



Rijkswaterstaat
Ministerie van Infrastructuur en Milieu

RWS ONGECLASSIFICEERD

Generiek Programma van Eisen Fysieke Beveiliging

Wegen- en Watersteunpunten en monumentale Vuurtorens

Datum	8 februari 2022
Status	Definitief
Versienummer	1.0

Colofon

Uitgegeven door	Rijkswaterstaat Corporate Dienst
Informatie	Afdeling Facility Management; team Safety & Security
Uitgevoerd door	Facility Management in samenwerking met Vastgoed Management, SLA managers en CIV
Datum	8 februari 2022
Status	Definitief
Versienummer	1.0

Wijzigingenoverzicht

Datum	Versie	Wijziging
Oktober 2021	0.1	Concept document - stakeholders
November 2021	0.2	Concept – MT
December 2021	0.3	Concept - DT
Februari 2022	1.0	Definitief

Afkortingenlijst

Afkorting	Betekenis
AT	Alarmtransmissie
B&O	Beheer en Onderhoud RWS-CD
BIO	Baseline Informatiebeveiliging Overheid
BK	Bouwkundig / Braakwerend
BSN	Basis Security Niveau
CBD	Code Bedien Deel
CCS	Centrale Controle- en Stuureenheid
CCV	Centrum van Criminaliteitspreventie & Veiligheid
CD	Corporate Dienst
CIV	Centrale Informatievoorziening
CO	Compartiment
CSIR	Cyber Security Implementatie Richtlijn
DC	deurcontroller
DFF	Directeur Facilitair en Financiën RWS-CD
DOS	Dicht- en Opslotsignalering
DS	Dicht-Signaleringen
DSM	Dubbelstaafsmat-hekwerk
EL	Elektronisch
GPvE	Generiek Programma van Eisen
HBS	Handboek Security RWS
HVWN	Hoofdvaarwegennet
HWN	Hoofdwegennetwerk
HWS	Hoofdwatersystemen
ISS	Indringer Signaleringssysteem
KNRM	reddingsbrigade
ME	Meeneembeperkende
NDO	Nood Deur Opener
NVR	Netwerk videorecorder
RBK	RWS-CD Beveiligingsklasse
RBKI	RWS BeveiligingsKlasseIndeling
RBO	RijksBeveiligingsOrganisatie
RE	Reactie
RWS	Rijkswaterstaat
SMS	Security Management Systeem
SN	Security Netwerk
STUVER	STUrende en VERtragende beplanting
T	Terrein
TCS	Toegangscontrolesysteem
TzC	ToezichtCentrale
VCA	Video Content Analyse
VMD	Video Motion Detectie
VRKI	Verbeterde Risicoklassen Indeling
VSS	Video Surveillance Systeem
VWM	Verkeer- en Watermanagement

Inhoud

Afkortingenlijst	3
1 Inleiding	1
1.1 Voorwoord	1
1.2 Aanleiding	1
1.3 Doelstelling Generiek Programma van Eisen	1
1.4 Scope	1
1.5 Leeswijzer	1
2 Rijkswaterstaat	2
2.1 Organisatie	2
2.2 Missie	2
2.3 Vastgoed Corporate Dienst	2
2.4 Algemene beschrijving Objecten	2
2.5 Externe gebruikers	3
3 Het beveiligingssysteem	4
3.1 Inleiding	4
3.2 Algemeen	4
3.3 Beveiligingsconcept CD-Objecten	4
4 Beveiligingsconcept wegen- en watersteunpunten	5
4.1 Algemeen	5
4.2 Terreinbeveiliging	5
4.3 Gebouwbeveiliging steunpunten	6
5 Beveiligingsconcept vuurtorens	8
6 Toegangsverlening	9
6.1 Autorisaties	9
6.2 Toegangsverleningsconcept	9
6.3 Alarmopvolging	10
7 Terreinbeveiliging (T)	12
7.1 T1	12
7.2 T2	13
7.3 Verlichting	14
8 Bouwkundige maatregelen (BK)	15
8.1 BK1	15
8.2 BK2	15
8.3 BK3	15
9 Compartimenterende maatregelen (CO)	16
9.1 CO2	16
9.2 CO3	16
10 Meeneembeperkende maatregelen (ME)	17
10.1 ME2	17
10.2 ME3	17
11 Specificaties Toegangscontrolesysteem (TCS)	18
11.1 Algemeen	18
11.2 Systeemconfiguratie	18
12 Het Indringer Signaleringsysteem (ISS)	23
12.1 Algemeen	23
12.2 Beveiligingsmodi	23
12.3 Alarmmeldingen	24

12.4	Toegankelijkheid tot de CCS-en	24
12.5	Systeemconfiguratie	25
13	Specificaties (Video) Intercomsystemen	31
13.1	Algemeen	31
13.2	Uitvoering	31
14	Specificaties Video Surveillance Systemen (VSS-en)	33
14.1	VSS1	33
14.2	VSS2	33
14.3	Systeemconfiguratie	34
15	ToezichtCentrale (TzC)	38
16	Het Security Netwerk (SN)	39
16.1	Algemeen	39
17	Het Security Management Systeem (SMS)	39
17.1	Algemeen	39
18	Overige specificaties	40
18.1	De voedingsspanningsvoorziening	40
Bijlage 1	RWS-CD RBKI	41
Bijlage 2	RBK Tabel – Specifieke objecten	43
Bijlage 3	Stuver-soorten	44

DEEL 1 ALGEMEEN

1 Inleiding

1.1 Voorwoord

Dit document bevat het Programma van Eisen voor de fysieke beveiliging van Wegen- en Watersteunpunten en monumentale Vuurtorens in beheer van Rijkswaterstaat Corporate Dienst.

1.2 Aanleiding

Voor de RWS CD-Objecten Water- en Wegensteunpunten en monumentale Vuurtorens (hierna CD-Objecten) is een uniforme Richtlijn Fysieke Beveiliging opgesteld (feb 2022). Deze beschrijft waarom voor deze CD-Objecten een richtlijn aanvullend op de geldende RWS richtlijnen voor de Fysieke Beveiliging is opgesteld, inclusief de te beschermen belangen en hoe er beleidsmatig vanuit RWS CD met de fysieke beveiliging wordt omgegaan.

Naast de Richtlijn beschrijft het Kader Fysieke Beveiliging (feb 2022) welke organisatorische-, bouwkundige- en elektronische beveiligingsmaatregelen getroffen moeten worden om de beveiliging te optimaliseren. Hierbij is gebruik gemaakt van een voor RWS specifiek aangepaste VRKI (Verbeterde Risicoklassen Indeling), de zogenaamde RBKI (RWS Beveiligingsklassen Indeling). De RBKI staat weergegeven in Bijlage 1 RWS-CD RBKI.

Aanvullend op de Richtlijn en het Kader beschrijft voorliggend document, het Generieke Programma van Eisen (GPvE), de functionele eisen en de technische specificaties van de bouwkundige en elektronische beveiligingsmaatregelen voor deze CD-Objecten.

1.3 Doelstelling Generiek Programma van Eisen

Het doel van het GPvE is het borgen van standaardisatie en uniformiteit voor de eisen en specificaties met betrekking tot de Fysieke Beveiliging voor de CD-Objecten. Dit document dient zowel voor intern als extern gebruik en voor zowel bestaande bouw als voor nieuwbouw.

1.4 Scope

De objecten zijn in beheer van de CD en liggen verspreid over heel Nederland. Het GPvE is in principe van toepassing op alle huidige objecten en alle nieuw te realiseren objecten van de CD.

De scope van de fysieke beveiliging omvat de beveiligingsmaatregelen uit het RBKI. Daar waar van toepassing, zal ook aandacht worden besteed aan de fysieke beveiliging van ICT-middelen en systemen en worden maatregelen benoemd voor het verkrijgen van een veilige werkomgeving. Ook de samenhang met de ToezichtCentrale (TzC) wordt meegenomen. Wat betreft de elektronische beveiligingsmaatregelen zitten de volgende systemen in de scope:

- a. ToegangsControlesystemen (TCS-en),
- b. Inbraaksignaleringssystemen (ISS-en),
- c. Video Surveillance Systemen (VSS-en),
- d. Intercomsystemen (IS-en).

De alarmtransmissie (AT) en reactie (RE) zijn niet gespecificeerd in dit GPvE. Voor de AT wordt verwezen naar de vigerende versie VRKI. De RE wordt verzorgd door de RijksBeveiligings-Organisatie (RBO). De in de VRKI beschreven reactie is daarbij het uitgangspunt, echter RWS is afhankelijk van hoe de RBO de reactie heeft georganiseerd.

Er mag niet van dit PvE worden afgeweken. Uitsluitend daar waar specifieke eisen gelden, mag aan de hand van dit PvE in overleg middels een 'Explain' worden afgeweken. Deze Explain dient te worden voorgelegd en geaccordeerd te zijn door de Directeur Facilitair en Financiën RWS-CD (DFF).

1.5 Leeswijzer

In het eerste deel van dit PvE is na de inleiding een beschrijving opgenomen van de Objecten van RWS-CD. In hoofdstuk 3 tot en met 5 wordt het beveiligingsconcept toegelicht. Hoofdstuk 6 omschrijft het toegangsconcept. Vervolgens staan in Deel 2 de technische specificaties van alle te nemen maatregelen.

2 Rijkswaterstaat

2.1 Organisatie

Rijkswaterstaat is de beheerder van het Hoofdwegennetwerk (HWN), het Hoofdvaarwegennet (HVWN) en het Hoofdwatersystemen (HWS). Rijkswaterstaat werkt aan de vlotte en veilige doorstroming van het verkeer, aan een veilig, schoon en gebruikersgericht landelijk watersysteem en aan de bescherming van ons land tegen overstromingen.

Op de genoemde gebieden ontwikkelt Rijkswaterstaat de benodigde kennis en expertise en levert zij voor het publiek betrouwbare en bruikbare informatie. Rijkswaterstaat werkt daarbij steeds intensiever samen met andere netwerkbeheerders. Vooral in drukke, grootstedelijke gebieden, maar ook in internationaal verband.

2.2 Missie

Rijkswaterstaat is de uitvoeringsorganisatie van het ministerie van Infrastructuur en Waterstaat. We beheren en ontwikkelen de rijkswegen, -vaarwegen en -wateren en zetten in op een duurzame leefomgeving.

Samen met anderen werken we aan een land dat beschermd is tegen overstromingen. Waar voldoende groen is en voldoende en schoon water. En waar je vlot en veilig van A naar B kunt. Dat doen we onder andere door het garanderen van de beschikbaarheid van het wegennet door gladheidbestrijding en incidentmanagement.

Samenwerken aan een veilig, leefbaar en bereikbaar Nederland. Dat is Rijkswaterstaat.

2.3 Vastgoed Corporate Dienst

Rijkswaterstaat Corporate Dienst (CD) is verantwoordelijk voor het beheer van gebouwen met een regio overstijgende functie en bijbehorende gebouw gebonden terreinen. De regio's zijn verantwoordelijk voor Primaire proces locaties, zoals sluizen, bruggen, stormvloedkeringen met een lokale functie (o.a. bediening sluizen en bruggen, meetstations). De governance is vastgelegd in het sturingsmodel gebouwen.

Binnen de vastgoedportefeuille van de CD vallen de Verkeerscentrales, Wegensteunpunten, Watersteunpunten, Districts- en dienstkantoren, monumentale Vuurtorens en voormalige dienstwoningen.

Voorliggend GPvE is van toepassing op de Wegensteunpunten, Watersteunpunten en monumentale Vuurtorens (hierna: CD-Objecten). Bij de vuurtorens bestaat het object enkel uit de vuurtoren zelf en eventueel het omliggende terrein. Bij de Wegen- en Watersteunpunten betreft het object het terrein en de daarop aanwezige objecten, zoals het steunpunt zelf, maar ook bijvoorbeeld loodsen en overkappingen.

2.4 Algemene beschrijving Objecten

2.4.1 Wegensteunpunten

RWS heeft 56 wegensteunpunten, deze zijn gesitueerd langs de wegen (droge steunpunten). De CD is beheerder van deze wegensteunpunten en verantwoordelijk voor het onderhoud. De hoofdgebruiker van de wegensteunpunten is VWM. Zij gebruiken het o.a. voor de processen met betrekking tot de wegininspecteurs, gladheidbestrijding, incidentmanagement, handhaving en meetdiensten. Daarnaast maken derden (zoals provincie, gemeente, ANWB, ILT en andere) steeds meer gebruik van deze steunpunten.

2.4.2 Watersteunpunten

RWS heeft 77 watersteunpunten, deze zijn gesitueerd langs het water (natte steunpunten). De CD is beheerder van deze watersteunpunten en verantwoordelijk voor het onderhoud. De hoofdgebruikers van de watersteunpunten zijn VWM, Rijksrederij, Handhaving, CIV, regio en derden (o.a. politie, douane). Zij gebruiken het onder andere voor de processen met betrekking tot nautisch personeel, vaarwegmarkering, meet- en informatiedienst, incident management (oliebestrijding) en patrouillevaartuigen. De scope van de Fysieke Beveiliging heeft betrekking op

de watersteunpunten zelf, niet op de (Rijksrederij)schepen welke afmeren bij een aantal van de watersteunpunten.

2.4.3 Monumentale Vuurtorens

RWS heeft 18 rijks monumentale Vuurtorens. De CD is beheerder van deze vuurtorens en verantwoordelijk voor het onderhoud. De hoofdgebruikers van de vuurtorens zijn heel divers, dit betreffen o.a. Rijksoverheidsorganisaties zoals RWS, politie, defensie, kustwacht en derden zoals reddingsbrigade (KNRM), telecomproviders, etc. Zij gebruiken het onder andere voor de processen met betrekking tot nautische verkeerscentrale, nautische verkeerspost, openstelling bezoekers, radarinstallaties, vaarwegmarkering, positiebepaling systemen, etc. Er zijn twee vuurtorens die op basis van hun cybersecurityniveau extra moeten worden beveiligd. Deze locaties betreffen Vuurtoren Schiermonnikoog en Vuurtoren Terschelling (Brandaris).

2.5 Externe gebruikers

De beheerder en hoofdgebruiker van de CD-Objecten is RWS. Het komt voor dat CD-Objecten in afstemming ook gebruikt worden door externe gebruikers. In dit geval zullen de gebouwdelen van de verschillende gebruikers, waar nodig, afzonderlijk afsluitbaar zijn met behulp van een Rijkspas.

3 Het beveiligingssysteem

3.1 Inleiding

RWS-CD heeft behoefte aan een integraal beveiligingssysteem voor de Wegen- en Watersteunpunten en monumentale Vuurtorens (CD-Objecten). Dit beveiligingssysteem dient zoveel mogelijk schade door een onbevoegde beïnvloeding te voorkomen aan mensen, onze processen, onze middelen en onze vertrouwelijke informatie. Hiertoe is een gecontroleerde toegangsverlening, een vroegtijdige detectie en een zo snel mogelijke alarmmelding benodigd.

3.2 Algemeen

3.2.1 *Eén Security Richtlijn ('de Richtlijn'), één integraal beveiligingssysteem*

Voor de CD-Objecten wordt één Security Richtlijn gehanteerd. Dit betekent onder andere dat alle beveiligingsmaatregelen en -procedures voor de steunpunten op dezelfde wijze worden uitgevoerd.

Verder is binnen RWS één universeel geïntegreerd beveiligingssysteem in gebruik dat op elke locatie op dezelfde wijze werkt. Op elke locatie dient de Rijkspas te kunnen worden gebruikt voor de toegangsverlening. Tenslotte zal op brede schaal worden gestandaardiseerd in de aanschaf van en het onderhoud aan beveiligingscomponenten.

3.2.2 *Beveiligingsniveaus CD-Objecten*

Voor deze CD-Objecten worden verschillende beveiligingsniveaus gehanteerd. De objecten zijn geclassificeerd middels een sterrensystematiek, waarbij een object 1, 2 of 3 sterren kan hebben. Het aantal sterren bepaalt welke functionele voorzieningen er aanwezig zijn. De sterrensystematiek is in het Kader opgenomen als onderdeel ter bepaling van het Basis Security Niveau (BSN) en daarmee van de RWS-CD Beveiligingsklasse (RBK) voor CD-Objecten. Afhankelijk van de RBK kan een combinatie van beveiligingsmaatregelen worden toegepast. De RWS-CD Beveiligingsklassen Indeling (RBKI) is te vinden in het Kader en in Bijlage 1 RWS-CD RBKI. De RBKI is afgeleid en in lijn met de VRKI 2.0. Tevens kan voor de fysieke beveiliging van specifieke ruimten en toepassingen, een afwijkende RBK classificering gelden, zie hiervoor Bijlage 2 RBK Tabel – Specifieke objecten

Het beveiligingsconcept is op hoofdlijnen voor de CD-Objecten gelijk. Afhankelijk van het beveiligingsniveau worden specifieke eisen aan de beveiligingsmaatregelen gesteld. Het GPvE beschrijft alle beveiligingsmaatregelen uit Bijlage 1 RWS-CD RBKI.

