerder van de iCentrale neemt de volgende acties:

1. De beheerder van de iCentrale neemt naar aanleiding van de storingsmelding contact op met de door de opdrachtgever aangegeven contractpersoon voor afstemming van uit te voeren acties en het tijdstip waarop deze acties nodig zijn;
2. Indien er sprake is van een acute dreiging dan zorgt de beheerder van de iCentrale er voor dat er voldoende technisch personeel standby is om de iCentrale en de verbindingen met de aangesloten managementsystemen in het verzorgingsgebied te bewaken;
3. Indien er daadwerkelijk 'hacks' plaatsvinden dan gelden de stappen onder Hack.

10.3.2 Knelpunten Cameratoezicht

1
Knelpunt Integrale Beveiliging.#iLogging.Knelpunt 1
Via camera's kan een persoon zonder onevenredige inspanning identificeerbaar zijn. Dan kan doordat een persoon voldoende herkenbaar in beeld wordt gebracht of via een identiteitskenmerk zoals een kentekennummer te identificeren is. Bij iedere taak is het dan ook de vraag of de doeleinden waarvoor de camerabeelden worden ingezet niet op een andere wijze kunnen worden verwezenlijkt, die minder nadelig is voor de betrokkenen, dan is het betreffende cameratoezicht niet toegestaan (subsidiariteit)
Oplossingsrichting
Uitvoeren van een <i>Privacy impact assessment (PIA)</i>, waarbij onderstaande uitgangspunten moeten in elk geval in acht worden genomen voordat een camera wordt ingezet. 1. Stel vast wie de verantwoordelijke zal zijn voor het verwerken van persoonsgegevens door middel van een camera. In het algemeen geldt dat degene die beslist over de doeleinden en de inzet van een camera als verantwoordelijke wordt aangemerkt; 2. Bepaal samen met deze verantwoordelijke de doeleinden van de inzet van een camera. Benoem expliciet zowel de hoofddoelen als de neven-doelen, zodat er geen twijfel over bestaat waarvoor een camera zal worden ingezet. Voor overheden is het doel gerelateerd aan de wettelijke taak van de betreffende overheidsorganisatie; 3. Stel vast op welke grondslag een camera zal worden ingezet. De verwerking van persoonsgegevens door middel van een camera mag alleen plaatsvinden indien daarvoor een grondslag in de zin van de Wbp aanwezig is. Artikel 8 Wbp noemt zes algemene grondslagen, waarvan er slechts vier relevant zijn voor cameragebruik, namelijk: • de gegevensverwerking noodzakelijk is om een wettelijke verplichting na te komen waaraan de verantwoordelijke onderworpen is. Deze wettelijke verplichting moet worden benoemd, alsmede de noodzaak van gebruik van camerabeelden daarbij; • de gegevensverwerking noodzakelijk is ter vrijwaring van een vitaal belang van de betrokkene. Dit vitale belang moet worden benoemd, alsmede de noodzaak van gebruik van camerabeelden daarbij; • de gegevensverwerking noodzakelijk is voor de goede vervulling van een publiekrechtelijke taak door het desbetreffende bestuursorgaan dan wel het bestuursorgaan waaraan de gegevens worden verstrekt. Deze publiekrechtelijke taak moeten worden benoemd, alsmede de noodzaak van gebruik van camerabeelden daarbij; • de gegevensverwerking noodzakelijk is voor de behartiging van het gerechtvaardigde belang van de verantwoordelijke of van een derde aan wie de gegevens worden verstrekt. Dit belang moet worden benoemd, alsmede de noodzaak van gebruik van camerabeelden daarbij. Aanvullend moet de reden worden benoemd waarom dit belang en het gebruik van camerabeelden prevaleert boven het belang of de fundamentele rechten en vrijheden van de betrokkene(n), in het bijzonder het recht op bescherming van de persoonlijke levenssfeer; 4. Stel vast dat de inzet van een cameratoezicht noodzakelijk is. De inzet van een camera moet noodzakelijk zijn om de gestelde doeleinden te kunnen bereiken. Hierbij moeten de belangen van de betrokkenen worden meegewogen. Op deze belangen mag namelijk geen onevenredige inbreuk worden gemaakt in verhouding tot de gestelde doeleinden (proportionaliteit). Als de doeleinden bovendien op een andere wijze kunnen worden verwezenlijkt die minder nadelig is voor de betrokkenen, dan is het betreffende cameratoezicht niet toegestaan (subsidiariteit) 5. Bepaal welk soort camera of softwaretechniek in het concrete geval gerechtvaardigd is om in te zetten. De ene camera of softwaretechniek kan een grotere inbreuk op de persoonlijke levenssfeer maken dan de andere. Ook hierbij moeten de belangen van de betrokkenen worden meegewogen (proportionaliteit en subsidiariteit);

