Interpretatiedocument

Monitoring en Alarmontvangstcentrales & Alarm Transmissie Service Providers

Goedgekeurd door het College van Deskundigen Security

06-06-2024

Trust
Quality
Progress

Kiwa Nederland B.V.
Kiwa FSS Certification
Dwarsweg 10
5301 KT Zaltbommel
The Netherlands

Tel. +31 88 998 51 00
NL.info.fss@kiwa.com
www.kiwafss.nl

Inhoudsopgave

Versiegeschiedenis

Versie	Wijziging	Datum
1	Eerste opzet van het document	2020/05/27
2	Toevoegen van VSS Control Room	2020/07/31
3	Toevoegen items vanuit het CvD	2020/09/09
4	Aanpassing na overleg CvD	2021/10/02
5	Gecombineerde wijzigingen na vergaderingen College van deskundigen Security	2022/11/17
6	Wijziging reactietijden en business continuïteit na CvD 03-2023	2023/03/27
7	Wijziging samenstelling CvD en toevoegen guidance op remote access/apps en portals.	2024/0606

1 Introductie

Dit interpretatiedocument is van toepassing op de internationale normen voor inspectie en certificering van EN 50518 monitoring- en alarmontvangstcentrales (MARC) en K21030 alarmtransmissiedienstverleners (ATSP) en is geaccepteerd door het College van Deskundigen Security, waarin alle relevante partijen in het gebied van beveiliging zijn vertegenwoordigd. Het College van Deskundigen houdt ook toezicht op de werkzaamheden en eist indien nodig dat deze scope wordt herzien en bepaalt wanneer aanvullende interpretatie nodig is.

Het College van Deskundigen security bestaat uit de volgende personen:

Board of Experts Security		
Bert Bambach	Avans Hogeschool	Voorzitter
John van Schaik	M2M Services	Leverancier
Ronald van Duijn	ENAI	Leverancier / ATSP
Mathijs de Vaal	Protify	Advisering
Iwan Debets	ASB Security	Leverancier / ATSP / MARC
Robèrt Wijmans	Verisure	Leverancier / MARC
Rens Krijgsman	KOP Beveiliging	Installateur
Jurjen Burghgraef	JBRisicobeheer	Risico beoordelaar
Bram Vandenbergen	NVD Beveiligingen	MARC
Erwin Schoemaker	Federatie Veilig Nederland	Branche
Kim van Heemskerk-Grimbergen	Nationale Politie	Politie
Jan Willem Verwoert	Kiwa FSS Testing	Certificeringsinstelling
Albertine Ibrahim	Kiwa FSS Testing	Certificeringsinstelling
Peter Voshol	Kiwa FSS Certification	Certificeringsinstelling
Mischa van der Geld	Kiwa FSS Certification	Certificeringsinstelling
Dio Kock	Kiwa FSS Certification	Certificeringsinstelling/Secretaris

Tabel 1; Leden college van deskundigen security

Technologische ontwikkelingen wachten niet op wet- en regelgeving en normen. Deze wetten, voorschriften en normen volgen de ontwikkelingen. Dit "interpretatiedocument" belichaamt de technologische en marktontwikkelingen. Het doel van dit document is om de context te verduidelijken door nieuwe definities op te stellen over bepaalde thema's en onderwerpen. Dit maakt voor personen en marktpartijen duidelijk wat de randvoorwaarden zijn bij het vaststellen van de naleving van de geldende eisen. Ook wordt uitgelegd welke ontwikkelingen spelen op het niveau van normen en hoe deze aansluiten bij de ontwikkelingen in de markt en aansluiten bij wet- en regelgeving.