3.2.3 *Uitgangspunten en randvoorwaarden*

De algemene uitgangspunten van het fysieke beveiligingsconcept zijn:

- **Detectie en alarmverificatie.** *Er wordt gestreefd naar een effectieve detectie van indringers en een effectieve verificatie van alarmen door middel van meervoudige detectiepunten en in sommige gevallen camera's ter verificatie.*
- **Omvang van de beveiligingsmaatregelen.** *De omvang van de te nemen beveiligingsmaatregelen wordt bepaald aan de hand van de RWS Beveiligingsklassenindeling (RBKI).*

Aan de realisatie van de fysieke beveiliging worden de volgende randvoorwaarden gesteld:

- Er moet zoveel mogelijk gebruik worden gemaakt van bestaande systemen en materialen.
- Bij de implementatie van de elektronische systemen dient te worden gewaakt voor overdaad en te complexe oplossingen.
- De gebruikte systemen en materialen moeten gebruiksvriendelijk zijn en robuust zijn uitgevoerd.

3.3 Beveiligingsconcept CD-Objecten

Het beveiligingsconcept voor de wegen- en watersteunpunten is gelijk. Het concept wordt in hoofdstuk 0 toegelicht. Het beveiligingsconcept voor de vuurtorens wordt in hoofdstuk 5 toegelicht. De technische specificaties worden in hoofdstukken daarna besproken.

4 Beveiligingsconcept wegen- en watersteunpunten

4.1 Algemeen

Het beveiligingsconcept is op hoofdlijnen gelijk voor de wegensteunpunten en de watersteunpunten. Er is onderscheidt tussen terreinbeveiliging en gebouwbeveiliging. Binnen de gebouwbeveiliging is onderscheidt tussen verschillende type gebouwen en gecompartmenteerde ruimtes. De hoofdlijnen van het concept worden hieronder toegelicht. De technische specificaties worden in afzonderlijke hoofdstukken nader toegelicht, waarbij afhankelijk van de beveiligingsklasse verschillende technische criteria worden gesteld.

In de omschrijving wordt verwezen naar de beveiligingsmaatregelen zoals weergegeven in de RBKI tabel uit Bijlage 1 RWS-CD RBKI.

Aandachtspunt: het concept geeft niet de huidige, maar de gewenste eindsituatie weer.

4.2 Terreinbeveiliging

4.2.1 Terreinafscherming

De terreinen van de steunpunten dienen met een fysieke barrière van de buitenwereld te worden afgescheiden. Deze barrière functioneert tevens als juridische terreinafscherming. Afhankelijk van de beschikbare ruimte kan worden gekozen uit muren, hekwerken, natuurlijke barrières en/of combinaties hiervan (T1, T2). Het verdient de voorkeur om gebruik te maken van natuurlijke barrières, zoals sloten, en/of terreinverhogingen (taluds) in combinatie met sturende en vertragende beplanting (Stuver, zie Bijlage 3 Stuver-soorten).

Daar waar geen terreinafscherming mogelijk is, zoals aan de waterkant waar boten kunnen aanmeren, dienen 'virtuele hekwerken' met behulp van camera's te worden toegepast. Ook dienen virtuele hekwerken te worden toegepast langs buitenopstelplaatsen van waardevolle goederen (zoals vaarwegmarkering) en bepaalde vervoermiddelen (zoals sneeuwschuivers en zoutstrooiers). De virtuele hekwerken zijn alleen actief als er geen personeel op het steunpunt aanwezig is.

Het Video Surveillance Systeem (VVS2) dient zódanig te worden aangebracht dat men vanuit de TzC een overzicht krijgt van de situatie langs de niet-afgeschermd terreingrenzen en bepaalde opstelplaatsen. Hiertoe dienen geschikte camera's op hoge masten te worden geplaatst. In de masten dient infraroodverlichting te worden aangebracht, waarmee het mogelijk wordt om ook 's nachts met de camera's op het terrein te kunnen kijken.

De camera's moeten van 'Videomotiondetectie (VMD)' worden voorzien. Detectiemeldingen van het VMD moeten naar de TzC worden gestuurd, de overzichtsbeelden moeten door de centralisten in de TzC kunnen worden bekeken.

Daar waar geen terreinafscherming mogelijk is, zoals bij gebouwen die direct aan de straatzijde grenzen, gelden de beveiligingsmaatregelen gespecificeerd voor gebouwen.

4.2.2 Toegangspoort

Voor een gecontroleerde afscherming van het terrein dient één elektrisch bedienbare toegangsschuifpoort in de terreinafscherming te zijn aangebracht. Zowel aan de buitenzijde als binnenzijde van het terrein dient links naast de oprit/afrit een buitenzuil, dan wel binnenzuil, te worden aangebracht voor toegangsverlening door de poort. De inrichting op de zuilen wordt dubbel uitgevoerd, zowel op hoogte voor automobilisten, als op hoogte voor vrachtwagenchauffeurs.

Toegangsverlening vindt primair plaats middels het aanbieden van een Rijkspas aan een Rijkspas lezer op de buitenzuil. Een booster kan gebruikt worden om het hek vanaf een afstand met de Rijkspas te openen. Toegangsverlening vindt secundair plaats middels een intercomverbinding via een intercompost met geïntegreerde camera op de buitenzuil. De spreek-luister- en videoverbinding is gekoppeld aan de TzC en, indien van toepassing, met een bedienunit (met drukknop) in het steunpunt, zodat een medewerker/centralist van afstand de poort kan openen.

Om het terrein te verlaten zitten op de binnenzuil twee rode grote drukknoppen op voldoende afstand van de poort (zodat deze niet vanaf buiten het hek, kan worden gemanipuleerd) van het

water- en wegensteunpunt. In specifieke gevallen kan er worden afgeweken van de buitenzuil, bijvoorbeeld door de ligging en ruimtelijke indeling van het terrein. De poort kan na een telefonische melding ook op afstand worden geopend door een centralist (als de drukknoppen niet werken). Hiertoe dient bordje met het telefoonnummer van de TzC op de zuil te worden geplaatst. Ook dient indien nodig een calamiteitendrukknop te worden geplaatst op een logistiek logische locatie in het hoofdgebouw van het Wegensteunpunt, waarmee de poort voor één voertuig kan worden geopend.

Ter hoogte van beide zuilen dient een detectielus in het wegdek te worden aangebracht: de inrijdlus en uitrijdlus. Als om het openen van de poort wordt gevraagd, detecteren de lussen of het wel of niet om een voertuig gaat (lusdetector kan afgesteld worden op massa metaal). Bij een voertuig opent de poort in zijn geheel en anders over een afstand van slechts 100 cm. Dit om voetgangers en fietsers door te laten. Om onbevoegde beïnvloeding te voorkomen, dient de uitrijdlus bij voorkeur op tenminste 10 meter vanaf de poort te liggen

De uitrijdlus maakt het ook mogelijk om de poort automatisch te openen als er een auto of een motorfiets op staat. Vanuit de TzC kan hier ook een tijdsperiode voor ingesteld worden, bv tijdens gladheidsbestrijding.

Voor het Video Surveillance Systeem (VSS1) dient er een camera in een cameramast worden aangebracht waarmee in de TzC en indien van toepassing op een bedienunit op het terrein een overzicht kan worden verkregen van de situatie bij de poort. In de mast dient infraroodverlichting te worden aangebracht waarmee het mogelijk wordt om ook 's nachts met de camera naar de poort te kunnen kijken.

4.2.3 Verlichting

Ten slotte dient er een verlichtingssysteem op het terrein te worden aangebracht langs de wegen en bij de parkeerplaatsen. Het systeem moet werken tijdens schemer en in nachtelijke uren, onder speciale omstandigheden.

4.3 Gebouwbeveiliging steunpunten

4.3.1 Algemeen

In dit hoofdstuk wordt allereerst een aantal algemene uitgangspunten beschreven voor de beveiliging van de gebouwen op steunpunten. Vervolgens staan per type ruimte de te nemen fysieke beveiligingsmaatregelen benoemd.

Op de terreinen kunnen de volgende elementen en componenten voorkomen:

- Eén hoofdgebouw;
- Overige gebouwen;
- Werkplaatsen en interne garages;
- Overkappingen.

Daarnaast kan de aanwezigheid van specifieke apparatuur of installaties een aparte RBK classificering vereisen voor een compartiment, zie hiervoor Bijlage 2 RBK Tabel – Specifieke objecten.

4.3.2 Het hoofdgebouw en overige gebouwen

Het hoofdgebouw en de overige gebouwen hebben één hoofdentree deur. Uitsluitend elektronisch met een valide Rijkspas kan deze worden ontgrendeld. Achter de deur bevindt zich het Code Bedien Deel (CBD) met daarnaast een (specifiek gekenmerkte) Rijkspaslezer waarmee het InbraakSignaleringsSysteem (ISS) in het gebouw geheel of gedeeltelijk met behulp van valide Rijkspas kan worden in- of uitgeschakeld.

Aan de buitenzijde van het hoofdgebouw naast de hoofdentree deur dient een sleutelkluis te worden gemonteerd, inclusief bordje met het telefoonnummer van de TzC. De sleutelkluis kan vanuit de TzC en door een toegewezen Rijkspas geopend worden. Sleuteluitname wordt toegekend door en geregistreerd in TCS.

Indien er geen terreinafscheiding is, dient de sleutelkluis inpandig te worden geplaatst. In dit geval wordt naast de hoofdentree deur een camera-intercompost geplaatst, voor een spreek-luisterverbinding met een medewerker in het gebouw of met een centralist in de TzC om zo de deur vanuit de TzC te ontgrendelen.

De buitenkant van gebouwen dient een braakwerendheid (BK) te bieden conform de keuze van de combinatie van beveiligingsmaatregelen conform RBKI.

4.3.3 De bereikbare ruimten

De ruimten die bereikbaar zijn conform NEN 5087 moeten worden beveiligd conform de RBKI.

Bouwkundige maatregelen.

Deuren, niet zijnde hoofdentree- of entreedeuken, in de buitengevel moeten van een mechanisch slot worden voorzien. De deuren dienen te worden voorzien van een anti-panieksluiting waarmee in geval van calamiteiten de ruimte probleemloos kan worden ontlucht. De deuren moeten aan de buitenzijde zijn voorzien van blindbeslag.

Alle elektrisch vergrendelde deuren dienen zelfsluitend te zijn.

Geautoriseerde toegangsverlening

Het is mogelijk om in overleg met de gebruiker gebouwdelen of ruimten te voorzien van toegangscontrolevoorzieningen (o.a. Rijkspaslezer, elektromechanisch slot enz.), om daarmee verschil tussen de toegang door verschillende groepen van geautoriseerden mogelijk te maken.

4.3.4 Compartimenten

Indien in een ruimte een voor de organisatie belangrijk systeem of waardevol goed aanwezig is, zal voor de betreffende ruimte een hogere RBK kunnen gelden, dan van toepassing is voor het terrein of de rest van het gebouw. Voor de betreffende ruimte geldt dan een andere (hogere) combinatie aan beveiligingsmaatregelen.

Specifieke aandacht moet daarbij worden gegeven aan de ICT-ruimten, zijnde MER-ruimten. Hiervoor geldt aanvullend op de RBK, de toepassing van camera observatie in de ruimte, gericht op de toegang van deze ruimte.

4.3.5 Overkappingen

Voor overkappingen gelden geen specifieke beveiligingsmaatregelen, tenzij er specifieke apparatuur of installaties staan conform Bijlage 2 RBK Tabel – Specifieke objecten. In dit geval wordt een virtueel hekwerk middels camera's gecreëerd.

5 Beveiligingsconcept vuurtorens

Bij de beveiliging van de monumentale Vuurtorens dient nadrukkelijk de regelgeving geldend voor rijksmonumenten in acht te worden genomen. Hierbij moet het vereiste niveau van beveiliging worden behaald in lijn met de regelgeving voor rijksmonumenten.

Daar waar vanuit cultuurhistorisch oogpunt geen (nieuw / hoog) hekwerk toegestaan is, blijft de huidige situatie gehandhaafd.

5.1.1 Bouwkundige beveiligingsmaatregelen

Bouwkundige beveiligingsmaatregelen bij monumentale Vuurtorens zullen op basis van maatwerk moeten worden voorbereid. Maatwerk met name in de zin van wat er mag vanuit monumentaal oogpunt en niet maatwerk in de zin van de VRKI.

Bij monumentale Vuurtorens zonder hoge RBK kunnen op basis van BK1 aanwezige maatregelen (bestaand hang- en sluitwerk zonder classificatie van de inbraakwerendheid), worden gehandhaafd.

Daar waar bedrijfskritische processen plaatsvinden, zal op basis van maatwerk moeten worden gezorgd dat BK2 (CO2) wordt behaald bij binnendeuren.

5.1.2 Elektronische beveiligingsmaatregelen

In overleg met de gebruiker wordt er op de monumentale Vuurtorens zonder bedrijfskritische processen, geen aansluiting op de TzC gemaakt. Toegangsverlening zal dan plaatsvinden op basis van (lokale) beheerders en organisatorische afspraken.

6 Toegangsverlening

6.1 Autorisaties

Het is uitsluitend aan daartoe geautoriseerde personen toegestaan om zich op een RWS-terrein of in een RWS-gebouw te bevinden. Het volgende geldt:

- **Geautoriseerde personen** krijgen uitsluitend toegang tot terreinen en gebouwen en/of delen daarvan, waarvoor zij op basis van hun functie-uitoefening moeten zijn. Per situatie kan worden bepaald wie zelfstandig en wie uitsluitend onder begeleiding toegang mag krijgen.
- **Niet-geautoriseerde personen** krijgen uitsluitend toegang onder begeleiding van een geautoriseerde persoon na voorafgaande toestemming van de Locatiemanager.

6.2 Toegangsverleningsconcept

Hieronder staat het concept van de toegangsverlening. De regelgeving m.b.t. toegangsverlening is van toepassing voor zowel interne RWS medewerkers, als geautoriseerde medewerkers van contractpartijen en derden. De volgende situaties zijn denkbaar:

- Het als eerste betreden van een terrein of gebouw;
- Het uitsluitend betreden van een terrein;
- toegangsverlening aan volgende personen;
het als laatste verlaten van een terrein of gebouw.

6.2.1 *Het als eerste betreden van een terrein of gebouw*

Wanneer een geautoriseerde medewerker als eerste een terrein of gebouw wil betreden, is het ISS in alle gebouwen nog ingeschakeld. Geautoriseerde medewerkers kunnen vervolgens:

- Met behulp van hun Rijkspas de elektrisch bediende voertuigpoort openen.
- De hoofdentree deur met behulp van hun Rijkspas openen.
- Als zij als eerste het gebouw betreden, zal het ISS nog zijn ingeschakeld. Zij moeten dan binnen 30 seconden hun Rijkspas aanbieden aan een Rijkspaslezer naast het CBD. Wanneer een valide pas is aangeboden, zal het Inbraak SignaleringsSysteem van het gebouw worden uitgeschakeld. De ISS-en van de overige gebouwen blijven nog steeds ingeschakeld.
- Wanneer vervolgens de medewerker zijn Rijkspas aan een paslezer bij een beveiligde binnendeur aanbiedt, wordt (als hij daartoe geautoriseerd is) de deur ontgrendeld en kan hij de betreffende ruimte betreden. Indien géén valide pas wordt aangeboden, wordt de deur niet ontgrendeld. Een geforceerde toegangsverschaffing (dus zonder het aanbieden van een valide Rijkspas) wordt gedetecteerd en wordt gemeld aan de TzC als een inbraakmelding.

6.2.2 *Het uitsluitend betreden van een terrein*

Wanneer een geautoriseerde medewerker een terrein wil betreden zonder dat hij een gebouw wilt ingaan, kunnen geautoriseerde medewerkers achtereenvolgens:

- Met behulp van hun Rijkspas de elektrisch bediende voertuigpoort openen.
- Indien nodig een sleutel uit de sleutelkluis halen door het openen van de sleutelkluisdeur na het aanbieden van een valide Rijkspas. Ook kan de deur van de sleutelkluis op afstand door de TzC worden ontgrendeld, nadat de medewerker daar telefonisch om heeft gevraagd.
- Na afloop van hun werkzaamheden de sleutel weer terugplaatsen in de kluis, nadat de TzC op verzoek de deur heeft ontgrendeld.

6.2.3 *Toegangsverlening aan volgende personen tot het terrein of gebouw*

Als het ISS van een gebouw is uitgeschakeld, kunnen personen met een valide Rijkspas het gebouw betreden, zonder dat zij het ISS hoeven uit te schakelen.