6. Bepaal wat er met de camerabeelden zal worden gedaan. Aan wie zullen de beelden worden verstrekt? Hoe lang zullen de beelden worden bewaard?) De van toepassing zijnde wettelijke regelingen kunnen hierover nadere regels stellen;
7. Zorg ervoor dat de camerabeelden adequaat zullen worden beveiligd. Maak hierbij gebruik van algemeen geaccepteerde beveiligingsstandaarden. Controleer vervolgens periodiek of de beveiligingsmaatregelen daadwerkelijk zijn getroffen en worden nageleefd. Evalueer tevens periodiek of de getroffen beveiligingsmaatregelen nog voldoende zijn. Pas waar nodig de beveiligingsmaatregelen aan;
8. Bepaal of, en zo ja, op welke wijze, de betrokkenen moeten worden geïnformeerd over de inzet van cameratoezicht. Het adequaat informeren van de betrokkenen over de inzet van cameratoezicht is een belangrijk instrument om de gegevensverwerking transparant te maken. De van toepassing zijnde wettelijke regelingen kunnen hierover nadere regels stellen, bijvoorbeeld over het moment van informeren en de inhoud van de informatie;
9. Houd er rekening mee dat de betrokkenen hun rechten, zoals het recht op inzage of correctie, kunnen uitoefenen. De betrokkenen hebben diverse rechten jegens de verantwoordelijke die camerabeelden van hen maakt. Zo hebben de betrokkenen bijvoorbeeld recht op inzage van hun persoonsgegevens en kunnen zij de verantwoordelijke in bepaalde gevallen verzoeken om hun gegevens te verbeteren, aan te vullen, te verwijderen of af te schermen. De van toepassing zijnde wettelijke regelingen kunnen hierover nadere regels stellen.

2

Knelpunt **Integrale Beveiliging.#iLogging.Knelpunt 2**

Eenmaal inzet, moet bewaakt worden dat camerabeelden niet ongeoorloofd worden gebruikt.

Oplossingsrichting

Voor het beveiligingsbewust omgaan met camera's en systemen waarin camerabeelden worden opgeslagen gelden de volgende instructies:

1. Alleen geautoriseerde medewerkers van de opdrachtnemer mogen beheren onderhoudswerkzaamheden uitvoeren aan camera's en systemen die camerabeelden opslaan;
2. 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;
3. Zonder uitdrukkelijke toestemming van de opdrachtgever worden camerabeelden niet vernietigd, verwijderd of verstrekt aan derden of gebruikt voor persoonlijke of bedrijfsdoeleinden;
4. 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 achtname 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;
5. 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;
6. Indien onregelmatigheden worden geconstateerd rondom de inzet, werking en opslag van camerabeelden dient dit direct als beveiligingsincident bij de opdrachtgever gemeld te worden.

1.1 Input andere projecten

1.1.1 Project 1.2: Verantwoordelijkheidsverdeling publiek-privaat als randvoorwaarde voor de iCentrale

Doel van het project is:

- Het aangeven van de knip tussen publieke en private partij(en) voor nu en in de toekomst.
- Overzicht taken van de private en publieke partijen.
- Specificeren van functies die uitgevoerd moeten worden door de assets en het personeel van de centrales.
- Opdelen taken en functies in strategisch, tactisch en operationeel.

Relatie met veiligheidskaders

De verantwoordelijkheid van het borgen van veiligheid moet duidelijk belegd worden

Input: Voorgestelde verantwoordelijkheidsverdeling

Output: iCentrale veiligheidskaders tbv toetsing verantwoordelijkheidsverdeling.

Project 1.2 is niet uitgevoerd. Er is geen input van dit project.

1.1.2 Project 1.3: Back-up- Overnametaken

1. In dit project wordt gekeken onder welke voorwaarden iCentrales als backup-centrale voor elkaar kunnen dienen in noodsituaties.

Relatie met veiligheidskaders

Back-up en overname functie moet aan de veiligheidskaders worden getoetst

Input: Back-up/overnametaken zijn als scenario's input voor de knelpunten analyse

Output: Knelpunten en oplossingsrichtingen t.b.v. optimalisatie.

Project 1.3 is niet uitgevoerd. Er is geen input van dit project.

1 1.3 Project 1.5: Combineren functies binnen de verschillende domeinen

Relatie met veiligheidskaders

Veiligheidsconcepten kunnen domeinafhankelijk zijn.

Input: scenario's tbv knelpunten analyse.

Output: Knelpunten en oplossingsrichtingen tbv optimalisatie.

Project 1.5 is niet uitgevoerd. Er is geen input van dit project.

1 1.4 Project 1.7: Functionele Koppelvlakken

Relatie met veiligheidskaders

Veiligheidskaders zijn input voor het vaststellen van de mogelijke automatiseringsgraad

Project is in een later stadium opnieuw gedefinieerd naar 'Agile-proces SLA's voor alle iCentrale HG toplevel onderdelen'.

Doel is te komen tot reële en bruikbare indicatoren voor de SLA's van de iCentrale hoofdgroep toplevel onderdelen.

De gewenste in- en output is daardoor niet relevant.

De verwachte in-/output was:

Input: Gewenste automatiseringsgraad kan als input gelden voor de oplossingsrichtingen.

Output: Automatiseringsgraad is in de mogelijkheden afhankelijk van de veiligheidskaders.