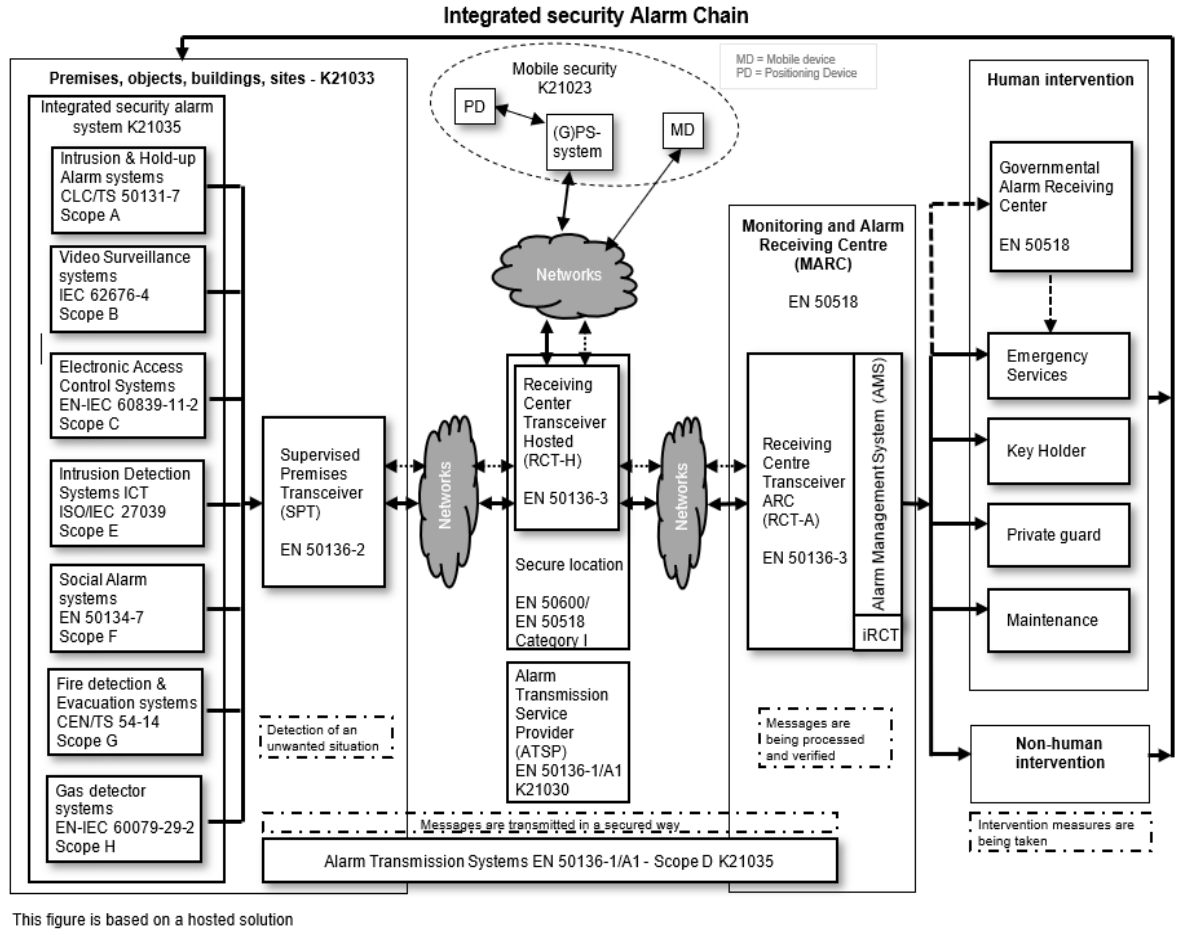
Dit interpretatiedocument is opgesteld om twee doelen te stellen:

- Richting geven in het kader van ontwerp, installatie en bediening van systemen en is gemarkeerd met de letter “G”;
- Om aanvullende of alternatieve vereisten te geven over zaken die niet duidelijk zijn gedefinieerd in de normen of waar de normen het probleem of de ontwikkeling nog niet hebben aangepakt en is gemarkeerd met de letter "R".

1.1 Geintegreerde beveiligingsalarmketen

Op de volgende pagina is de geïntegreerde beveiligingsalarmketen getekend zoals gezien door Kiwa FSS. Uitleg:

1. Links genereert een alarmsysteem in een pand, object, gebouw of terrein een alarm. Dit alarm wordt vervolgens verzonden via een Supervised Premises Transceiver (SPT). Dit alarmsysteem en SPT zijn geïnstalleerd in overeenstemming met certificatieschema K21049/K21035: Beveiligingsalarmsystemen.
2. Bij een gehoste oplossing geldt een veilige datalocatie. In dat geval communiceert een Receiving Center Transceiver-Hosted (RCT-H) met een interface Receiving Center Transceiver (iRCT). Dit valt onder de verantwoordelijkheid van een Alarm Transmission Service Provider (ATSP).
3. Het alarm komt nu in het MARC-proces, de ARC verifieert het alarm en heeft dan twee opties: menselijke interventie of niet-menselijke interventie.
4. Een mobiel apparaat of een positioneringsapparaat kan ook een alarm genereren dat in een MARC terechtkomt.