Geautoriseerde medewerkers kunnen dan:

- Met behulp van hun Rijkspas de elektrisch bediende poort openen. Vervolgens kunnen zij hun pas aanbieden aan een paslezer bij een entree deur of beveiligde binnendeur. Wanneer zij geautoriseerd zijn om toegang te krijgen, wordt de deur ontgrendeld en kan men het betreffende gedeelte betreden. Indien géén valide pas wordt aangeboden, wordt de deur niet ontgrendeld.

6.2.4 *Het als laatste verlaten van een terrein of gebouw*

- Wanneer een medewerker als laatste een terrein verlaat, zal hij achtereenvolgens:
- het gebouw waarin hij zijn werkzaamheden heeft verricht, verlaten. Voordat hij naar buiten loopt, kan hij door het aanbieden van zijn Rijkspas aan de (specifiek gekenmerkte) paslezer naast het CBD naast de entree deur het alarm van het betreffende gebouw (of een sectie van het gebouw met behulp van een genummerde drukknop) inschakelen.

Hij moet op het Code Bedien Deel een overzicht kunnen opvragen van de beveiligingsstatus van alle detectiegroepen in het gebouw. Indien alle groepen in rust zijn, wordt het systeem ingeschakeld. Hierna heeft hij 30 seconden (de zogenaamde uitlooptijd) om het gebouw via de entree deur te verlaten. Indien hij niet binnen de gestelde 30 seconden de deur achter zich heeft afgesloten, dienen de binnensirenes lokaal een luidalarm te genereren en moet een melding worden gegenereerd naar de TzC.

Gedurende de 30 seconden uitlooptijd klinkt er binnen het gebouw een zoemer. Zodra deze ophoudt met zoemen, worden de magneetcontacten op de buitendeuren van het gebouw geactiveerd.

- Naar het hoofdgebouw gaan om daar de eventueel gebruikte sleutels in de sleutelkuis aan de buitenzijde naast de hoofdentree deur op te bergen.
- Een elektrisch bediende poort openen door het indrukken van een drukknop op de binnenzijde bij de toegangspoort.
- De poort dient, vanuit de uitrijdzijde gezien, bij voorkeur van rechts naar links open te schuiven over een lengte die niet verder gaat dan de breedte van de uitrijdbaan. Als er geen voertuig op de uitrijdlaan staat, zal de poort slechts 100 cm openen om voetgangers en/of fietsers naar buiten te laten.

6.3 Alarmopvolging

De effectiviteit van de beveiliging van RWS is afhankelijk van een tijdige en adequate response na het constateren van een incident. Na een alarmering wordt, gereageerd door een particuliere beveiligingsorganisatie en/of door de politie.

DEEL 2 SPECIFICATIES BEVEILIGINGSMAATREGELEN

7 Terreinbeveiliging (T)

In aanvulling op de beveiligingsmaatregelen uit de VRKI past RWS zogenaamde terreinbeveiligingsmaatregelen toe, namelijk T1 en T2.

RWS wil bij voorkeur gebruik maken van 'sturende en vertragende (Stuver-)' beplanting, eventueel in combinatie met landschappelijke elementen, zoals sloten en/of taluds. Als alternatieve oplossing kunnen hekwerken worden toegepast. Tenslotte kunnen in een uitzonderlijk geval, in nauw overleg met RWS, ook muren worden toegepast.

In de volgende paragrafen staan de beschrijvingen en specificaties vermeld van de verschillende maatregelen. De specificaties zijn afhankelijk van de beveiligingsklasse waarvoor ze worden toegepast. Een overzicht van de maatregelen per zwaarte staat vermeld in de matrix in Bijlage 1 RWS-CD RBKI.

7.1 T1

In afnemende volgorde van voorkeur kan worden gekozen voor de volgende componenten:

7.1.1 Schuifpoort

In de terreinafscheiding moet ter plaatste van de hoofdontsluiting een elektrisch bediende schuifpoort worden aangebracht. De specificaties van de schuifpoort zijn als volgt:

- Hoogte: 1800 mm
- Type geleiding: Vrijdragend
- Soort poort: Enkele poortvleugel
- Type hek: Spijlen hekwerk
- Overklimbeveiliging: getande kam
- H.o.h afstand Spijlen: 132 mm
- Materiaal: Verzinkt
- Dikte spijlen: 26 x 1.5mm
- RAL-kleur: n.v.t. (doorzichtige coating bij locaties aan de kust)
- Onderdoorkruip: kleiner dan 150 mm

Een schuifpoort moet in de volgende standen kunnen worden geopend:

- Loopstand (voor voetgangers en fietsers);
- Half;
- Volledig.

De poort dient door middel van een drukknop en standenschakelaar eenmalig geopend, permanent geopend of op 'automatisch sluiten' te kunnen worden gezet. De drukknop en standenschakelaar worden in de intercomzuil achter een serviceluikje geplaatst. Bij netspanningsuitval komt de motor van het hek in vrijloop te staan en kan het hek met kracht handmatig worden opengeduwd.

Eventueel nieuw aan te leggen terreintoegangen moeten een netto vrije doorgang bieden van minimaal 10 meter breed en minimaal 4,50 meter hoog. Mocht dit uitgangspunt niet haalbaar zijn, dan dient hierover afstemming met RWS plaats te vinden.

Ter hoogte van zowel de binnenzuil als buitenzuil dient in het wegdek een detectielus te worden aangebracht: de inrijdlus en uitrijdlus. De uitrijdlus dient tenminste 10 meter vanaf de poort te liggen. Als om het openen van de poort wordt gevraagd (via Rijkspas, intercom of drukknop), detecteren de lussen of het wel of niet om een voertuig gaat. Bij een voertuig opent de poort in zijn geheel. Indien geen voertuig wordt waargenomen, opent de poort over een afstand van slechts 100 cm. Dit om voetgangers en fietsers door te laten.

De uitrijdlus maakt het ook mogelijk om de poort automatisch te openen als er een auto of een motorfiets op staat. De centralist van de TzC kan de uitrijdlus voor een bepaalde tijdsperiode activeren om de poort automatisch open te sturen als er een voertuig overheen rijdt. Dit is nodig om uitrijdende vrachtwagens voor de gladheidsbestrijding zo min mogelijk te vertragen. Deze instellingen kunnen nadien geprogrammeerd worden.

Bij de poort dient een veiligheidssysteem te worden aangebracht waarmee wordt voorkomen dat een poort dicht gaat als er een voertuig tussen staat.

De toegangspoort dient van een Dicht-Signaleringssysteem (DS) te worden voorzien. Dit detectiesysteem moet zodanig worden aangebracht dat deze niet door passanten in alarm kan worden gebracht. Ook dient de Dicht-Signalering niet van buitenaf te malverseren te zijn.

7.1.2 Looppoort

Indien de gebruiker een looppoort expliciet wenst, moet deze naast de elektrische schuifpoort worden aangebracht en worden voorzien van een Rijkspaslezer.

De specificaties van de looppoort zijn;

- hoogte: 1800 mm
- Overklimbeveiliging: getande kam
- H.o.h afstand Spijlen: 132 mm
- Materiaal: Verzinkt
- Dikte spijlen: 26 x 1.5mm
- RAL-kleur: n.v.t. (doorzichtige coating bij locaties aan de kust)

Voor sommige locaties kan een met de vluchtrichting meedraaiende vluchtpoort expliciet nodig zijn, bijvoorbeeld als er op het terrein te weinig ruimte is om een verzamelplaats voor de BHV te realiseren. Deze doorgang dient zonder sleutel van binnenuit te openen zijn. Van buitenaf mag dit niet kunnen worden gemanipuleerd.

7.1.3 Stuver-beplanting

De natuurlijke barrières, bestaande uit hagen met sturende en vertragende beplantingen moeten voor T1 een hoogte hebben van 120cm boven maaiveld en een minimale breedte van 300cm.

Voor een specificatie van te gebruiken Stuver beplanting wordt verwezen naar Bijlage 3 Stuver-soorten. Bij de uiteindelijke keuze van de beplanting, kan het biodiversiteitsbeleid RWS als input worden meegenomen.

7.1.4 Gaashekwerk

Daar waar nodig, wordt een gaashekwerk toegepast. Ten behoeve van het gaashekwerk moeten de volgende specificaties worden aangehouden:

- Gaashoogte: 1800 mm
- Totale hoogte: 2050 mm
- Aantal puntdraden: 2 of 3
- Aantal spandraden: 2
- Diameter staanders: 60 mm
- Maaswijdte: 50 mm
- Staaldikte: 3 mm
- RAL-kleur: Groen

7.1.5 Sloten

Er hoeven geen nieuwe sloten te worden gegraven. Daar waar sloten reeds aanwezig zijn, dient de waterspiegel van de sloten tenminste 300 cm breed te worden.

7.2 T2

In afnemende volgorde van voorkeur kan worden gekozen voor de volgende componenten:

7.2.1 Schuifpoort

Ter plaatste van de hoofdontsluiting is een elektrisch bediende schuifpoort aangebracht. De specificaties van de schuifpoort zijn dezelfde als bij 7.1.1 vermeld, maar met een afwijkende hoogte van 220cm.

7.2.1 Looppoort

Indien de gebruiker een looppoort expliciet wenst, wordt een looppoort aangebracht. De specificaties van de looppoort zijn dezelfde als bij 7.1.2 vermeld, maar met een afwijkende hoogte van 220cm.

7.2.1 Stuver-beplanting

De natuurlijke barrière bestaande uit hagen met Stuver-beplanting moeten voor T2 een hoogte hebben van 120cm en een minimale breedte van 500cm.

Voor een specificatie van te gebruiken Stuver beplanting wordt verwezen naar Bijlage 3

Stuver-soorten. Bij de uiteindelijke keuze van de beplanting, kan het biodiversiteitsbeleid RWS als input worden meegenomen.

7.2.2 Dubbelstaafsmat-hekwerk (DSM)

Het hekwerk moet tenminste 220 cm boven het maaiveld uitsteken. Het DSM moet zijn opgebouwd uit 8/6/8 mm staven, waarbij de horizontale staven een diameter van 8 mm hebben en de verticale staaf een diameter van 6 mm.

De maaswijdte van de mat, de ruimte tussen de staven in, mag maximaal 5 cm breed en 20 cm hoog zijn.

De DSM moet een hoogte hebben van 223 cm inclusief 3 cm uitstekende verticale staven.

RAL: 9005 (zwart) of groen.

7.2.3 Sloten

De sloten moeten een breedte van de waterspiegel van minimaal 500 cm hebben.

7.3 Verlichting

Ten slotte dient er een verlichtingssysteem op het terrein te worden aangebracht langs de wegen en bij de parkeerplaatsen. Het systeem moet werken tijdens schemer en in nachtelijke uren onder de volgende omstandigheden:

- Wanneer het terrein van buitenaf via de poort wordt opgegaan, moet de verlichting langs de weg van de poort naar de parkeerplaatsen gedurende 5 minuten worden ingeschakeld.
- Wanneer een gebouw wordt verlaten, dient de verlichting langs het voetpad van het betreffende gebouw naar de parkeerplaatsen en langs de weg van de parkeerplaatsen naar de poort gedurende 5 minuten te worden ingeschakeld.
- Bij nieuw te plaatsen verlichting kan er ook voor worden gekozen om de lantaarnpaal te voorzien van aanwezigheidsdetectie. Aanwezigheidsdetectie is een vereiste als het terrein op andere manier dan via de toegangspoort regulier kan worden betreden, bijvoorbeeld vanaf een RWS vaartuig aan de kade of steiger.
- De lichtkleur is erg belangrijk voor een juiste kleurweergave van de camerabeelden. Bij voorkeur wordt er wit licht gebruikt. Indien door omgevingsfactoren wit licht niet is toegestaan (Fauna, zoals vleermuizen) dan kan er worden gekozen om groen- of amberkleurige verlichting toe te passen. De verlichtingskleur amber of groen kan vrij worden gekozen naargelang de te beschermen fauna.
- Bij het toepassen van een andere verlichtingskleur dan de kleur wit, dienen de camera's in de nacht om te schakelen naar zwart/wit.

Hierbij moet er minimaal 5 lux op vloerniveau worden bereikt.

8 Bouwkundige maatregelen (BK)

Voor de bouwkundige maatregelen wordt verwezen naar respectievelijke hoofdstukken uit de vigerende versie van de VRKI van het Centrum van Criminaliteitspreventie & Veiligheid (CCV) op het moment van opdrachtverlening.

Bouwkundige maatregelen (BK-maatregelen) zijn maatregelen die bijdragen aan de inbraakwerendheid van de buitenschil of compartimenten van een gebouw. Dit betreft de maatregelen die betrekking hebben op de beveiliging van ramen en deuren (gevelelementen), zoals complete inbraakwerende gevelelementen, inbraakwerend hang- en sluitwerk en rolluiken en rolhekken. Daarnaast zijn de muren, het dak en de vloer- / kruipruimte van een gebouw bepalend voor het niveau van de bouwkundige weerstandsklasse.

8.1 BK1

Deze bouwkundige maatregelen bestaan uit het controleren op en toepassen van functionerend (bestaand) hang- en sluitwerk, eventueel zonder een specifieke beveiligingsklasse. Het hang- en sluitwerk moet zijn / worden aangebracht in gevelelementen van een goede kwaliteit. Indien de kwaliteit van het betreffende gevelement van een onvoldoende kwaliteit is, dient dit te worden vervangen.

Hiermee wordt een afgesloten (buiten)schil gerealiseerd, deze heeft echter geen minimaal geclassificeerde inbraakwerendheid.

8.2 BK2

Voor bereikbare gevelelementen conform NEN 5087 geldt een braakwerendheid van 3 minuten. Dit kan worden verkregen door toepassing van gevelelementen met weerstandsklasse 2 conform de NEN 5096 of NEN-EN 1627:2021 of door toepassing van hang- en sluitwerk dat voldoet aan het gestelde in de NEN 5089 (ook wel "PKVW-niveau" genoemd). Bij de upgrade van bestaande gevelelementen geldt dat zowel de hang- als de sluitnaad moet worden beveiligd.

Tevens moet SKG***® beslag met kerntrekbeveiliging worden toegepast.

8.3 BK3

Voor bereikbare gevelelementen conform NEN 5087 geldt een braakwerendheid van 5 minuten. Dit kan bij bestaande bouw worden gerealiseerd door een maatwerk uitvoering van een braakwerendheid van maximaal 5 minuten door toepassing van NEN 5089 hang- en sluitwerk (ook wel PKVW-niveau 'Zwaar' genoemd). Bij de upgrade van bestaande gevelelementen geldt dat zowel de hang- als de sluitnaad moeten worden beveiligd.

Bij nieuwbouw moet de braakwerendheid van 5 minuten worden gerealiseerd door toepassing van gevelelementen met weerstandsklasse 3 conform de NEN 5096 of NEN-EN 1627:2021.

Tevens moet bij bestaande en bij nieuwbouw SKG***® beslag met kerntrekbeveiliging worden toegepast.

9 Compartimenterende maatregelen (CO)

Voor de compartimenterende maatregelen wordt verwezen naar respectievelijke hoofdstukken uit de vigerende versie van de VRKI van het Centrum van Criminaliteitspreventie & Veiligheid (CCV) op het moment van opdrachtverlening.

De CO-maatregelen staan voor compartimentering. Een compartiment is een ruimte in een gebouw die is voorzien van een bouwkundige schil, die voldoet aan de BK-prestatie-eis. Voor een kluis, die onderdeel is van een gebouw, geldt minimaal dezelfde eis. (De kluis is in dit geval dus ook een compartiment.)

Compartimentering kan worden toegepast door middel van:

1. een bouwkundig compartiment: bouwkundige beveiliging van een ruimte in een gebouw;
2. een inbraakwerende kast (safe en/of kluis).

9.1 CO2

Voor compartimenten CO2 geldt een braakwerendheid van 3 minuten. Dit kan worden bereikt door toepassing van gevelelementen met weerstandsklasse 2 conform de NEN 5096 of NEN-EN 1627:2021 of door toepassing van hang- en sluitwerk dat voldoet aan het gestelde in de NEN 5089 (ook wel 'PKVW-niveau').

Tevens moet SKG***® beslag met kerntrekbeveiliging worden toegepast.

9.2 CO3

Voor compartimenten CO3 geldt een braakwerendheid van 5 minuten. Dit kan bij bestaande bouw worden gerealiseerd door een maatwerk uitvoering van een braakwerendheid van maximaal 5 minuten door toepassing van NEN 5089 hang- en sluitwerk (ook wel PKVW-niveau 'Zwaar'). Bij de upgrade van bestaande gevelelementen geldt dat zowel de hang- als de sluitnaad moet worden beveiligd.

Bij nieuwbouw moet de braakwerendheid van 5 minuten worden gerealiseerd door toepassing van gevelelementen met weerstandsklasse 3 conform de NEN 5096 of NEN-EN 1627:2021.

Tevens moet bij bestaande en bij nieuwbouw SKG***® beslag met kerntrekbeveiliging worden toegepast.