1 1.5 Project 2.3: High Level MMI: bedienproces verschillende domeinen

Doel

Analyseren en uitwerken van de verschillende bedienprocessen per domein en de daarbij horende informatie- en bedienbehoefte gezien vanuit de bedienaar

Relatie met veiligheidskaders

Uniforme bedienfilosofie is input om te komen tot de uiteindelijk veiligheidskaders

Input/ Output

Input: Uniforme bedienfilosofie is input voor de knelpuntenanalyse

1 1.6 Project 2.4: Uniforme bediening iCentrale

Doel

Het ontwikkelen van geautomatiseerde informatieverwerking (bijvoorbeeld beeldverwerking en data-analyse) met tot doel taakverlichting operators en integratie van domeinen.

Relatie met veiligheidskaders

Uniforme bedienfilosofie is input om te komen tot de uiteindelijk veiligheidskaders

Input/ Output

Input: Uniforme bedienfilosofie is input voor de knelpuntenanalyse

Output: Veiligheidskaders en oplossingsrichtingen gelden als input voor het definiëren van de uniforme bediening.

1 1.7 Project 4.1: Functionele Architectuur

Doel

De blauwdruk belichaamt de kern van de gebruiksfuncties voor iCentrales én is de basis voor de iCentrale technische architectuur én in Nieuwe en bestaande iCentrales de werkomgeving waarmee operators hun bestaande en nieuwe taken gaan vervullen.

Relatie met veiligheidskaders

Kaderscheppend

Input/ Output

Input: Functionele integratie is input voor de knelpuntenanalyse

1 1.8 Project 4.2: Technische koppelvlakken

Doel

Completering van de blauwdruk voor het technisch platform voor een iCentrale met de bijbehorende open koppelvlakken.

Relatie met veiligheidskaders

Randvoorwaardelijk

Input/ Output

Input: Technische koppelvlakken beschreven (on)mogelijkheden

Output: Oplossingsrichtingen vragen mogelijk om technische oplossingen in de vorm van koppelvlakdefinities.

Zie hiervoor de #Koppelvlakken.

12 Conclusie

Het doel van het project Veiligheidskaders was het komen tot een bruikbare leidraad voor implementatie van veiligheid voor iCentrale producten/diensten en was bedoeld voor een ieder die betrokken is bij de implementatie van iCentrale producten/diensten.

Er is methodisch gewerkt om via veiligheidsthema's, de relevante veiligheidsdocumenten te identificeren en te koppelen aan iCentrale-onderdelen.

Het in kaart brengen van de relevante veiligheidsdocumenten, is een project op zich gebleken. Het geeft een duidelijk overzicht. Deze grote hoeveelheid aan informatie biedt veel inzicht. Bij de lezer kan de indruk zijn gewekt, dat al deze informatie gecomprimeerd in deze leidraad is opgenomen. Echter, door experts is een keuze gemaakt, in wat als relevant voor de iCentrale werd gezien.

Een lezer kan, met de geboden documentatie en methode, zelf op zoek naar gedetailleerdere informatie of de iCentrale belichten vanuit zijn eigen kader.

De leidraad ondersteunt de op te stellen modeluitvragen en modelcontracten.

Niet in de vorm van vaste teksten, maar in de vorm van oplossingsrichtingen, aandachtspunten en beschouwingen van de veiligheidsthema's.

De leidraad geeft hierdoor handvatten. Deze kunnen in een volgende versie nog concreter worden gemaakt, door toe te werken naar kant en klare artikelen, zodat ze nog directer aansluiten bij aanbiedingen en contracten.

Uit deze leidraad blijkt dat er geen onoverkomelijke problemen zijn om te komen iCentrale gerelateerde uitvragen en aanbiedingen. Voor elk geconstateerd probleem, blijkt een oplossing voorhanden.

13 Lijsten

13.1 Referentie Configuratie-items naar documentpassage

Deze lijst kan worden gebruikt om, per configuratie-item, de relevante teksten op te zoeken.

#

#Bedienfilosofie

- Externe Veiligheid, 35, 36
- Tunnelveiligheid, 47
- Tunnelveiligheid.Knelpunt1, 50
- Verkeersveiligheid, 25

#Bedieninstructies

- Arbeidsveiligheid, 21
- Externe Veiligheid, 35, 36
- Externe Veiligheid.Knelpunt1, 36
- Nautische Veiligheid, 31
- Tunnelveiligheid, 47
- Tunnelveiligheid.Knelpunt1, 50
- Veiligheid Beweegbare Objecten, 39, 40
- Verkeersveiligheid, 25

#Communication Logic<-> domein

- Integrale Beveiliging, 53

#Emergency stop

- Veiligheid Beweegbare Objecten, 43

#Headset

- Tunnelveiligheid, 49

#Horn

- Tunnelveiligheid, 49

#Hosting

- Arbeidsveiligheid, 17, 18, 21
- Knelpunt 1, 55
- Knelpunt 2, 56
- Knelpunt 3, 57

#Housing

- Arbeidsveiligheid, 16, 17, 18, 19, 20, 21
- Arbeidsveiligheid.knelpunt1, 21
- Integrale Beveiliging, 53
- Knelpunt1, 22