10 Meeneembeperkende maatregelen (ME)

Voor de meeneembeperkende maatregelen wordt verwezen naar respectievelijke hoofdstukken uit de vigerende versie van de VRKI van het Centrum van Criminaliteitspreventie & Veiligheid (CCV) op het moment van opdrachtverlening.

Onder de ME-maatregelen vallen de meeneembeperkende maatregelen die de zichtbare drempel voor de indringer zo hoog mogelijk legt en die zorgt dat de goederen niet direct kunnen worden verzameld om mee te nemen

10.1 ME2

Prestatie-eis: 3 minuten diefstalvertraging conform de mogelijkheden als geboden en beschreven in de VRKI. Voorbeelden zijn:

- Verplaatsen;
- Koppelen;
- Verankeren.

10.2 ME3

Prestatie-eis: 5 minuten diefstalvertraging conform de mogelijkheden als geboden en beschreven in de VRKI. Voorbeelden hiervan zijn:

- Kisten of kasten;
- Hekwerken.

11 Specificaties Toegangscontrolesysteem (TCS)

11.1 Algemeen

Het TCS moet het mogelijk maken om daartoe geautoriseerde personen, automatisch toegang tot het terrein, de gebouwen en bepaalde ruimtes in de gebouwen te verschaffen.

11.2 Systeemconfiguratie

De volgende systeemdelen zijn te onderscheiden:

1. Toegangspassen;
2. Paslezers
3. Boosters;
4. Lokale deurcontrollers;
5. Elektrisch bedienbare poorten;
6. Zuilen;
7. Elektrisch bedienbare deurvergrendelingen en deurautomaten;
8. Nood Deur Opener (Noodverbreekschakelaar);
9. Elektrisch bedienbare, beveiligde en gecontroleerde sleutelkluizen.

11.2.1 Toegangspassen

RWS gebruikt Rijkspassen. Voor de installatie van het TCS, de programmering en het gebruik wordt verwezen naar het 'normenkader Rijkspas en de aansluitvoorwaarden Rijkspas RWS CD'. De volgende 4 types Rijkspassen worden gebruikt:

- Type P voor intern Personeel;
- Type E voor Extern personeel (met een contract op naam);
- Type B voor Bezoekers (niet-gepersonaliseerd);
- Type F voor gecontracteerde partijen.

11.2.2 Paslezers

De toegangspassen dienen te worden gelezen door specifieke Rijkspaslezers. De paslezers inclusief deurcontrollers van het TCS moeten voldoen aan het gestelde in de 'Aansluitvoorwaarden Rijkspas RWS' versie 1.6.

De lezers moeten op een hoogte van 110 cm boven de vloer worden aangebracht. Voorafgaand aan de realisatiewerkzaamheden dient uitvoerig overleg te worden gevoerd met de opdrachtgever over de wijze waarop de paslezers en de bijbehorende bekabeling moeten worden aangebracht. De lezers moeten op een hoogte van 110 cm boven de vloer worden aangebracht. De paslezer voor bediening alarm, dient naast het CBD te worden gepositioneerd, op een afwijkende hoogte.

11.2.3 Boosters

Boosters dienen voor het versterken van het Rijkspassignaal, zodat de toegangspoort op afstand kan worden geopend. Een booster is een versterker die wordt geplaatst in het voertuig. De Rijkspas kan in de booster worden gestoken, waarna de booster het kaartnummer van de Rijkspas verstuurd naar de controller, net zoals gebeurd bij het aanbieden van een Rijkspas aan een paslezer maar dan over grote afstand.

Rijkspasbeheer dient gebruik van boosters nog vast te leggen en te specificeren. Hierna productspecificaties van de leveranciers volgen die hieraan voldoen.

11.2.4 Lokale deurcontrollers

De paslezers dienen te worden aangesloten op lokale deurcontrollers (DC's). De exacte locaties van deze DC's dienen tijdens site-surveys in nauw overleg met de opdrachtgever te worden bepaald.

Indien de verbinding tussen de DC's en de server wegvalt, moeten de controllers autonoom blijven functioneren. Wanneer de verbinding is hersteld, dienen de lokale controllers automatisch de data die tijdens de verbindingsuitval is veranderd aan de server door te geven of van de server te ontvangen.

De onderstations dienen conform de Aansluitvoorwaarden Rijkspas RWS te zijn voorzien van een no-break-noodspanningsvoorziening.

11.2.5 Elektrisch bediende poorten

Een groot aantal RWS-terreinen is voorzien van elektrisch bediende voertuigpoorten. In nauwe samenwerking met de leverancier van de poorten en na nauw overleg met de opdrachtgever dient een koppeling te zijn aan gebracht tussen de poortsturing en het TCS. Daar waar die nog niet aanwezig is, of daar waar blijkt dat de bestaande poort dient te worden verwijderd en afgevoerd, dient in nauw overleg met de opdrachtnemer een elektrische poort te zijn geïnstalleerd.

11.2.6 Zuilen

Er dient aan de inrijdijde een zuil te worden geplaatst, waarin twee paslezers en twee video-intercomposten zijn geïnstalleerd. De belangrijkste eisen zijn:

- De zuilen en alle daarin op te nemen voorzieningen dienen te zijn afgestemd op het gebruik onder alle in Nederland denkbare weersomstandigheden, windinvloeden (voor de verstaanbaarheid van de intercoms), zoninstraling (bij de camera's), condensvorming en regen.
- RVS 316 zal moeten worden toegepast.
- Aan de achterzijde zijn de zuilen voorzien van twee inbraakwerende montage-deuren, die met een sleutel kunnen worden afgesloten. De weerstandsklasse van zuil dient 3 minuten te bedragen. Achter één van de montage-deuren dienen in de buitenzuil een drukknop voor éénmalig openen en een draaiknop voor de handmatige elektrische bediening van de poort te worden aangebracht om de poort permanent open te zetten. Dit in het geval van calamiteiten of als de toegangscontrole niet werkt.
- De afmetingen van de zuilen zijn boven het maaiveld: 2300 mm x ø 204 mm.
- De bovenste paslezer op ca. 2100 mm met daarbij de video intercom en de onderste paslezer op ca 1200 mm met daarbij de andere video intercom.
- Intercom. In de buitenzuilen moeten in de daarvoor bestemde frontpanelen video-intercomposten worden aangebracht, waarmee men verbinding kan krijgen met een centralist in de ToezichtCentrale (TzC).
- De kabelinvoer gebeurt via een opening in de bodemplaat van de zuil.
- Naar de locaties waar de zuilen worden geplaatst, dienen HDPE-mantelbuizen met een diameter van 50 mm en een dikte van 3,35 mm te worden gelegd. De buizen zijn voorzien van een trekdraad die voldoende stevig is om de aan te brengen voedings- en stuurkabels door de buis te trekken.
- Rode drukknoppen. Op de aan de binnenzijde geplaatste zuilen moeten op de daarvoor bestemde frontpanelen rode, slagvaste, waterdichte drukknoppen van het type 'paddenstoel' worden geplaatst, waarmee de poorten met één druk op een knop worden open gestuurd. De knoppen moeten dusdanig zijn geplaatst dat ze niet van buiten de terreinafscheiding kunnen worden bediend.

11.2.7 Elektrische deurvergrendelingen en deurautomaten

Er moet een aantal elektrische deurvergrendelingen worden aangebracht. Deze vergrendelingen zorgen ervoor dat deuren met behulp van de lokale onderstations elektrisch kunnen worden vergrendeld en ontgrendeld. RWS kent de volgende type deuren:

- **Hoofdentreedeur.** Er wordt naar gestreefd om per gebouw slechts één buitendeur als hoofdentreedeur aan te merken. Deze deur moet zijn voorzien van een éézijdig elektrisch bediend solenoidslot (met eenpunts- of driepuntsvergrendeling, afhankelijk van de RBK) van het type 'spanningsloos vergrendeld'. RWS heeft voor dit type sloten gestandaardiseerd in het type EL 460 en EL560 van Assa Abloy. Op de deur dient een 'Dicht-en-Opslot-Signalering' (DOS) te worden aangebracht die is opgenomen in het ISS.

Hoofdentreedeeuren die ook als vluchtdeuren dienen, moeten in één handeling die voldoet aan het Bouwbesluit, zonder pasje of sleutel, van binnen zijn te openen. Eventueel in en rondom deze deuren aangebrachte ramen (daglichten) dienen te zijn voorzien van braakwerende beglazing. Hiervoor geldt dat voor bestaande situaties thermopane beglazing wordt geaccepteerd. In nieuwbouw situaties is P5a beglazing vereist.

- **Buitendeuren.** Alle buitendeuren, die geen hoofdentreedeur zijn, maar waardoor wel het pand kan worden verlaten, moeten zijn voorzien van een mechanisch slot met één- of driepuntsvergrendeling (afhankelijk van de RBK) en dienen bij voorkeur te zijn voorzien van blinde buitenschilden. De deuren moeten zijn voorzien van een DOS.
- **Nood- en vluchtdeuren.** De ontgrendeling van alle nood- en vluchtdeuren dient te voldoen aan het gestelde in de normen NEN-EN 179 of NEN-EN 1125 en NEN-EN 13637. De deuren moeten zijn voorzien van een DOS.
- **Overige buitendeuren.** Alle buitendeuren, zoals deuren van technische ruimten en opslagruimten, moeten worden beveiligd conform de RBK waarin het gebouw of de ruimte is ingeschaald.
- **Overige binnendeuren.** Alle binnendeuren die toegang verschaffen tot een compartiment uit de RBK 3 of 4 moeten zijn voorzien van een elektrisch bediend slot (spanningsloos ontgrendeld) met driepuntsvergrendeling en een DOS. Ruimtes uit de RBK 1 of 2 en overige ruimtes worden voorzien van een mechanisch slot en hoeven niet te worden voorzien van een DS of DOS.

De volgende typen elektrische vergrendelingen, kabeldoorvoeren, deurstand-signaleringen, drangers, beslag en deurautomaten moeten worden gebruikt:

- Elektrische driepuntsvergrendelingen in de hoofdentreedeeuren;
 - Elektrische driepuntsvergrendelingen in binnendeuren;
 - Elektrische éénpuntsvergrendelingen in binnendeuren;
 - Inbouw kabeldoorvoeren;
 - Inbouw deurstandsignaleringen;
 - Drangers;
 - Beslag;
 - Deurautomaten in geval van MiVa doorgang.
- a. Elektrische driepuntsvergrendelingen in hoofdentreedeeuren. In de hoofdentreedeeuren waar nog geen elektrische driepuntsvergrendelingen zijn aangebracht, dienen deze te worden aangebracht als dit conform de RBK noodzakelijk is. Gelet op de standaardisatie binnen RWS, dienen deze sloten bij SKG***® van het type EL 460 (smaldeurslot) en EL560 van Assa Abloy te zijn. Bij SKG***® moet EL466 (smaldeurslot) of EL 566 van Assa Abloy worden toegepast. De gebruikte vergrendelingen moeten vanuit de beveiligde ruimte te allen tijde met één handeling zijn te openen. Het gebruikte slot dient te voldoen aan de volgende specificaties:
- Zelf vergrendelend na het sluiten van de deur;
 - Voorzien van schootstand signalering, "triggerbolt"-signalering en signaleringen van het bedienen van de kruk en de cilinder;
 - Arbeidsstroom (spanningsloos vergrendeld);
 - Aan de aanvalszijde voorzien van een hoogwaardige, halve Europrofielcilinder, SKG *** ®, waarmee het slot uitsluitend kan worden ontgrendeld (in geval van een defect) en waarmee het slot dus NIET kan worden vergrendeld;
 - 12 of 24 Volt = en voorzien van blusdiode;
 - Voorzien van bekabeling waarmee alle op het slot aanwezige elektrische aansluitingen zonder lasverbindingen kunnen worden aangesloten op een lokale deurcontroller.
- b. Elektrische driepuntsvergrendelingen in binnendeuren. In de binnendeuren die toegang geven tot BK3-ruimten, dienen elektrische driepuntsvergrendelingen te worden

aangebracht. Voor deze sloten geldt hetzelfde als hierboven bij a. is beschreven.

- c. Elektrische éénpuntsvergrendelingen in binnendeuren. In de binnendeuren die toegang geven tot BK2-ruimten, dienen elektrische éénpuntsvergrendelingen te worden aangebracht. Voor deze sloten geldt hetzelfde als hierboven bij b. is beschreven, met uitzondering van het aantal vergrendelpunten.
- d. Inbouw kabeldoorvoeren voor gebruik bij sloten die in de deuren worden gemonteerd. Voor deze doorvoeren geldt:
- Verchroomd staal of zwart gemoffeld of gespoten;
 - Geschikt voor kabels tot 10 mm dik;
 - Voor toepassing in deuren met een draaipunt tot 36 mm en opening tot 180°.
- e. Inbouw deurstandsignaleringen. Deze magneetcontacten moeten voldoen aan het volgende:
- Wisselcontact in messing behuizing;
 - Excentrisch aangebracht magneetdeel en contactdeel;
 - Schakelafstand instelbaar, maximaal 7 mm in stalen kozijn.
- f. Drangers. De elektrisch ontgrendelde deuren dienen te worden voorzien van drangers die de deuren na het openen mechanisch weer sluiten. De drangers moeten voldoen aan de volgende specificaties:
- Hydraulisch tandheugelsysteem;
 - Geschikt voor deuren tot een breedte van 1300 mm en een gewicht van 120 kg;
 - Openingshoek maximaal 180°;
 - Instelbare sluitsnelheid tussen 180° en 10°;
 - Instelbare eindslag tussen 10° en 0°;
 - Kleur in nauw overleg met de opdrachtgever te bepalen.
- g. Beslag. De braakwerendheid van het toe te passen beslag moet gelijk zijn aan het slot waarop het wordt toegepast. Levering en plaatsing van het beslag mag uitsluitend gebeuren na voorafgaande toestemming van de opdrachtgever. Het beslag op buitendeuren moet zijn voorzien van kerntrekbeveiliging.
- h. Deurautomaten voor het elektrisch openen van een deur moeten voldoen aan het volgende:
- Geschikt voor deuren tot een breedte van 1300 mm en een gewicht van 140 kg;
 - Instelbare openingstijd;
 - Instelbare sluitingstijd;
 - Instelbare openhoudtijd;
 - Zelfsluitend bij spanningsuitval;
 - Kleur in overleg met de opdrachtgever te bepalen;
 - 230 VAC, bekabeling VMVL 3 x 0,75 mm²;
 - Voorzien van bekabeling waarmee alle op de automaat aanwezige elektrische externe besturingsaansluitingen zonder lasverbindingen kunnen worden aangesloten op een lokale deurcontroller.
 - Voorzien van knelbeveiliging.

11.2.8 Nood Deur Opener (Noodverbreekschakelaar)

Als er toegangscontrolevoorzieningen zijn geplaatst in de vluchtrichting moet in geval nood door het indrukken van een groene noodverbreekschakelaar (verder: 'Nood Deur Opener' (NDO)) naast een deur, het 'spanningsloos ontgrendeld slot' worden vrijgegeven, door het onderbreken van de aansluiting op de voedingsspanning. Er is vanaf dit moment dus onbepaald en onbeheerd door het systeem, toegang tot de betreffende inpandige ruimte mogelijk. De noodrukknop dient in vluchtrichting gezien in de directe nabijheid van de te ontgrendelen deur(-en) te worden geplaatst.

Wanneer een ontruimings- of brandalarm wordt gegenereerd, dienen de elektrisch bediende deuren die zijn voorzien van een 'spanningsloos ontgrendeld slot' elektrisch te worden ontgrendeld. Ook moet de buitenpoort worden open gestuurd. De opdrachtnemer dient hiertoe in nauw overleg met de opdrachtgever de benodigde sturing te maken tussen de brandmeldcentrale en het TCS.

Wanneer een deur in geval van nood wordt geopend, dient hiervan via het SMS een alarmmelding te worden gegeven aan de TzC. De NDO dient hiertoe te zijn voorzien van dubbel uitgevoerde 'normally closed' contacten.

11.2.9 Elektrisch bedienbare en gecontroleerde sleutelkluizen

RWS heeft ervoor gekozen om zo min mogelijk sleutels op een locatie te gebruiken. De weinige sleutels die nog worden gebruikt, moeten worden opgeborgen in een elektronisch bedienbare, beveiligde en gecontroleerde sleutelkuis voor B&O. Deze sleutelkuis wordt geplaatst in de directe omgeving van de hoofdentreedeur. De sleutelkuis dient te voldoen aan de volgende specificaties:

- Een gecertificeerde braakwerendheid van tenminste 5 minuten;
- Aantal op te hangen sleutelbossen: zes;
- Voorzien van een elektronisch slot dat wordt ontgrendeld door:
 - het aanbieden van een valide Rijkspas; of
 - toegang door middel van een autorisatie vanuit de TzC.
- De betreffende sleutels mogen vervolgens uitsluitend worden vrijgegeven aan de daartoe geautoriseerde personen. De uitname van de sleutels moet per pas worden geregistreerd in het TCS of uitgifte door middel van een autorisatie vanuit de TzC;
- Indicatie led dat een sleutel mag worden uitgenomen;
- Indicatie led dat een sleutel op de juiste manier is geretourneerd;
- IP65 (vocht en stof bestendig)

12 Het Indringer Signaleringsysteem (ISS)

12.1 Algemeen

Het ISS is van toepassing bij de beveiligingsmaatregelen EL en SD. Het ISS detecteert ongeautoriseerde toegang en/of indringing in de gebouwen. Alle te beveiligen groepen zijn daartoe in onafhankelijk te bedienen zones aangesloten op een Centrale Controle- en Stuureenheid (CCS).