#iAudiomanager

- Arbeidsveiligheid.Knelpunt1, 21
- Knelpunt1, 22

#iAuthenticator

- Tunnelveiligheid, 48

#iData Mapper

- Nautische Veiligheid.Knelpunt1, 34
- Verkeersveiligheid.Knelpunt1, 26
- Verkeersveiligheid.Knelpunt2, 26

#iEmergency Stop

- Arbeidsveiligheid, 20

#iEmergency stop manager

- Tunnelveiligheid, 48
- Veiligheid Beweegbare Objecten, 43

- #iEvent detector
 - Tunnelveiligheid, 48
 - Tunnelveiligheid.Knelpunt1, 49
 - Veiligheid Beweegbare Objecten, 43
 - Veiligheid Beweegbare Objecten.Knelpunt1, 44
 - Verkeersveiligheid.Knelpunt1, 26
- #iHMI
 - Verkeersveiligheid.Knelpunt1, 26
- #iLogging
 - Arbeidsveiligheid, 21
 - Integrale Beveiliging, 54
 - Knelpunt 1, 59
 - Knelpunt 2, 60
 - Nautische Veiligheid, 32
- #iNotification panel
 - Tunnelveiligheid, 48, 49
 - Veiligheid Beweegbare Objecten, 39, 43
 - Veiligheid Beweegbare Objecten.Knelpunt1, 44
- #iOrkestrator
 - Arbeidsveiligheid, 16, 19, 21
 - Arbeidsveiligheid.knelpunt1, 16
 - Knelpunt1, 22
 - Nautische Veiligheid, 31
 - Nautische Veiligheid.Knelpunt1, 34
 - Tunnelveiligheid, 48
 - Tunnelveiligheid.Knelpunt1, 50
 - Veiligheid Beweegbare Objecten, 41
 - Veiligheid Beweegbare Objecten.Knelpunt1, 44
- #iPixel Space Manager
 - Integrale Beveiliging, 53
 - Nautische Veiligheid, 31, 32
 - Tunnelveiligheid, 48
- #iPredictor
 - Tunnelveiligheid, 48
- #iState Estimator
 - Tunnelveiligheid, 48
- #iWorkspace manager
 - Veiligheid Beweegbare Objecten, 43
- #joystick
 - Tunnelveiligheid, 48
- #keyboard&mouse
 - Tunnelveiligheid, 48
- #Keyboard&mouse
 - Arbeidsveiligheid, 20
- #koppelvlakken business logic
 - Nautische Veiligheid, 32
 - Veiligheid Beweegbare Objecten, 43
- #koppelvlakken presentation logic
 - Arbeidsveiligheid, 20
 - Tunnelveiligheid, 48
 - Veiligheid Beweegbare Objecten, 39, 43
- #Loudspeaker
 - Arbeidsveiligheid, 21
 - Arbeidsveiligheid.Knelpunt1, 21
 - Knelpunt1, 22
 - Nautische Veiligheid, 32

Tunnelveiligheid, 49	
#Monitor	
Arbeidsveiligheid, 20	
Nautische Veiligheid, 32	
Tunnelveiligheid, 48	
#Personnel	
Arbeidsveiligheid, 16, 17, 19	
Externe Veiligheid, 35	
Integrale Beveiliging, 53	
Nautische Veiligheid, 31, 32	
Tunnelveiligheid, 46	
Tunnelveiligheid.Knelpunt1, 49	
Veiligheid Beweegbare Objecten, 40	

13.2 Figuren

Figuur 1 Hoofdzaken veiligheid	5
Figuur 2 Weergave reikwijdte veiligheid	6
Figuur 3 Allocatie Veiligheidsthema's	9
Figuur 4 Gevolgde aanpak per veiligheidsthema	10
Figuur 5 Regelgeving	11
<i>Figuur 6 Snapshot configuratie-items veiligheid (14.3 Configuratie-items veiligheid).....</i>	<i>13</i>
Figuur 7 Coördineren	13
Figuur 8 Attenderen	13
Figuur 9 Observeren.....	13
Figuur 10 Communiceren.....	14
Figuur 11 Managen	14
Figuur 12 VEILIG INGRIJPEN	14
Figuur 13 Cross-reference systeemfuncties met configuratie-items	14
Figuur 14. Hoofdtaken van regionale operationele verkeersbeheersing (ROV) (bron: AVB-VA)	25
Figuur 15 IVS90 en Marifoon in scope, schip en vaarweg buiten scope	28
Figuur 16 Noodbediening (out of scope) vs Noodstop (scope).....	38
Figuur 17 - Hiërarchie van baselines en richtlijnen informatiebeveiliging	52

13.3 Tabellen

Tabel 1 Inventarisatie documenten Arbeidsveiligheid.....	16
Tabel 2 Inventarisatie documenten Verkeersveiligheid	23
Tabel 3 Inventarisatie documenten Nautische veiligheid	27
Tabel 4 Schutproces	31
Tabel 5 Inventarisatie documenten externe veiligheid.....	35
Tabel 6 Inventarisatie documenten Veiligheid beweegbare objecten	37
Tabel 7 Stappenplan beweegbare brug	39
Tabel 8 Eisen beweegbare brug	39
Tabel 9 Inventarisatie documenten Tunnelveiligheid.....	45
Tabel 10 Stappenplan Afhandeling Incidenten en calamiteiten	46
Tabel 11 Soorten Incidenten en calamiteiten	46