De CCS moet softwarematig kunnen worden onderverdeeld in minimaal vijf soorten groepen, namelijk vertraagde uitgangsgroepen, buitenbeveiligingsgroepen, gevelbeveiligingsgroepen, ruimtelijke beveiligingsgroepen en 24-uurs bewaakte groepen.

De vertraagde uitgangsgroep bestaat uit magneetcontacten in de hoofdentreedeeuren en de detectoren in de hoofdentree- en entreeruimte. De buitenbeveiligingsgroepen worden gevormd door de buitendetectiesystemen op basis van videomotiondetectie. De gevelbeveiligingsgroepen bestaan uit Dicht-en-Opslot-Signaleringen (DOS-en) en Dicht-Signaleringen (DS-en) op de buitendeuren en ramen en uit trilcontacten op de kozijnen. De ruimtelijke beveiligingsgroepen bestaan uit de ruimtelijke detectoren in de bereikbare ruimten (conform NEN 5087) en overige risicoruimten. De 24-uur bewaakte groepen worden gevormd door de sabotagecontacten en DS op nooddeuren.

In een gebouw met meerdere gebruikersorganisaties, waarvan het alarm van de ruimtes afzonderlijk kan worden geschakeld, worden nooit alle detectoren van een ISS in één keer uitgeschakeld. Zodra een geautoriseerde Rijkspas én een genummerde drukknop wordt ingedrukt, worden de detectoren in de ruimten van de betreffende organisatie uitgeschakeld.

12.1.1 EL2

Voor gebouwdelen met een EL2 classificatie wordt verwezen naar betreffende paragraaf uit de vigerende versie van de VRKI van het Centrum van Criminaliteitspreventie & Veiligheid (CCV) op het moment van opdrachtverlening.

In aanvulling op de VRKI wordt het gestelde uitgevoerd met **dual** ruimtelijke detectoren in de 'EN configuratie', om onnodige meldingen zoveel mogelijk te voorkomen.

12.1.2 EL3

Voor gebouwdelen met een EL3 classificatie wordt verwezen naar betreffende paragraaf uit de vigerende versie van de VRKI van het Centrum van Criminaliteitspreventie & Veiligheid (CCV) op het moment van opdrachtverlening.

In aanvulling op de VRKI wordt het gestelde uitgevoerd met **dual** ruimtelijke detectoren **met anti-cloak** in de 'EN configuratie', om onnodige meldingen zoveel mogelijk te voorkomen en om maximale detectiewaarschijnlijkheid te verkrijgen.

12.1.3 Het ISS in een gebouw

Het ISS in een gebouw waarin geen andere gebruikersorganisaties aanwezig zijn, wordt in- en uitgeschakeld door het aanbieden van een geautoriseerde Rijkspas aan een paslezer naast het CBD in de buurt van de hoofdentree.

In gebouwen waarin naast RWS nog andere gebruikersorganisaties aanwezig zijn, worden de RWS-verdiepingen voorzien van elektrisch vergrendelde entreedeeuren tot de afdelingen. Zodra een geautoriseerde pas wordt aangeboden aan een paslezer bij een dergelijke entreedeur, worden de detectoren in de ruimte achter die deur uitgeschakeld. Dit betekent dat dus nooit alle inbraakdetectoren in een gebouw gelijktijdig worden uitgeschakeld. Het inschakelen van de beveiliging op een afdeling gebeurt als de laatste aanwezige zijn Rijkspas aanbiedt aan een paslezer naast het CBD in de buurt van de entreedeur en het indrukken van een genummerde drukknop op een tableau dat ook in de nabijheid van de het CBD is geplaatst.

12.2 Beveiligingsmodi

De detectoren in een gebouw dienen in de navolgende beveiligingsmodi te kunnen worden geschakeld:

- a. Beveiligd. Dit is de normale beveiligingsmodus. In deze stand zal iedere activering van een magneetcontact, een indringerdetectiesensor, een tampercontact en/of sabotage-detectiecircuit in de betreffende zone een alarmmelding veroorzaken.
- b. Niet beveiligd. In deze modus wordt de activering van indringerdetectoren niet door de CCS als een alarm gemeld. De activering van een tampercontact en/of een sabotagecircuit in een zone zal wél tot een alarmmelding leiden.
- c. Overbrugd. In deze stand wordt een alarm van een specifieke detector tijdelijk niet door de CCS aan de TzC gemeld. Een detector kan uitsluitend door een centralist van de TzC, door een locatie manager of mobiele surveillancedienst worden overbrugd. Na toestemming van de dienstdoende piketofficier van RWS worden overbrugd. Hierbij dient de software de keuze te bieden uit de volgende mogelijkheden om de overbrugging op te heffen:
 - Het automatisch opheffen van de overbrugging bij het uitschakelen van het ISS in het gebouw.
 - Het handmatig op afstand uit de overbruggingsstand halen van de detector door een centralist van de TzC of een medewerker van het Team Safety en Security (adviseur fysieke beveiliging).
- d. Uit bedrijf. In deze stand wordt een specifieke detector geheel uit bedrijf genomen. Dit mag uitsluitend door een servicemonteur na toestemming van de betreffende locatiemanager na afstemming met het 'Team Safety & Security' gebeuren.

12.3 Alarmmeldingen

De CCS-en dienen op de volgende wijze na een indringdetectie te functioneren:

- a. Het aansturen van binnensirenes en flitslichten. Binnensirenes mogen maximaal 3 minuten afgaan. Bij een nieuw alarm gaan ze weer af. Flitslichten blijven aan. Deze aansturingen blijven gehandhaafd, totdat de bewuste sectie is uitgeschakeld.
- b. Het bekrachtigen van één of meerdere relais waarmee de buitenverlichting op het terrein kan worden ingeschakeld.
- c. Het bekrachtigen van één of meerdere relais waarmee elektronische vertragingsmiddelen (zoals mistgeneratoren en stroboscopen) kunnen worden ingeschakeld.
- d. Het via het Security Netwerk (SN, zie hoofdstuk 11) melden van het alarm aan de TzC. In deze melding moeten volgens één van de gangbare transmissieprotocollen tenminste de volgende gegevens worden vermeld:
 - Het aansluitnummer van de RWS-locatie waarop het alarm zich voordoet;
 - De status van het systeem;
 - Het type alarm;
 - Het zonenummer van het alarm;
 - De zonenaam waarin het alarm zich voordoet.
- e. Het via een 4G-backup-modem geven van een alarmmelding aan de TzC. In deze melding moeten volgens één van de gangbare transmissieprotocollen dezelfde gegevens worden vermeld die via het Security Netwerk (zouden) zijn gestuurd.

12.4 Toegankelijkheid tot de CCS-en

- a. Functionele niveaus. T.a.v. de toegankelijkheid tot de CCS-en dient onderscheid te worden gemaakt in de volgende functionele niveaus:
 - Beveiligingsmedewerkers;
 - ISS-beheerders (o.a. Locatiebeheerder en Team Safety en Security);
 - Servicetechnici.

In de hierboven vermelde niveaus dienen de beveiligingsmedewerkers de minste bevoegdheden en de servicetechnici de meeste bevoegdheden toegewezen te krijgen. Hierbij dient te worden opgemerkt dat de servicetechnici slechts na het inloggen van een beveiligingsmedewerker of een ISS-beheerder, toegang tot het systeem mogen krijgen.

- b. Pincodes. Zowel de beveiligingsmedewerkers, als de ISS-beheerders, als de servicetechnici dienen slechts via het intoetsen van een pincode toegang te kunnen krijgen tot het gebruik van het systeem.
- c. Wijzigen van systeemparameters. De systeemparameters mogen slechts door de installateur of het onderhoudsbedrijf (servicetechnici), na het intoetsen van zijn zakelijke pincode, kunnen worden ingevoerd c.q. gewijzigd.
- d. Wijzigen van service- / onderhoudsbedrijf. De (zakelijke) pincode van de installatie ten behoeve van service- en onderhoud, dienen bij wijziging van het service- en onderhoudsbedrijf, aan RWS te worden overgedragen.

12.5 Systeemconfiguratie

De volgende systeemdelen zijn te onderscheiden:

1. Buitendetectieapparatuur;
2. Geveldetectieapparatuur;
3. Binnendetectieapparatuur;
4. Centrale Controle- en Stuureenheid;
5. Codebediendeel;
6. Meldapparatuur;
7. Apparatuur t.b.v. de no-breakspanningsvoorziening.

12.5.1 Buitendetectieapparatuur

RWS beschikt over een aantal productie-elementen die buiten staan opgesteld, de zogenaamde buitenopstelplaatsen. De beveiliging van deze buitenopstelplaatsen is maatwerk en dient te bestaan uit een afgewogen combinatie van bouwkundige en elektronische beveiligingsmaatregelen. Het toe te passen detectiesysteem bestaat uit Videomotion detectoren.

- **Algemeen.** Op diverse plaatsen langs afmeerplaatsen en langs opstelplaatsen van strooi- en sneeuwschuifapparatuur kunnen beveiligingscamera's worden geplaatst die worden voorzien van een videodetectiesysteem.
- **Uitvoering.** Bij de uitvoering moet rekening worden gehouden met de volgende aspecten:
 - Installatie. Het aansluiten en programmeren van de camera's op een server van het Video Management Systeem, voorzien van Videomotiondetectie software, conform de externe bijlagen Aansluitvoorwaarden TzC, zoals nader gespecificeerd in het hoofdstuk VSS.
 - Programmering. In nauw overleg met de opdrachtgever dienen detectiezones en -richtingen te worden geprogrammeerd.
 - Mechanische aanpassingen. Het verrichten van alle noodzakelijke mechanische aanpassingen om de hierboven genoemde voorzieningen te kunnen realiseren. Deze aanpassingen dienen pas na overleg met en toestemming van de opdrachtgever te worden gerealiseerd.
 - Verbindingen. Het realiseren van de verbindingen tussen de camera's en de videoserver en de CCS.
 - Testen. De goede werking van de videomotiondetectoren moet na de installatie volgens een vooraf door de opdrachtgever goedgekeurde testprocedure worden aangetoond.
- **Detectiewaarschijnlijkheid.** Het detectiesysteem moet elke indringing via lopen, kruipen, sluipen, tijgeren en springen kunnen detecteren. Per zone wordt een detectiewaarschijnlijkheid van 95% geëist.
- **Signalering.** Iedere zone dient als een afzonderlijke detectiegroep te worden signaleerd.
- **FAR (False Alarm Rate).** Het systeem mag per maand maximaal drie (3) vals alarm per zone genereren. De leverancier dient, teneinde zich aan dit maximumaantal oneigenlijke alarmen te kunnen conformeren, in de offerte de door hem geëiste omgevingscondities en

installatie-eisen te vermelden.

- **MTTF (Mean Time To Failures).** De MTTF dient minimaal 30.000 uren te bedragen.
- **MTTR (Mean Time To Repair).** De MTTR dient maximaal 240 minuten te bedragen, gerekend vanaf de tijd van aankomst van de servicetechnicus bij het defecte apparaat.

12.5.2 Geveldetectieapparatuur

De geveldetectieapparatuur bestaat uit 'Dicht-en-Opslot-Signaleringen' (DOS-en) en 'Dicht-Signaleringen' (DS-en) op de buitendeuren en sommige beweegbare ramen. Bij SD2 maken trillingsdetectoren of glasbreukmelders deel uit van de geveldetectieapparatuur.

a. Dicht-en-Opslot-Signaleringen (DOS-en).

- **Algemeen.** Om zeker te stellen dat de hoofdentreedeeuren en overige buitendeuren van een gebouw bij het inschakelen van het ISS zijn gesloten én vergrendeld, dient het dicht en tevens op slot zijn van die deuren te worden geverifieerd door middel van een DOS. Indien de deuren na het inschakelen van het ISS niet binnen 30 seconden zijn vergrendeld, dient een binnensirene te klinken en moet door het systeem een melding worden gemaakt aan de TzC.
- **Uitvoering.** De volgende werkzaamheden dienen te worden uitgevoerd:
 - Dichtsignalering. Het aanbrengen van magneetcontacten t.b.v. de dichtsignalering van de hoofdentree- en entreedeeuren. Er dient gebruik te worden gemaakt van gebalanceerde magneetcontacten.
 - Opslotsignalering. Het inbouwen van een corrosiebestendig schootcontact in de sluitkom of, daar waar mogelijk, het gebruik maken van het opslot-signaleringscontact van het slot in de deur.
 - Mechanische aanpassingen. Het verrichten van alle noodzakelijke mechanische aanpassingen om de hierboven genoemde voorzieningen te kunnen realiseren. Deze aanpassingen dienen pas na overleg met en toestemming van de opdrachtgever te worden gerealiseerd.
 - Verbindingen. Het realiseren van de verbindingen tussen de apparatuur op de deur en een CCS.
- **Detectiewaarschijnlijkheid.** Het detectiesysteem moet elke indringing via het openen van de deuren kunnen detecteren. Per toegang wordt een detectiewaarschijnlijkheid van 99% geëist.
- **Signalering.** Iedere contact dient als een afzonderlijke detectiegroep te worden gesignaleerd.
- **Nodeloze alarmen.** Het detectiesysteem mag geen alarm veroorzaken ten gevolge van het ontstaan van kieren in de kozijnconstructie, die kleiner zijn dan 0,5 cm.
- **FAR.** Het systeem mag per 24 maanden maximaal één (1) vals alarm per deur of tourniquet genereren. De leverancier dient, teneinde zich aan dit maximumaantal oneigenlijke alarmen te kunnen conformeren, in de offerte de door hem geëiste omgevingscondities en installatie-eisen te vermelden.
- **MTTF.** De MTTF dient minimaal 30.000 uren te bedragen.
- **MTTR.** De MTTR dient maximaal 240 minuten te bedragen, gerekend vanaf de tijd van aankomst van de servicetechnicus bij het defecte apparaat.

b. Dicht-Signaleringen (DS-en).

- **Algemeen.** Met behulp van deze detectoren kan een inbraak door het openen van de deuren, ramen en luiken worden gedetecteerd.
- **Uitvoering.** De volgende werkzaamheden dienen te worden uitgevoerd:
 - Dichtsignalering. Het aanbrengen van een magneetcontact ten behoeve van de dichtsignalering van tourniquets, deuren, ramen, putdeksels en luiken. Er dient gebruik te worden gemaakt van gebalanceerde magneetcontacten.
 - Mechanische aanpassingen. Het verrichten van alle noodzakelijke mechanische aanpassingen om de hierboven genoemde voorzieningen te kunnen realiseren. Deze aanpassingen dienen pas na overleg met en toestemming van de opdrachtgever te worden gerealiseerd.
 - Verbindingen. Het realiseren van de verbindingen tussen de apparatuur op de deuren en tourniquets en een CCS.
- **Detectiewaarschijnlijkheid.** Het detectiesysteem moet elke indringing via het openen van de buitendeuren kunnen detecteren. Per deur wordt een detectiewaarschijnlijkheid van 99% geëist.
- **Signalering.** Iedere deur dient als een afzonderlijke detectiegroep te worden gesignaleerd.
- **Alarmeringen.** Het detectiesysteem mag geen alarm veroorzaken ten gevolge van het ontstaan van kieren in de kozijnconstructie, die kleiner zijn dan 0,5 cm.
- **FAR.** Het systeem mag per 24 maanden maximaal één (1) vals alarm per deur of raam genereren. De leverancier dient, teneinde zich aan dit maximum aantal oneigenlijke alarmen te kunnen conformeren, in de offerte de door hem geëiste omgevingscondities en installatie-eisen te vermelden.
- **MTTF.** De MTTF dient minimaal 30.000 uren te bedragen.
- **MTTR.** De MTTR dient maximaal 30 minuten te bedragen, gerekend vanaf de tijd van aankomst van de servicetechnicus bij het defecte apparaat.

c. Dicht-Signaleringen (DS-en).

SD2 bestaat uit detectie, met als doel inbraaksignalering bij de eerste aanval op vaste en beweegbare gevelelementen van of voor, de periferie van ruimten waar de attractieve goederen zich bevinden. SD2 kan op meerdere wijzen worden gerealiseerd: bijvoorbeeld glasbreukdetectie en trillingsdetectie op de gevelelementen van de ruimten. Voor de bereikbaarheid van gevelelementen die zich aan de buitengevel bevinden moet de NEN 5087 worden gebruikt.

12.5.3 Binnendetectieapparatuur

De binnendetectieapparatuur bestaat uit 'dual PIR-radardetectoren' (Dual PIRR) en 'dual PIR-radardetectoren' met anti-cloak (Dual PIRR AC).

a. Dual Passief InfraRood Radardetectoren (Dual PIRR).

- **Algemeen.** Ten behoeve van het detecteren van de aanwezigheid van personen in ruimten met EL2 classificatie, worden deze ruimten voorzien van Dual Passief InfraRood Radardetectoren (Dual PIRR-en). Deze detectoren dienen te zijn voorzien van een 'Onderdoorkruip-detectie' en een "Maskeerdetectie".
- **Uitvoering.** De volgende werkzaamheden dienen te worden uitgevoerd:
 - Installatie. Het plaatsen van de Dual PIRR-en in de bereikbare ruimten op de begane grond en de bereikbare verdiepingen, het leggen van de vereiste bekabeling en het aansluiten op de CCS-en.

- Uitrichten en uitlopen. Het uitrichten van de detectoren en het uitlopen volgens de voorschriften van de fabrikant.
- Verbindingen. Het realiseren van de verbindingen tussen de Dual PIRR-en en een CCS.
- **Detectiewaarschijnlijkheid.** De Dual PIRR-en moeten een detectiewaarschijnlijkheid hebben van meer dan 80% daar waar een indringer, zwaarder dan 35 kg zonder hulp en/of hulpmiddelen kruipend, lopend, springend of rennend met een snelheid tussen 0,3 en 3,0 meter per seconde, zich begeeft in de detectiezone.
- **Maskeerdetectie.** De Dual PIRR-en moeten iedere maskeerpoging kunnen detecteren. Wanneer het ISS wordt ingeschakeld dient een gemaskeerde Dual PIRR, niet te kunnen worden ingeschakeld en moet hiervan een melding op het CBD worden weergegeven.
- **Signalering.** De Dual PIRR-en die worden gebruikt in de kantoren en de gangen dienen op onvertraagde lussen te worden aangesloten. De Dual PIRR achter de hoofdentreedeur moet worden aangesloten op een vertraagde in-/uitloopzone van het ISS. Zodra iemand na het inschakelen van het ISS een alarm bij de hoofdentreedeur veroorzaakt, moet de zoemer in het CBD een melding geven. De persoon in kwestie dient nu binnen 30 seconden zijn pas te laten lezen om het systeem uit te schakelen, waarna de zoemer uitschakelt.

Indien binnen de gestelde tijd geen valide pas wordt aangeboden, wordt een alarm verstuurd aan de TzC en gaan de binnensirenes loeien en de buiten flitslichten branden. In alle overige gevallen moet bij een ingeschakelde ISS direct na het ontstaan van een indringdetectie een alarmering naar de TzC worden verstuurd en de binnensirenes en de flitslichten worden ingeschakeld.

- **Alarmeringen.** De detectoren mogen geen alarm veroorzaken ten gevolge van het betreden van de detectiezone door kleine dieren lichter dan 10 kilogram.
- **FAR.** Een Dual PIRR mag per 24 maanden maximaal één (1) vals alarm genereren. De leverancier dient teneinde zich aan dit maximumaantal oneigenlijke alarmen te kunnen conformeren, in de offerte de door hem geëiste omgevingscondities en installatie-eisen te vermelden.
- **MTTF.** De MTTF dient minimaal 30.000 uren te bedragen.
- **MTTR.** De MTTR dient maximaal 30 minuten te bedragen, gerekend vanaf de tijd van aankomst van de servicetechnicus bij het defecte apparaat.

b. Dual Passief InfraRood Radardetectoren met 'anti-cloak-detectie' (Dual PIRR AC).

- **Algemeen.** Ten behoeve van het detecteren van de aanwezigheid van personen in ruimten met EL3 classificatie, worden deze ruimten voorzien van Dual Passief InfraRood Radardetectoren met 'anti-cloak-detectie' (Dual PIRR-en AC) Deze detectoren dienen te zijn voorzien van een 'Onderdoorkruip-detectie', een "Maskeerdetectie" en een anti-cloak-detectie, waarmee indringers kunnen worden gedetecteerd door middel van de radardetector, zonder dat de PIR de indringer heeft gedetecteerd.
- **Uitvoering.** De volgende werkzaamheden dienen te worden uitgevoerd:
 - Installatie. Het plaatsen van de Dual PIRR-en AC in EL3 geclassificeerde ruimten, het leggen van de vereiste bekabeling en het aansluiten op de CCS-en.
 - Uitrichten en uitlopen. Het uitrichten van de detectoren en het uitlopen volgens de voorschriften van de fabrikant.
 - Verbindingen. Het realiseren van de verbindingen tussen de Dual PIRR-en AC en een CCS.
- **Detectiewaarschijnlijkheid.** De Dual PIRR-en AC moeten een detectiewaarschijnlijkheid hebben van meer dan 95% daar waar een indringer, zwaarder dan 35 kg zonder hulp en/of hulpmiddelen kruipend, lopend, springend of rennend met een snelheid tussen 0,3 en 3,0 meter per seconde, zich begeeft in de detectiezone.

- **Maskeerdetectie.** De Dual PIRR-en AC moeten iedere maskeerpoging kunnen detecteren. Wanneer het ISS wordt ingeschakeld dient een gemaskeerde Dual PIRR AC, niet te kunnen worden ingeschakeld en moet hiervan een melding op het CBD worden weergegeven.
- **Signalering.** De Dual PIRR-en AC die worden gebruikt in de EL3 geclassificeerde ruimten dienen op onvertraagde lussen te worden aangesloten. Zodra iemand na het inschakelen van het ISS een alarm in deze ruimte veroorzaakt, wordt een alarm verstuurd aan de TzC en gaan de binnensirenes loeien en de buiten flitslichten branden.
- **Alarmeringen.** De detectoren mogen geen alarm veroorzaken ten gevolge van het betreden van de detectiezone door kleine dieren lichter dan 10 kilogram.
- **FAR.** Een Dual PIRR AC mag per 12 maanden maximaal één (1) vals alarm genereren. De leverancier dient teneinde zich aan dit maximumaantal oneigenlijke alarmen te kunnen conformeren, in de offerte de door hem geëiste omgevingscondities en installatie-eisen te vermelden.
- **MTTF.** De MTTF dient minimaal 30.000 uren te bedragen.
- **MTTR.** De MTTR dient maximaal 30 minuten te bedragen, gerekend vanaf de tijd van aankomst van de servicetechnicus bij het defecte apparaat.

12.5.4 Centrale Controle-en Stuur eenheid (CCS)

De detectoren worden door middel van beveiligde verbindingen aangesloten op een CCS. De CCS verzorgt via een netwerkverbinding de doormelding van alarmen aan de TzC, vanwaar men de Particuliere Beveiligingsorganisatie (PBO) als contractpartner van de RBO, en/of de politie waarschuwt. Het CCS moet hiertoe worden aangesloten op het Security Network.

12.5.5 Code Bedien Deel (CBD)

Het ISS dient lokaal te kunnen worden bediend en beheerd met behulp van een CBD. In elk gebouw dient achter de (hoofd-)entree deur een CBD te worden geplaatst, waarmee het ISS kan worden bediend en beheerd en waarop de status van het systeem en/of van de beveiligingscomponenten op een alfanumeriek display kan worden afgelezen.

Op het CBD kan de status van het ISS en diens componenten worden afgelezen. Ook kunnen met behulp van het CBD delen van het ISS worden bediend en handmatig worden overbrugd.

Een gebouw kan bestaan uit meerdere secties (bijvoorbeeld omdat er meerdere partijen gebruik maken van het gebouw). In dat geval vindt het in- en uitschakelen plaats door het aanbieden van een Rijkspas en het vervolgens indrukken van een genummerde drukknop, waarvan het nummer overeenstemt met de betreffende sectie.

12.5.6 Meldapparatuur

Het ISS dient minimaal de onderstaande alarmmeldingen te kunnen verzorgen:

- een inbraakalarm na de detectie van een indringer;
- een overvalalarm (ook wel 'hold-upalarm' genoemd) na het indrukken van een overvaldrukknop;
- een sabotagealarm ('tamperalarm') na de detectie van sabotagehandelingen (zoals het kortsluiten van bedrading, het verwijderen van bedrading en/of systeemdelen en het ongeautoriseerd openen van de behuizing van systeemdelen);
- een communicatiealarm ter indicatie van storingen in het datatransmissiesysteem;
- een voedingsspanningsalarm ter indicatie van fouten in de voedingsspanningsvoorziening.

Om de alarmmeldingen lokaal kenbaar te maken, dienen in elk beveiligd gebouw minimaal één binnensirene te worden geïnstalleerd, die hoorbaar is in het gehele gebouw. Ook moet een flitslicht aan de wegzijde op de bovenste verdieping van het betreffende gebouw worden geplaatst.

Alarmmeldingen moeten via het Security Netwerk aan de TzC worden gemeld. Alarmmeldingen die niet via het SN kunnen worden verzonden ten gevolge van netwerkproblemen, moeten via een 4G-router aan de TzC worden verstuurd. Deze router dient in de CCS te worden geïntegreerd.

12.5.7 De voedingsspanningsvoorziening

- a. De nominale voedingsspanning. De complete ISS-apparatuur dient te worden aangesloten op de lokale netspanningsvoorziening met de volgende specificaties: 230V AC +10%; 50Hz +5%. De aansluiting op de bestaande spanningsinstallatie dient door de leverancier in zeer nauw overleg met de opdrachtgever te gebeuren.
- b. Netspanningsuitval. In geval van een onderbreking van de 230V-voedingsspanningsvoorziening, moet een alarmmelding worden gegenereerd naar de TzC. Een door de opdrachtnemer te leveren en in de systeemkast van het CCS te installeren no-breaksysteem dient dan gedurende minimaal 30 uur alle systeemdelen van spanning te kunnen voorzien. Als de capaciteit van het no-breaksysteem na die tijd zover afneemt dat de geleverde spanning beneden de nominaal vereiste werkspanning komt, moet hiervan een melding worden gegeven aan de TzC. Er is vanaf dit moment dus ongedetecteerd door het systeem, toegang tot de gebouwen mogelijk.
- c. Batterijen. Het ISS dient een beveiliging te bezitten tegen het te ver ontladen van de batterijen van het no-breaksysteem en tegen het optreden van een te hoge laadstroom. Een eventueel benodigde separate batterijruimte dient afsluitbaar te zijn en van een tamper-detectie te zijn voorzien.
- d. Aarding. Alle aarding, benodigd voor het goed en veilig functioneren van het ISS dienen door de leverancier te worden verzorgd na overleg met de opdrachtgever.
- e. Overspanningsafleiding. De elektrische voeding van de centrale ISS-apparatuur en de deelsystemen dienen te worden voorzien van een overspanningsafleiding van 2kV.

De wandcontactdozen ten behoeve van de voedingsaansluiting van de ISS-apparatuur dienen te zijn voorzien van een overspanningsafleiding voor spanningen vanaf 250V AC.

13 Specificaties (Video) Intercomsystemen

13.1 Algemeen

Om vanuit de TzC en de intercompost vanuit een gebouw op het terrein personen bij de poorten en een hoofdentree die aan de openbare weg ligt te woord te staan, dient een (video)intercominstallatie (hierna intercom) te worden aangelegd. De intercomapparatuur dient op het Security Netwerk te worden aangesloten.

Op alle steunpunten worden intercomposten geplaatst bij de toegangspoort en bij hoofdentreedeeuren welke aan de openbare weg grenzen. In overleg kan op specifieke locaties bij het hoofdgebouw ook een intercompost worden geplaatst. Deze intercomposten worden geïntegreerd in het SMS van de TzC.

Bij een intercomoproep wordt deze gemeld aan de centralisten binnen de TzC. Intercomoproepen komen binnen in de intercomafhandelingsomgeving op volgorde van binnenkomst en prioriteit.

Het moet voor RWS mogelijk zijn om aan locaties en intercomposten verschillende prioriteiten te programmeren, waardoor het voor de centralist direct duidelijk is, welke intercomoproep als eerste moet worden behandeld.

Een intercomoproep kan afkomstig zijn van de intercompost bij een toegangspoort of in of bij een gebouw. Een intercomoproep zal veelal gevolgd worden door een actie van de centralist. Een intercomoproep bij een toegangspoort zal veelal leiden tot het verzoek voor het openen van de toegangspoort.

Om de centralist te ondersteunen in het afhandelen van de intercomoproep zal er op de werkplek van de centralist een hoofdintercompost worden geplaatst. Deze intercompost zal worden voorzien van een aantal functieknoppen die per oproep van functie kunnen wijzigen. Door middel van de functieknoppen kan de centralist snel, eenvoudig en ergonomisch de acties uitvoeren die met de bewuste intercomoproep gepaard gaan. Dit kan bijvoorbeeld zijn het openen van de toegangspoort voor fietsers en voetgangers, het openen van de poort voor voertuigen of het openen van de toegangspoort voor een langere periode (ad-hoc in te stellen aantal uren) als er meerdere voertuigbewegingen zijn te verwachten, bijvoorbeeld bij het uitvoeren van de gladheidsbestrijding.

Ter ondersteuning van de centralist zullen de intercomoproepen worden voorzien van videobeelden van een videocamera in de intercompost en een overzichtscamera bij de toegangspoort.

13.2 Uitvoering

Het juiste type intercom dient te worden gekozen uit de voorkeurslijst van RWS.

De volgende werkzaamheden dienen te worden uitgevoerd:

a. Het installeren van hoofdposten in de intercompost in de gebouwen. Vanaf deze hoofdposten dienen verbindingen te worden aangelegd naar de nevenposten in de zuilen bij de voertuigpoorten en bij de hoofdentreedeeuren die aan de openbare weg liggen. Ook dienen de hoofdposten te worden verbonden met de TzC. De hierbij noodzakelijk aansluitingen, kabellussen e.d. en programmeringen te worden gerealiseerd.

b. Het installeren van nevenintercomposten in de zuilen aan de buitenzijde van de poorten. Per zuil dient één nevenpost ten behoeve van gesprekken met autochauffeurs en één ten behoeve van gesprekken met vrachtwagenchauffeurs te worden geïnstalleerd. In totaal zijn dus twee nevenposten nodig per poort.

Nevenintercomposten op locatie moeten zijn uitgevoerd in RVS. Nevenintercomposten die in de kustprovincies worden geplaatst, dienen te zijn uitgevoerd in RVS 316 of voorzien van transparante roestwerende coating.

De nevenintercomposten zijn voorzien van een videocamera met een grote openingshoek van 135 graden of meer. De videocamera wordt ondersteund door extra verlichting uit de intercompost, zodat ook in de nacht een goed beeld kan worden getoond van de persoon die zich bij de intercom

heeft gemeld. De neven intercomposten zijn in staat om achtergrondgeluiden, zoals wegverkeer en draaiende (vrachtwagen)motoren, weg te filteren.

Het intercomsysteem is naar keuze full duplex of simplex in te regelen. Ook bij full duplex verkeer zal het achtergrond geluid niet de communicatie overstemmen.

Als op basis van de intercomoproep wordt besloten om de poort of deur te openen zal de functietoets op de intercompost aan de toegangscontrole de opdracht geven om de poort of deur te openen. Het intercomsysteem grijpt niet zelf in op de sturing van poort of deur. Het is mogelijk om door middel van verschillende functietoetsen de poort/deur gedeeltelijk te openen, volledig te openen, voor een bepaalde periode te openen of permanent open te sturen.

Deze functies zijn per hoofdpst, per functieknop vrij te programmeren

De intercomposten op locatie worden aangesloten op het intercomsysteem welke is geïntegreerd in het SMS van de TzC. Ook is het mogelijk om op de locatie zelf een hoofdintercompost te plaatsen.

Als er op de locatie een hoofdintercompost is geplaatst kan er een voorkeurschakeling worden geprogrammeerd. Deze schakeling kan een doorschakeling naar de TzC inhouden die wordt geactiveerd bij niet opnemen, na kantoortijden of bij afwezigheid.

De hoofdintercompost voorzien hiervoor in een selecteerbare afwezigheidsfunctie.

14 Specificaties Video Surveillance Systemen (VSS-en)

Ten behoeve van de observatie van de poort, de situatie langs de waterkant (en de afmeerplaatsen), langs de opstelplaatsen van strooiapparatuur en sneeuwschuivers en de serverruimten in de gebouwen, moet een VSS-systeem worden geïnstalleerd dat is gebaseerd op IP-technologie. Het systeem moet de centralisten in de TzC de mogelijkheid verschaffen om een goed overzicht te krijgen van de betreffende situatie. Ook moet het systeem na een alarmmelding volledig automatisch beelden van de betreffende alarmzone tonen aan de centralisten.