14 Bijlagen

14.1 Onderzochte veiligheidsdocumenten

Crosscheck Veiligheidsthema's - Domein
21-12-2017



					Status	
SOORT VEILIGHEID	Id	Gebied	Soort	Document	Verwerkt	Bevindingen Ja/Nee
ARBEIDSVEILIGHEID	1	EUROPEES	EU RICHTLIJN	Richtlijn Arbeidsmiddelen (richtlijn Arbeidsmiddelen in Nederland geïmplementeerd in hoofdstuk 7 van het Arbobesluit en de Arboregeling)	Nee	Nee
	2	NATIONAAL	NL WET	Arbowet	Ja	Ja
	3	NATIONAAL	NL BESLUIT REGELINGEN	Arbeidsomstandighedenregeling	Ja	Ja
	3			Arbobesluit	Ja	Ja
	4	NATIONAAL	NL Normen en Visie	CROW publicatie 96a 'Maatregelen op autosnelwegen	Nee	CROW publicatie 96a 'Maatregelen op autosnelwegen is een in principe niet bindende richtlijn waaraan bijv. RWS zich wel conformeert. Hier buiten beschouwing gelaten omdat de 'RWS-richtlijn voor verkeersmaatregelen bij wegwerkzaamheden op rijkswegen' die hier deel van uitmaakt reeds behandeld wordt onder verkeersveiligheid
	5	PROVINCIAAL	Noord-Holland	Beleid, Visie	-	
	5	PROVINCIAAL	Utrecht	Beleid, Visie	-	
	5	PROVINCIAAL	Flevoland	Beleid, Visie	-	
	6	LOKAAL	Almere	Beleid, Visie	-	
	6	LOKAAL	Den Haag	Beleid, Visie	-	
	6	LOKAAL	Rotterdam	Beleid, Visie	-	
	7	OVERIG				

Crosscheck Veiligheidsthema's - Domein
21-12-2017



SOORT VEILIGHEID	Id Gebied		Soort	Document	Status	
					Verwerkt	Bevindingen Ja/Nee
VERKEERSVEILIGHEID	1	EUROPEES	EU RICHTLIJN	Richtlijn Verkeersveiligheid	Ja	Ja
	2	NATIONAAL	NL WET	Meerjarenprogramma Infrastructuur	Ja	Nee
				Rijksinfrastructuurfonds	Ja	Nee
				Wegenwet	Ja	Nee
				Wegenverkeerswet	Ja	Ja
				Wet beheer Rijkswaterstaatswerken	Ja	Nee
				Wet Ruimtelijke Ordening	Ja	Nee
	3	NATIONAAL	NL BESLUIT REGELINGEN	Beleidsregels Incident Managment Rijkswaterstaat	Ja	Ja
				Besluit Algemene Regels Ruimtelijke Ordening	Ja	Nee
				Structuurvisie Infrastructuur en Ruimte	Ja	Nee
	4	NATIONAAL	NL Normen en Visie	Ministerie van V&W - Strategie Verkeersveiligheid	Ja	Nee
				Ministerie van V&W - Strategisch plan Verkeersveiligheid	Ja	Nee
				RWS - Richtlijn Wegwerkzaamheden	Ja	Ja
	5	PROVINCIAAL	Noord-Holland	Beleid, Visie	Ja	Nee
				Meerjarenprogramma Infrastructuur	Ja	Nee
				Provinciale Ruimtelijke Verordening	Ja	Nee
				Structuurvisie Ruimtelijke Ordening	Ja	Nee
	5	PROVINCIAAL	Utrecht	Beleid, Visie	-	-
	5	PROVINCIAAL	Flevoland	Beleid, Visie	Ja	Nee
	6	LOKAAL	Almere	Beleid, Visie	-	-
	6	LOKAAL	Den Haag	Beleid, Visie	-	-
	6	LOKAAL	Rotterdam	Beleid, Visie	-	-
	7	OVERIG		ProMeV - Proactief Meten Verkeersveiligheid	Ja	Ja
	7	OVERIG		Opmerking: het CROW kent enkele publicaties met richtlijnen op het gebied van o.a. verkeersmanagement en big data. Deze zijn in principe niet bindend (tenzij organisaties deze zelf verbindend verklaren)	-	-