De resolutie van het systeem dient zodanig hoog te zijn dat de centralisten een gedetailleerd beeld van de betreffende zone wordt gepresenteerd. De minimum resolutie van de beveiligingscamera's bedraagt twee megapixel (1080p), voor de camera's van de video-intercom bedraagt deze één megapixel (720p).

Op de locaties zal middels bordjes moeten worden aangegeven dat er camerabewaking aanwezig is.

Binnen de RBKI zijn de volgende mogelijkheden beschikbaar.

14.1 VSS1

VSS1 bestaat uit verificatie van meldingen met behulp van een eenvoudig Video Surveillance Systeem en beeldopslag.

Op aangewezen steunpunten voert de TzC cameraverificatie uit. De locaties waar cameraverificatie wordt uitgevoerd en de frequentie ervan kan variëren en wordt per casus vastgesteld. De cameraverificatie kan worden ingesteld in verband met toegangsverlening, incidenten, een activiteit op de locatie of anderszins bepaald.

Voor het kunnen uitvoeren van het cameraverificatie dient de TzC de beschikking te hebben over de camerabeelden van de locaties. Hiervoor dienen de videocamera's op de locaties te worden aangesloten en opgenomen op een door het SMS van de TzC ondersteund videomanagement-platform.

Het SMS dient zo te zijn ingericht dat de centralist snel en eenvoudig de juiste locatie kan selecteren waarna de beschikbare cameraposities worden getoond op een plattegrond van de locatie en de desbetreffende camerabeelden worden weergegeven op een multiscreen. Indien de locatie over meer cameraposities beschikt dan er in het multiscreen kan worden getoond dan kan de centralist een keuze maken welke in het multiscreen getoonde camerabeelden te vervangen door de camerabeelden die op dat moment zijn/haar interesse hebben.

14.2 VSS2

VSS2 bestaat uit videodetectie op basis van Video Content Analyse (VCA) en Alarmverificatie met behulp van een Video Surveillance Systeem inclusief beeldopslag.

Voor het beveiligen van terreinen en kades maakt RWS gebruik van videomotiondetectie (VMD). Met behulp van deze detectie worden personen die zich in een vooraf gedefinieerd detectievlak bevinden door de VMD techniek gedetecteerd. De gevoeligheid van de detectie en de duur hoelang een persoon zich in het detectievlak bevindt voordat hij wordt gedetecteerd, zijn instelbaar.

Het systeem heeft een hoge mate van betrouwbaarheid en detectie zekerheid. Het systeem kan personen onderscheiden van voertuigen en (groepen van) klein wild (tot 35kg). Een persoon wordt gedetecteerd als deze zich in het detectievlak bevindt, ongeacht de houding van de persoon (staan, zitten, liggen, kruipen, rennen, etc).

Bij het detecteren van een persoon zal de VMD via het videomanagementplatform een contact schakelen in het lokale inbraaksignaleringssysteem voor alarmering naar TzC. De TzC kan hierop verifiëren of het over eigen personeel gaat of over een onbevoegd persoon.

De videobeelden waarop de VMD heeft besloten een alarm te genereren worden opgeslagen op de lokale opnameserver. De opname gaat vergezeld van pre- en post-alarmbeelden. De duur van de

pre- en post-alarmbeelden zijn vrij instelbaar per camera. Het moment van het alarm dat door het VMD op basis van de videobeelden is getriggerd, wordt visueel in een tijdsbalk in de videobeelden, zowel bij live als bij de opgenomen beelden, weergegeven.

In de videobeelden is duidelijk zichtbaar waar het alarm in het detectievlak is getriggerd, zowel het alarmbeeld als het detectievlak wordt weergegeven.

In de volgende paragrafen worden de technische eisen nader uitgewerkt.

14.3 Systeemconfiguratie

De volgende systeemdelen zijn te onderscheiden:

- a. De buitencamera's;
- b. De poortcamera's
- c. De intercomcamera's;
- d. De binnencamera's;
- e. De videotransmissie;
- f. De video-presentatiesystemen;
- g. Het video-registratiesysteem;
- h. Het cameraboek.

14.3.1 De buitencamera's

a. Algemeen. Alle camera's dienen te worden voorzien van objectieven, weerbestendige en waterdichte buitenbehuizingen (inclusief voeding en verwarming) en bevestigingsbeugels. De camera's dienen over een voldoende lichtgevoeligheid te beschikken om een goed beeld te kunnen geven bij de nachtelijke verlichtingssterkte op het terrein (20 lux op het grondoppervlakte). Slechts een enkele camera dient te hoeven bijgelicht met behulp van infrarood spots.

b. Uitvoering. De volgende werkzaamheden dienen te worden uitgevoerd:

- Het assembleren van camera's, objectieven, weerbestendige en waterdichte buitenbehuizingen (inclusief voeding en verwarming) en bevestigingsbeugels tot één geheel.
- Het monteren van de complete camera's op de gevels en in de masten, zoals in nauw overleg met de opdrachtgever dient te worden bepaald.
- Buitencamera's in de masten:
 - Alle buitencamera's moeten op minimaal vier meter hoogte in de masten worden aangebracht. De hierbij noodzakelijk aansluitingen, kabellussen en dergelijke dienen te worden gerealiseerd. De spanningsvoorziening van elke mast dient apart te worden gezekeerd zodat bij werkzaamheden aan een mast of aan de apparatuur erin, veilig spanningsloos kan worden gewerkt.
 - Aan één zijde van de camera's dient een IR-spot te worden geplaatst met een lichtbundel met een lengte en een openingshoek die tijdens een test nader moet worden bepaald. De spots moeten zijn voorzien van Leds die een infrarood golflengte uitstralen die overeenkomt met de golflengte waarvoor de buitencamera's in het zwartwit bereik het gevoeligst zijn. De levensduur van de IR-spots dient minimaal vijf jaar te bedragen bij een gemiddelde brandtijd van 12 uur per dag.
- Buitencamera's aan de gevel:
 - Enkele camera's moeten op de eerste verdieping (op een hoogte van tenminste 550 cm boven het maaiveld) aan de buitengevel van gebouwen worden aangebracht. De bevestigingsconstructie van de camera's moet worden uitgevoerd in RVS 316i of in thermisch verzinkt, zwart gemoffeld staal. De constructie moet worden bevestigd met behulp van chemische ankers in de gevelelementen. De uitvoering van de ophangconstructie en de wijze van de bevestiging dient vooraf ter goedkeuring aan de opdrachtgever te worden voorgelegd.

Alle noodzakelijk aansluitingen, kabellussen e.d. dienen te worden gerealiseerd. De kabels moeten worden ingevoerd in het plenum van het plafond en mogen niet zichtbaar op de gevel zijn. De buitenbekabeling moet worden weggewerkt in de bevestigings-constructie. De kabeldoorvoeren door de gevel dienen waterdicht te worden uitgevoerd.

- Aan één zijde van de camera's dient een IR-spot te worden geplaatst met een lichtbundel met een lengte en een openingshoek die tijdens een test nader moet worden bepaald. De spots moeten zijn voorzien van Leds die een infrarood golflengte uitstralen die overeenkomt met de golflengte waarvoor de buitencamera's in het zwartwit bereik het gevoeligst zijn. De levensduur van de IR-spots dient minimaal vijf jaar te bedragen bij een gemiddelde brandtijd van 12 uur per dag.
 - Direct na de ingebruikname van het VSS-systeem dient gedurende minimaal een week 's-avonds en 's-nachts te worden bekeken of de infrarood spots voldoende licht produceren om de camera's een goed beeld te laten produceren. Indien de kwaliteit van de beelden in het donker niet voldoende is, dient in nauw overleg met de opdrachtgever proefondervindelijk een aantal IR-spots te worden bijgeplaatst.
 - Vanaf de camera's dienen glasvezelkabels te worden aangelegd naar de Security Techniekrimte. De te overbruggen afstanden moeten tijdens een schouw worden bepaald.
- c. Technische specificaties van de buitencamera's. De buitencamera's dienen te worden geselecteerd uit de 'CamIQCompatibilitylist.pdf' van RWS en dienen minimaal te voldoen aan de specificaties die hieronder zijn vermeld.
- **Elektrisch:**
 - Videostandaard - H.264 of hoger én M-JPEG
 - Voedingsspanning: - 230 Vac ± 15%
 - MTTF - > 80.000 u
 - MTTR - < 180 minuten.
- d. Buitenbehuizing. Aan de buitenbehuizing van de camera's worden de volgende eisen gesteld:
- Boxbehuizing, IP66, UV-bestendige kap, inclusief voeding 230 Vac-12 Vdc en ingebouwde verwarming.
 - Voorzien van de door de fabrikant voorgeschreven bevestigingsbeugels.
 - Bij installatie te voorzien van anti-spinnen spray, rondom de behuizing (10 cm).
 - Het aanbrengen van de anti-spinnen spray moet met jaarlijks onderhoud worden herhaald.
- e. Cameramasten. Een aantal buitencamera's dient te worden bevestigd in cameramasten. De volgende aandachtspunten dienen in acht te worden genomen:
- De masten moeten van het type kantelmast zijn en dusdanig zijn geplaatst dat de masten vrijelijk gekanteld kunnen worden.
 - De masten moeten tenminste vier meter hoog zijn.
 - Ze dienen te worden voorzien van een inklimbeveiliging en een opzetstuk of beugel ten behoeve van de plaatsing van één camera.
 - De fundering en de stijfheid van de masten moet zijn aangepast aan de gemiddelde windbelasting.
 - Alle masten moeten worden voorzien van een overspanningsbeveiliging, maar er mag niet worden gekozen voor bliksempieks.

14.3.2 De poortcamera's

Algemeen. De poortcamera's dienen te worden gemonteerd bovenin cameramasten met een lengte van tenminste 400 cm. Voor de overige specificaties: zie §14.3.1.

14.3.3 De intercomcamera's

- a. Algemeen. Alle intercomcamera's dienen te zijn voorzien van geïntegreerde objectieven die een openingshoek bieden van minimaal 135 graden horizontaal, de oplossing dient weerbestendige te zijn uitgevoerd (IP66). De camera's dienen over een voldoende lichtgevoeligheid te beschikken om een goed beeld te kunnen geven bij de nachtelijke verlichtingssterkte op het terrein. Indien noodzakelijk bijgevoerd met behulp geïntegreerde (infrarood) verlichting. De

videobeelden van de intercomcamera's dienen te worden opgenomen op het lokale video-registratiesysteem die compatible is met de aansluitvoorwaarden van de TzC.

b. Uitvoering. De volgende werkzaamheden dienen te worden uitgevoerd:

- Het monteren van de complete video-intercom units in de zuilen.
- Vanaf de video-intercom units dienen glasvezelkabels te worden aangelegd naar de (Security) Techniekruimte. De te overbruggen afstanden kunnen uit de plattegronden worden herleid.

c. Technische specificaties van de intercomcamera's. De intercomcamera's dienen minimaal te voldoen aan de specificaties die hieronder zijn vermeld.

• **Elektrisch:**

Videostandaard	- H.265 én M-JPEG
<u>Voedingsspanning:</u>	- 12 Vdc $\pm$ 15%
MTTF	- > 40.000 u
MTTR	- < 180 minuten.

d. Buitenbehuizing. Aan de behuizing van de intercomcamera's worden de volgende eisen gesteld:

- Behuizing, IP66, UV-bestendige kap, inclusief voeding.
- Voorzien van de door de fabrikant voorgeschreven bevestigingsbeugels.
- Bij installatie te voorzien van anti-spinnen spray, rondom de behuizing (10 cm).
- Het aanbrengen van de anti-spinnen spray moet met jaarlijks onderhoud worden herhaald.

14.3.4 *Het video-transmissiesysteem*

Om de beelden van de diverse camera's te kunnen routeren naar de lokale videoserver, dient gebruik te worden gemaakt van een door de opdrachtnemer te leveren en installeren securitynetwerk. De aansluiting van de videoserver op de TzC dient te gebeuren conform de aansluitvoorwaarden zoals zijn vermeld in de externe bijlagen Aansluitvoorwaarden TzC:

- CamIQCompatibilitylist.pdf;
- Compatibiliteit Informatie bulletin RWS Toezicht Centrale v1.1.pdf;
- Koppelingen SecuriNet.pdf.

De netwerkbekabeling dient door de opdrachtnemer in het kader van de opdracht te worden aangelegd. Het netwerk moet uit de volgende apparatuur bestaan:

- Glasvezelbekabeling tussen de gebouwen en buiten opgestelde beveiligingsapparatuur.
- Glasvezelbekabeling tussen de switches onderling.
- Glasvezelbekabeling naar en van de centrale apparatuur in de Security Techniekruimten.
- Cat 6 netwerkbekabeling tussen de switches en de overige apparatuur.
- Switches voor Gigabit netwerken.
- Voor apparatuur welke buiten wordt geplaatst en niet rechtstreeks op glasvezel kan worden aangesloten dient er in een bouwkundig en elektronisch beveiligde behuizing een mediaconverter te worden opgenomen. Het gebruik van meervoudige mediaconverters is enkel toegestaan als dit een door RWS toegelaten manageble switch betreft.
- Een lokale videoserver.

14.3.5 *De video-presentatiesystemen*

Bij bemande steunpunten kunnen de beelden ook lokaal bij de receptie of in het kantoor in het steunpunt worden getoond op de intercompost. De weergave is naar keuze in te stellen in een volbeeld (24"-monitor) van één camera of een multiscreen van twee of meer camera's, waarbij de indeling per locatie vrij is te definiëren.

Om de camerabeelden door centralisten in de TzC te kunnen laten bekijken, dient in nauw overleg met de opdrachtgever een verbinding te worden gemaakt tussen het lokale VSS en de apparatuur in de TzC.

14.3.6 Het video-registratiesysteem

De camerabeelden worden op de locatie zelf opgenomen, dit kan op een centrale opnameserver in een gebouw of in de camera zelf, een en ander afhankelijk van de mogelijkheden van de beveiligingscamera en de ondersteuning binnen het videomanagementplatform. De oplossing moet in ieder geval rekening houden met de bandbreedte beperkingen op de RWS locaties.

Indien er minder bandbreedte beschikbaar is, zal het videomanagementplatform het bandbreedte gebruik automatisch moeten beperken. Bij het uitkijken van de opgenomen videobeelden kunnen bepaalde situaties worden gemarkeerd als "te bewaren". De gemarkeerde videobeelden worden dan door het videomanagementsysteem in volledige resolutie naar de centrale omgeving in de TzC gehaald voor verdere verwerking, ter autorisatie door het Team Safety & Security. Door eventuele bandbreedte beperkingen kan dit enige tijd in beslag nemen.

Het videomanagementsysteem arrangeert de overdracht op een dusdanige wijze, dat de dagelijkse bedrijfsvoering hier geen hinder van ondervindt. De opnameserver op locatie wordt voorzien van een raid configuratie, waardoor er bij uitval van één harde schijf geen videobeelden verloren zullen aan en het systeem nog operationeel blijft.

Uitval van een harde schijf of andere hardware storingen (oplopen temperatuur, uitval ventilator etc.) worden aan het SMS van de TzC gemeld.

Om corruptie van de opnameserver tegen te gaan, wordt de opnameserver voorzien van een UPS. Hiervoor is het noodzakelijk dat de netspanningsuitval door de UPS wordt gedetecteerd en dit aan de opnameserver meldt, zodat deze gecontroleerd kan afsluiten. Deze actie wordt door de opnameserver aan het SMS van de TzC gemeld, alvorens daadwerkelijk af te sluiten. Bij herstel van de netspanning zal de opnameserver automatisch weer in operationele staat moeten opstarten, zonder menselijke tussenkomst.

De videoregistratie vindt plaats met behulp van een netwerk videorecorder (NVR). De complete hard- en software van dit systeem, dient in nauw overleg met de opdrachtgever te worden geplaatst in een door de opdrachtgever te bepalen (security) techniekruimte.

a. De lokale server. De lokale server van het systeem dient in de (security) techniekruimte te worden geplaatst. Voor de verbinding tussen de camera's en de server, dient gebruik te worden gemaakt van glasvezelkabels. Er moet een berekening te worden gemaakt en geleverd van de opslagcapaciteit voor de opslag van de camerabeelden gedurende 28 dagen.

b. Op te nemen parameters. Iedere opname dient tenminste de navolgende alfanumerieke gegevens te bevatten:

- De datum en het tijdstip van de opname.
- Het nummer van de registrerende camera en de bijbehorende zonenaam.
- Een onzichtbaar watermerk, waarmee achteraf de authenticiteit van een opname kan worden vastgesteld.

c. Bekijken van opgenomen beelden. De centralisten moeten vanuit de TzC de opgenomen beelden kunnen bekijken.

d. Opslaan van beelden. Team Safety en Security moet op afstand een selectie van de beelden kunnen downloaden om vervolgens op een USB-stick of externe harddisk op te kunnen slaan.

14.3.7 Het cameraboek

Na installatie van alle camera's dienen de beelden van de camera's in nauw overleg met de opdrachtgever te worden ingesteld conform het "Uitvoeringsprotocol cameratoezicht". Hierin staat verwoord onder welke voorwaarden, conform AVG, het cameratoezicht is geoorloofd in welke ruimten.

Van de door de opdrachtgever gewenste camerabeelden dienen hoge resolutie kleurenafdrukken te worden gemaakt. Deze afdrukken moeten in de vorm van een cameraboek ter accordering aan de opdrachtgever te worden overlegd om te bepalen of bepaalde zichtvelden van de camera's dienen te worden geblurred. Na accordering dienen de foto's digitaal te worden opgeslagen in een door de opdrachtgever te bepalen database.

15 ToezichtCentrale (TzC)

De ToezichtCentrale (TzC) van RWS vervult de dienstverlening voor toegangsverlening op afstand en alarmverificatie en -afhandeling, voor de Wegen- en Watersteunpunten en monumentale Vuurtorens.

De werkzaamheden betreffen:

- Toegangsverlening op afstand
Bij toegangsverlening op afstand controleert de centralist van de ToezichtCentrale of de persoon bij de ingang op identiteit en of er inderdaad toestemming is om het terrein te betreden. De centralist voert de volgende handelingen uit:
 - De persoon meldt zich aan via videointercom bij het object.
 - Er wordt een verbinding opgebouwd met de TzC en de centralist staat de persoon te woord.
 - Tegelijkertijd wordt de video verbinding ook opgebouwd zodat de centralist kan meekijken wie bij de intercom staat.
 - Na verificatie wordt de ingang/toegang vrijgegeven tot het object.
- Reageren op inbraakmeldingen:
De inbraaksignaleringsystemen op de steunpunten worden aangesloten op het Security Management Systeem van de TzC. Alle statusveranderingen, storingen en alarmmeldingen worden aan het SMS gemeld, daar geprioriteerd en ter afhandeling aan de centralist aangeboden. De centralist wordt in de afhandeling en interpretatie van de melding begeleid door de opvolgingsprotocollen, die in het SMS zijn vastgelegd. Voor iedere processtap in de opvolging zijn duidelijke instructies vastgelegd. Waar mogelijk wordt de centralist geautomatiseerd door het SMS ondersteund. Zo zal er bij een inbraakmelding direct en automatisch alle relevante beschikbare camerabeelden worden getoond, zowel live als een instant weergave van de camerabeelden ten tijde van het alarm. Op deze wijze kan de centralist een gedegen afweging maken van de melding en deze op de juiste wijze afhandelen.
Ten einde het verifiëren van inbraakmeldingen mogelijk te maken dient het SMS naast de omschreven videoverificatie ook het technisch verifiëren van meldingen mogelijk te maken. Het technisch verifiëren van meldingen geschiedt op basis van de ontvangst van twee of meer alarmmeldingen afkomstig van twee of meer verschillende inbraaksensoren.
- Begeleid openen en sluiten van Steunpunten en Vuurtorens
De TzC begeleidt RWS medewerkers op aanvraag bij het openen of sluiten van de locatie door middel van cameratoezicht. Een RWS medewerker kan de TzC telefonisch of via de intercom bij de toegangspoort vragen om extra toezicht te houden als de RWS medewerker zich niet veilig voelt.

16 Het Security Network (SN)

16.1 Algemeen

Ten behoeve van de verbindingen tussen alle beveiligingssystemen onderling en naar de TzC en TzC dient een Security Network (SN) te worden aangelegd. Dit netwerk bestaat uit een intern netwerk en een extern netwerk.

Een overzicht van de voor iedere locatie aanwezige bandbreedte is bekend bij team Safety & Security. In dit overzicht staat ook een schatting van de voor de beveiligingssystemen totaal benodigde bandbreedte. De opdrachtnemer dient deze schatting te controleren op basis van de benodigde bandbreedte voor de door hem aan te bieden beveiligingssystemen. Daar waar extra bandbreedte noodzakelijk is, dient opdrachtnemer in nauw overleg met de afdeling CIV van RWS deze extra bandbreedte te realiseren.

Het beveiligingsnetwerk is in beheer van RWS. De actieve apparatuur (switches, routers, etc) worden door RWS geleverd. Aanleg van de infrastructuur (netwerkbekabeling, glasvezel, patchkasten, etc) is voor de verantwoording van de beveiligingsinstallateur.

Voor de netwerkinfrastructuur wordt minimaal een Cat5e netwerk geïnstalleerd, het netwerk dient te worden afgewerkt in een patchkast op een patchpaneel. Aan het end-point wordt de bekabeling afgemonteerd op een wall-outlet. Indien het een aansluiting betreft voor een apparaat die aan de buitengevel wordt gemonteerd zal de wall-outlet aan de binnenzijde worden gemonteerd en het apparaat middels een patchsnoer worden aangesloten. Daar waar het apparaat aan de buitengevel van het gebouw wordt gemonteerd is netwerkaansluiting door de beveiligingsinstallateur voorzien van een galvanische scheiding of overspanningsbeveiliging.

Het beveiligingsnetwerk dat zich buiten en tussen de gebouwen bevindt is uitgevoerd als multimode glasvezel. De glasvezelkabel is aan beide zijde afgewerkt op een glasvezelpatchpaneel en voorzien van de door de fabrikant voorgeschreven trekcontlastingen.

Daar waar het niet mogelijk is om de apparatuur buiten de gebouwen rechtstreeks aan te sluiten op glasvezel zal er in overleg met RWS gezocht worden naar een goed alternatief zoals mediaconverters of netwerkswitches.

De mediaconverters of switches zijn gemonteerd in de behuizing van het netwerkapparaat. De behuizing is dan voldoende inbraakwerend en voorzien van sabotagedetectie.

Beide netwerken, glasvezel en Cat5e, worden gecertificeerd en voorzien van een meetrapport opgeleverd. Het aansluiten (patchen) van de apparatuur wordt door de beveiligingsinstallateur uitgevoerd op basis van de door RWS opgestelde patchlijsten.

Het beveiligingsnetwerk is door RWS per onderdeel ingedeeld in virtuele netwerken. Eventuele interactiviteit tussen systeemonderdelen wordt op centraal niveau geregeld. Interactiviteit op locatie kan alleen worden gerealiseerd op basis van een hardware-matige koppeling.

Alle apparatuur die wordt aangesloten op het beveiligingsnetwerk moet geschikt zijn voor 802.1x EAP-TLS authenticatie. Deze authenticatie zal in de toekomst boven op de MAC authenticatie worden uitgevoerd.

De serverruimte dient via één centrale Windows NTP server wordt het time synchronisatie voor RWS Rijkspas VPN centraal bijgehouden voor alle aangesloten apparatuur.

17 Het Security Management Systeem (SMS)

17.1 Algemeen

Het beheer van de beveiligingssystemen vindt plaats met behulp van het Security Management Systeem 'SecuriNet' van de firma Hisec. De beveiligingssystemen dienen in nauw overleg met de opdrachtgever te worden aangesloten op het SMS. De gegevens voor de aansluiting op SecuriNet staan vermeld in de 'Aansluitvoorwaarden TzC'.

18 Overige specificaties

18.1 De voedingsspanningsvoorziening

18.1.1 De nominale voedingsspanning

De complete beveiligingsapparatuur dient te kunnen worden aangesloten op de lokale netspanningsvoorziening met de volgende specificaties: 230V AC +10%; 50Hz +5%. De aansluiting op de spanningsinstallatie dient door de opdrachtnemer in zeer nauw overleg met de opdrachtgever te gebeuren.

18.1.2 Aarding

Alle aarding, benodigd voor het goed en veilig functioneren van de beveiligingssysteem dienen door de opdrachtnemer conform het gestelde in NEN 1014 te worden verzorgd in nauw overleg met de opdrachtgever.

18.1.3 Overspanningsafleiding

De aan te brengen overspanningscomponenten dienen te worden geïntegreerd in het reeds bestaande overspanningsbeveiligingssysteem van TenneT. Hiertoe dient voorafgaand aan de werkzaamheden nauw overleg tussen de opdrachtnemer en de opdrachtgever plaats te vinden.

Daar waar de kabels voor de elektrische voeding van de mastcamera's het gebouw worden ingevoerd, dient een overspanningsafleiding van 6kV met afstandssignalering, alsmede een overspanningsafleiding van 2kV op de kabels te worden aangebracht.

De elektrische voeding van de centrale VSS-apparatuur en de camera's, alsmede de netwerkkabels van de buitencamera's dienen te worden voorzien van een overspanningsafleiding van 2kV.

De wandcontactdozen ten behoeve van de voedingsaansluiting van de centrale apparatuur moeten zijn voorzien van een overspanningsafleiding voor spanningen vanaf 250V AC. De netwerkkabels van de buitencamera's dienen bij de switches te worden voorzien van een overspanningsafleiding voor spanningen vanaf 250V AC.

Bijlage 1 RWS-CD RBKI

De Basis Security Niveaus voor de verschillende risicoklassen zijn in onderstaande tabel 'RWS-CD Beveiligingsklassen' weergegeven. Op basis van de relevante securityrisico's en relevante algemene incidentscenario's is per niveau een beveiligingsmaatregelenpakket samengesteld, dat aan de security-eisen voor dat niveau zou moeten kunnen voldoen.

Deze tabel is integraal overgenomen uit het Kader Wegen- en Watersteunpunten en monumentale Vuurtorens, dit Kader-document is altijd leidend.

RBK	BSN	Terrein	Gebouw Beveiligingsmaatregelen
1	0#	O1 O1 + T1 + VSS1	1a*: O1 1b: O1 + BK1 + EL2 + AT2 + RE2
2	0	O1 O1 + T1 + VSS1	2a*: O1 2b: O1 + BK1 + EL3 + AT2 + RE2 + CO3 en/of ME3 2c**: O1 + BK2 + EL2 + AT2 + RE2 2d: O1 + BK2 + EL2 + AT2 + RE2 + CO2 en/of ME2 2e***: O1 + ME3 en/of VSS2 met RE3
3	1	O2 O2 + T2 + VSS1	3a*: O1 3b: O2 + BK1 + EL3 + AT3 + RE3 + CO3 en/of ME3 + VSS2 3c: O2 + BK2 + EL3 + AT3 + RE3 + SD2 + CO3 en/of ME3 3d**: O2 + BK3 + EL3 + AT3 + RE3 + SD2 3e**: O2 + BK3 + EL3 + AT3 + RE3 + VSS2 3f***: O2 + ME3 en/of VSS2 met RE3
4	2	O2 + T2 + VSS1	4a*: O1 4b: O2 + BK3 + EL3 + AT3 + RE3 + VSS2 + SD2 4c: O2 + BK3 + EL3 + AT3 + RE3 + CO3 en/of ME3 4d***: O2 + ME3 en/of VSS2 met RE3

Tabel: RWS-CD Beveiligingsklassen Indeling (RBKI)

Legenda

a t/m f Varianten van beveiligingsmaatregelen

- *: Van toepassing voor zoutopslag of opslag van boeien
- **: Niet toepassen bij goederen met een hoge attractiviteit, zoals gespecificeerd
- ***: Van toepassing bij bijvoorbeeld buitenopslag van materiaal en machines, en als virtueel hekwerk (m.b.v. camera's) bij afmeerplaatsen

O1 Standaard Organisatorische maatregelen conform de VRKI 2.0

O2 Standaard plus aanvullende (locatie specifieke) O-maatregelen (conform de VRKI 2.0)

T1 Een hekwerk of een muur met een hoogte van tenminste 180 cm boven maaiveld, een haag van 'Stuver-beplanting'¹ met een breedte van minimaal 300 cm en een hoogte van 120 cm boven maaiveld of een sloot met een breedte van de waterspiegel minimaal 300 cm, voorzien van een poort van minimaal 180 cm hoogte

¹ Stuver: STUrende en VERtragende beplanting; door toepassing van een specifieke mix van beplanting en in combinatie met de juiste breedte en hoogte ervan, wordt een natuurlijke barrière gerealiseerd.

T2	Een hekwerk of een muur met een hoogte van tenminste 220 cm boven maaiveld, een haag van 'Stuver-beplanting' ¹ met een breedte van minimaal 500 cm en een hoogte van 120 cm boven maaiveld of een sloot met een breedte van de waterspiegel minimaal 500 cm, voorzien van een poort van minimaal 220 cm hoogte
BK1	Bouwkundige maatregelen met functionerend hang- en sluitwerk en goede kwaliteit van de gevelelementen*
BK2	3 minuten braakwerend*, weerstandsklasse 2 NEN-EN 1627:2021; of 3 minuten braakwerend* conform PKVW
BK3	5 minuten braakwerend*, weerstandsklasse 3 NEN-EN 1627:2021
BK4	10 minuten braakwerend*, weerstandsklasse 4 NEN-EN 1627:2021
EL2	Detectiesysteem bestaande uit VRKI EL2 met aanvullingen conform PvE RWS, in combinatie met een Elektronisch Toegangsbeheerssysteem
EL3	Detectiesysteem bestaande uit VRKI EL3, met aanvullingen conform PvE RWS, in combinatie met een Elektronisch Toegangsbeheerssysteem
SD2	Schildetectie voor bereikbare vaste en beweegbare gevelelementen, wanden, vloeren en daken
VSS1	Bieden van overzicht bij de situatie aan de poort en in de serverruimte met behulp van een eenvoudig Video Surveillance Systeem en beeldopslag
VSS2	Videodetectie op basis van Video Content Analyse (VCA) en Alarmverificatie met behulp van een Video Surveillance Systeem inclusief beeldopslag
CO2	Inbraakwerende safe of bouwkundige compartimentering, 3 minuten braakwerend, met detectie buiten het compartiment
CO3	Bouwkundig compartiment, 5 minuten braakwerend, met detectie buiten het compartiment
ME2	Meeneembeperkende maatregelen, Prestatie-eis: 3 minuten diefstalvertraging
ME3	Meeneembeperkende maatregelen, Prestatie-eis: 5 minuten diefstalvertraging
AT2	DP1 Grade 2 alarmtransmissie
AT3	DP3 Grade 3 alarmtransmissie
RE2	Reactie door één of meerdere mobiele surveillance
RE3	Reactie door één of meerdere mobiele surveillance en politie

* de bereikbaarheid wordt bepaald aan de hand van de NEN 5087.

Bijlage 2 RBK Tabel – Specifieke objecten

RWS BEVEILIGINGSKLASSEN INDELING (RBKI)					
Objectsoort		Objectsoort		Objectsoort	
Gebouwsoort		Gebouwsoort		Gebouwsoort	
Ruimte	RBK	Ruimte	RBK	Ruimte	RBK
Wegensteunpunten		Watersteunpunten		Historische Vuurtorens	
Opslagruimte / voertuigstalling:		Opslagruimte / voertuigstalling:		Opslagruimte van:	
> € 150.000	3	> € 150.000	3		
> € 300.000	4	> € 300.000	4		
Patchkastruimte	2	Patchkastruimte	2	Patchkastruimte	2
ICT-netwerkknooppunt	3	ICT-netwerkknooppunt	3	Zeeverkeersruimte	3
		NSA primair object	3		
		Reserve sluisonderdelenopslag	3		
		Missie Kritische Onderdelen	3		
Derden		Derden		Derden	
		Politieboot			
Noot 1: Bij meerdere functionaliteiten in één ruimte, bepaalt de zwaarste wegende RBK de RBK van de hele ruimte.					

Patchkast: 19' inch rack met ICT-apparatuur.
 Patchkastruimte: ruimte waarin de patchkast staat.

Bijlage 3 Stuver-soorten

OVERZICHT STURENDE EN VERTRAGENDE BEGROEIING **(STUVER)**

Monocultuur: (inheems)	1. Meidoorn 2. Sleedoorn 3. Wegedoorn 4. Duindoorn
Mengsels: (inheems)	5. Meidoorn, Robinia, Roos (rankend) en Braam 6. Duindoorn en Meidoorn 7. Duindoorn, Braam en Veldesdoorn 8. Sleedoorn, Roos (rankend) en Robinia 9. Veldesdoorn, Sleedoorn, Duindoorn en Braam 10. Meidoorn, Veldesdoorn, Wegendoorn en Hondstroos
Monocultuur: (uitheems)	11. Vuurdoorn Pyracantha 12. Berberis Julianaea 13. Berberis Baggregata 14. Robinia Pseudoacacia 15. Picea Sitchensis
Mengsels: (uitheems)	16. Chaenomelis Cathayensis, Berberis Julianaea en Meidoorn 17. Rosa Rubiginosa, Vuurdoorn, Veldeshoorn en Robinia 18. Berberis Stenophylla, Hulst (Siberica) en Meidoorn 19. Berberis Thunbergii, Vuurdoorn, Rosa Multiflora en Robinia 20. Rosa Virg Harvest Song, Rosa Canina en Rosa Rubiginosa