Crosscheck Veiligheidsthema's - Domein
21-12-2017



SOORT VEILIGHEID	Id Gebied		Soort	Document	Status	
					Verwerkt	Bevindingen Ja/Nee
NAUTISCHE VEILIGHEID	1	EUROPEES	EU RICHTLIJN	-		
	2	NATIONAAL	NL WET	Deltafonds	Ja	Nee
				Scheepvaartverkeerswet	Ja	Ja
	3	NATIONAAL	NL BESLUIT REGELINGEN	Besluit Algemene Regeld Ruimtelijke Ordenning	Ja	Nee
				Binnenvaartpolitiereglement	Ja	Ja
				Binnenvaartregeling	Ja	Nee
				Regeling communicatie en afmetingen rijksbinnenwateren	Ja	Ja
				Rijnvaartpolitiereglement	Ja	Nee
				Structuurvisie Infrastructuur en Ruimte	Ja	Nee
	4	NATIONAAL	NL Normen en Visie	Richtlijnen Vaarwegen	Ja	Ja
				Beheer- en ontwikkelplan voor de Rijkswateren	Ja	Nee
				Basisvisie Recreatietoervaart	Ja	Nee
	5	PROVINCIAAL	Noord-Holland	Beleid, Visie	-	
	5	PROVINCIAAL	Utrecht	Beleid, Visie	-	
	5	PROVINCIAAL	Flevoland	Beleid, Visie	-	
	6	LOKAAL	Almere	Beleid, Visie	-	
	6	LOKAAL	Den Haag	Beleid, Visie	-	
	6	LOKAAL	Rotterdam	Beleid, Visie	-	
	7	OVERIG		AILA VTS in Inland Waters	Ja	Ja
				RIS Guidelines	Ja	Ja
	7	OVERIG		Zie thema veilige objecten voor LBS, NEN6787 etc.		

Crosscheck Veiligheidsthema's - Domein
21-12-2017



					Status		
SOORT VEILIGHEID	Id		Gebied	Soort	Document	Verwerkt	Bevindingen Ja/Nee
EXTERNE VEILIGHEID	1	EUROPEES		EU RICHTLIJN	-		
	2	NATIONAAL		NL WET	Wet ruimtelijke ordening	Ja	Nee
	2	NATIONAAL		NL WET	Wet Veiligheidsregio's	Ja	Ja
	2	NATIONAAL		NL WET	Wet vervoer gevaarlijke stoffen	Ja	Ja
	2	NATIONAAL		NL WET	Wet Milieubeheer	Ja	Nee
	3	NATIONAAL		NL BESLUIT REGELINGEN	Besluit externe veiligheid transport	Ja	Nee
	3	NATIONAAL		NL BESLUIT REGELINGEN	Besluit vervoer gevaarlijke stoffen	Ja	Nee
	3	NATIONAAL		NL BESLUIT REGELINGEN	Regeling Basisnet	Ja	Nee
	3	NATIONAAL		NL BESLUIT REGELINGEN	Regelingen vervoer gevaarlijke stoffen (land, spoor, binnenwater)	Ja	Nee
	4	NATIONAAL		NL Normen en Visie	-		
	5	PROVINCIAAL	Noord-Holland	Beleid, Visie	-		
	5	PROVINCIAAL	Utrecht	Beleid, Visie	-		
	5	PROVINCIAAL	Flevoland	Beleid, Visie	-		
	6	LOKAAL	Almere	Beleid, Visie	-		
	6	LOKAAL	Den Haag	Beleid, Visie	-		
	6	LOKAAL	Rotterdam	Beleid, Visie	-		
	7	Overig			-		

Crosscheck Veiligheidsthema's - Domein
21-12-2017



SOORT VEILIGHEID	Id Gebied			Soort	Document	Status	
						Verwerkt	Bevindingen Ja/Nee
VEILIGHEID BEWEEGBARE OBJECTEN	1	EUROPEES		EU RICHTLIJN	Machinerichtlijn	Ja	Ja
	2	NATIONAAL		NL WET	-		
	3	NATIONAAL		NL BESLUIT REGELINGEN	Warenwetbesluit Machines	Ja	Nee
	4	NATIONAAL		NL Normen en Visie	NEN-EN-ISO 12100	Ja	Nee
					NPR-ISO_TR 14121-2	Ja	Nee
					NEN-EN-IEC 60204-1	Ja	Ja
					NEN-EN-IEC 62061	Ja	Ja
					NEN-EN-ISO 13849-1	Ja	Ja
					NEN-EN-ISO 13849-2	Ja	Nee
					NEN-EN-ISO 13850	Ja	Ja
					NEN 6786	Ja	Ja
					NEN 6787	Ja	Ja
					NEN-EN-IEC 61508-1 - 2010 en	Ja	JA
					NEN-EN-IEC 61508-2 - 2010 en	Ja	Nee
					NEN-EN-IEC 61508-3 - 2010 en	Ja	Nee
					NEN-EN-IEC 61508-4- 2010 en	Ja	Nee
					NEN-EN-IEC 61508-5 - 2010 en	Ja	Nee
					NEN-EN-IEC 61508-6 - 2010 en	Ja	Nee
					NEN-EN-IEC 61508-7 - 2010 en	Ja	Nee
					LBS - Gebruikershandleiding Natte Beweegbare Objecten	Ja	Ja
					LBS - Procedure Veiligheidsfuncties	Ja	Nee
					LBS - Veiligheidsfuncties	Ja	Ja
					LBS - Faaldefinities	Ja	Ja
					LBS - Basisbeschrijving	Ja	Ja
					LBS Bedienplek nautische Objecten	Ja	Ja
					LBS Noodbediening	Ja	Ja
	5	PROVINCIAAL	Noord-Holland	Beleid, Visie	-		
	5	PROVINCIAAL	Utrecht	Beleid, Visie	-		
	5	PROVINCIAAL	Flevoland	Beleid, Visie	-		
	6	LOKAAL	Almere	Beleid, Visie	-		
	6	LOKAAL	Den Haag	Beleid, Visie	-		
	6	LOKAAL	Rotterdam	Beleid, Visie	-		
	7	OVERIG					

Crosscheck Veiligheidsthema's - Domein
21-12-2017



SOORT VEILIGHEID	Id Gebied		Soort	Document	Status	
					Verwerkt	Bevindingen Ja/Nee
TUNNELVEILIGHEID	1	EUROPEES	EU RICHTLIJN	Minimumveiligheidseisen Tunnels	Ja	Ja
	2	NATIONAAL	NL WET	WARVW	Ja	Ja
	3	NATIONAAL	NL BESLUIT REGELINGEN	RARVW	Ja	Ja
				Bouwbesluit	Ja	Ja
	4	NATIONAAL	NL Normen en Visie	LTS - Beheer&Organisatie Suite	n.v.t.	n.v.t.
				LTS - Juridische Suite	n.v.t.	n.v.t.
				LTS - Technische Suite	n.v.t.	n.v.t.
				Hoogtemelding tunnels NL_tcm21-98491	Ja	Nee
				Webversie brochure Tunnels_juli2016_tcm21-92165	Ja	Nee
				Webversie brochure Tunnels_juli2016_tcm21-92165	Ja	Nee
	5	PROVINCIAAL	Noord-Holland	Beleid, Visie	-	
	5	PROVINCIAAL	Utrecht	Beleid, Visie	-	
	5	PROVINCIAAL	Flevoland	Beleid, Visie	-	
	6	LOKAAL	Almere	Beleid, Visie	-	
	6	LOKAAL	Den Haag	Beleid, Visie	-	
	6	LOKAAL	Rotterdam	Beleid, Visie	-	
	7	OVERIG		-		

Crosscheck Veiligheidsthema's - Domein
21-12-2017



SOORT VEILIGHEID	Id Gebied		Soort	Document	Status	
					Verwerkt	Bevindingen Ja/Nee
INTEGRALE BEVEILIGING	1	EUROPEES		EU RICHTLIJN	Beveiliging Netwerk- en Informatiesystemen	Ja Nee
					Bescherming Persoonsgegevens	
	2	NATIONAAL		NL WET	Telecommunicatiewet	Ja Nee
					Wet bescherming persoonsgegevens	Ja Ja
	3	NATIONAAL		NL BESLUIT REGELINGEN	Beleidsregels cameratoezicht	Ja Ja
	4	NATIONAAL		NL Normen en Visie	NEN-EN-ISO_IEC 27001	Zie normen zelf. Op Dynniq Intranet staat versie uit 2013. Norm 27002 is niet
					NEN-EN-ISO_IEC 27002	
					BIR - Operationele Handreiking	
					BIR - E xplainprocedure	
					BIR - Quicksan	
					RWS - Cybersecurity Richtlijnen	
					RWS - Cybersecurity Implementatierichtlijn Objecten	
					NCSC - Virtualiseer met verstand	
					NCSC - Handreiking implementatie detectie-oplossingen	
					NCSC - ICT-Beveiligingsrichtlijnen voor Webapplicaties (3x)	
					NCSC - ICS_SCADA- en gebouwbeheersystemen online	
					Toetsmodel Privacy Impact Assessment (PIA) Rijksdienst	
	5	PROVINCIAAL	Noord-Holland	Beleid, Visie	Cybersecurity Implementatierichtlijn	
					Cybersecurity Richtlijnen	
	5	PROVINCIAAL	Utrecht	Beleid, Visie	-	
	5	PROVINCIAAL	Flevoland	Beleid, Visie	-	
	6	LOKAAL	Almere	Beleid, Visie	-	
	6	LOKAAL	Den Haag	Beleid, Visie	-	
	6	LOKAAL	Rotterdam	Beleid, Visie	-	
	7	OVERIG			-	

14.2 Bevindingen per veiligheidsthema

ARBEIDSVEILIGHEID

ARBEIDSVEILIGHEID

ARBEIDSVEILIGHEID

NAUTISCHE VEILIGHEID

NAUTISCHE VEILIGHEID

NAUTISCHE VEILIGHEID

NAUTISCHE VEILIGHEID

$\frac{1}{2}$

EXTERNE VEILIGHEID

VEILIGHEID BEWEEGBARE OBJECTEN

VEILIGHEID BEWEEGBARE OBJECTEN

VEILIGHEID BEWEEGBARE OBJECTEN

VEILIGHEID BEWEEGBARE OBJECTEN

VEILIGHEID BEWEEGBARE OBJECTEN

VEILIGHEID BEWEEGBARE OBJECTEN

TUNNELVEILIGHEID

TUNNELVEILIGHEID

4/10

TUNNELVEILIGHEID

TUNNELVEILIGHEID

TUNNELVEILIGHEID

TUNNELVEILIGHEID

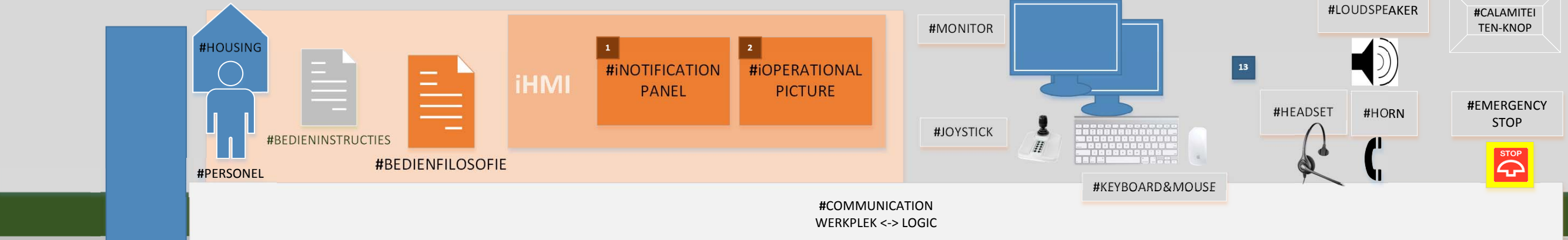
INTEGRALE BEVEILIGING

INTEGRALE BEVEILIGING

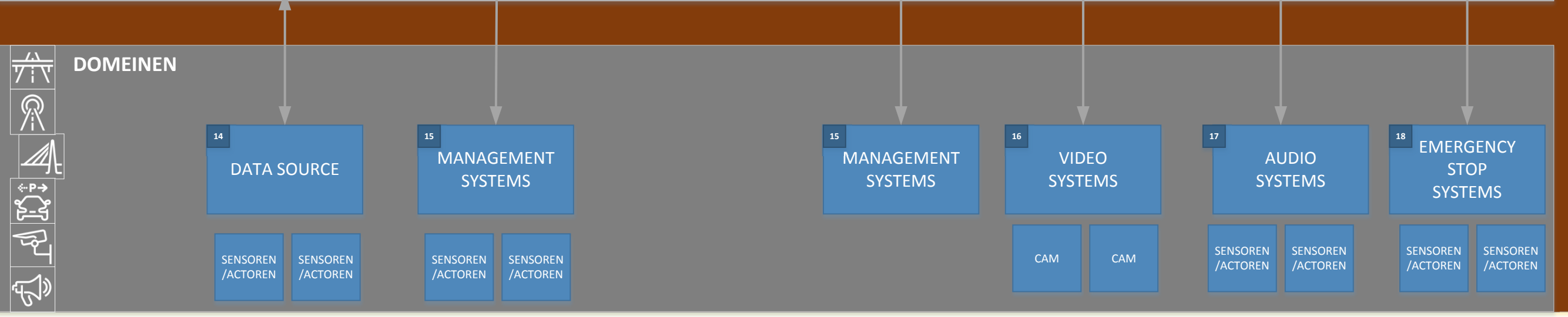
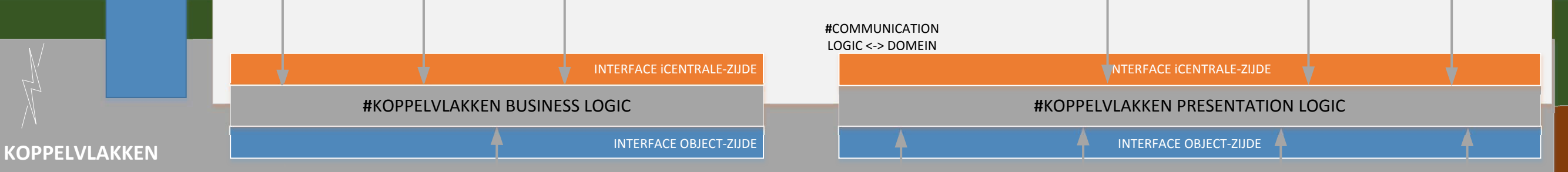
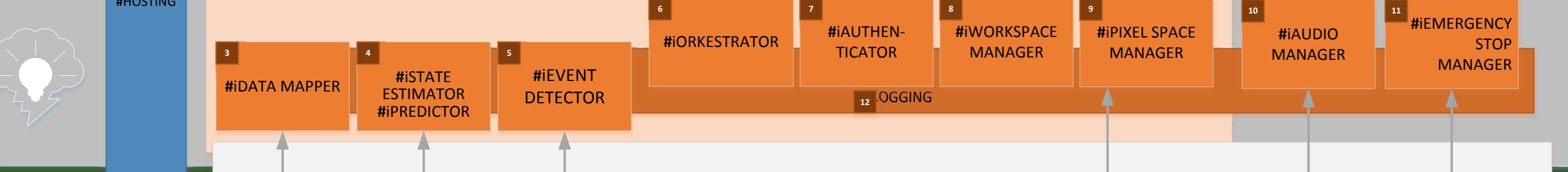
14.3 Configuratie-items veiligheid

SCOPE

DISPLAY AND USER INTERFACE



BUSINESS LOGIC



OUT OF SCOPE

LEGENDA									



Gemeente Almere



Den Haag