Figuur 1

Hieronder vindt u een schema met de Europese normen en de bijbehorende verantwoordelijkheden.

Rollen gedefinieerd in de beveiligingsketen				
Installateur		Alarm Transmissie Service Provider		Monitoring and Alarm Receiving Centre
Van toepassing zijnde Europese normen in de beveiligingsalarmketen				
EN 50131 / TS54-14 / etc / Alarmsystemen op het terrein of object	⇨	EN 50136-1/A1 Alarm transmissie	⇨	EN 50518 Alarmafhandeling door de ARC
Audit door Kiwa gebaseerd op certificatie schema:				
Installateur geïntegreerde veiligheids- en beveiligingsoplossingen K21049/K21035	⇨	Alarm transmissieservice provider (ATSP) K21030	⇨	EN 50518 met van toepassing zijnde scopes
Verantwoordelijkheden				
Alarm systeem + doormeldeenheid (SPT)	⇨	Configuratie ATS, testen van initiële & periodieke SPT & RCT & rapportage aan cliënt	⇨	AMS + RCT periodieke rapportage door de MC

Figuur 2

2 Categorieën en scopes “G”

De meeste landen in Europa stellen eisen aan de werking van alarmontvangstcentra (ARC). Bijna al deze landen verwijzen naar de norm EN 50518 voor ‘Monitoring & Alarm Receiving Centers’. De eerste versie van deze Europese norm is gemaakt in 2010 en op dit moment is de EN 50518 tot zijn derde versie gekomen.

Vanaf augustus 2019 is de derde versie van de norm EN 50518 geïntroduceerd. Deze vervangt EN 50518 deel 1, 2 en 3 uit 2013. Nieuwe ARC’s worden vanaf 6-2-2019 beoordeeld op de nieuwe norm. Huidige (M)ARC's moeten uiterlijk op 6-2-2022 aan de nieuwe norm voldoen.

De norm EN 50518 vereist certificering onder accreditatie in de 2013- en 2019-versie. Dit betekent dat als de eis wordt gesteld om te voldoen aan deze norm, certificering onder accreditatie verplicht is. De accreditatie die van toepassing is voor EN 50518 is de EN-ISO/IEC 17065. Deze accreditatie-norm schrijft in art. 3.10 ‘scope of certification’. Hiermee maakt de certificatie-instelling duidelijk voor welke producten, processen of diensten de certificering van toepassing is. Dit komt ten uiting in de certificatie-overeenkomst, in de auditrapportage en op het certificaat.

Certificering voor EN 50518 is gebaseerd op de norm met zijn vereisten voor de constructie-elementen, systemen en processen van een ARC. Daarnaast biedt EN 50518 meerdere scopes voor het verwerken van verschillende soorten berichten. Deze berichten zijn onderverdeeld in twee categorieën:

- Categorie I: ARC’s die berichten afhandelen van security toepassingen
- Categorie II: ARC’s die berichten afhandelen van niet-security toepassingen

De EN 50518 specificeert welk soort berichten tot welke categorie behoren. Het volledige overzicht van de per categorie genoemde scopes wordt hieronder beschreven. De tweede kolom koppelt het toepassingsgebied aan de van toepassing zijnde norm die wordt vermeld in EN 50518. Waar geen norm wordt genoemd, heeft het College van Deskundigen verwezen naar een specificatie. De scopes die worden uitgevoerd door het ARC worden na certificering vermeld op hun certificaat.

Scopes category I	**Van toepassing zijnde norm**
Alarm Receiving Centre (ARC) for Intrusion & Holdup Alarm systems (I&HAS) *(Alarmontvangstcentrale voor inbraak en overvalsystemen (I&HAS)*	TS 50131-7
Alarm Receiving Centre (ARC) for Video Surveillance Systems (VSS) for security applications *(Alarmontvangstcentrale voor videotoezichtsystemen (VSS) voor security doeleinden)*	EN-IEC 62676-4
Alarm Receiving Centre (ARC) for Access Control Systems (ACS) for security applications *(Alarmontvangstcentrale voor toegangscontrolesystemen (ACS) voor security doeleinden)*	EN-IEC 60839-11-2

Alarm Receiving Centre (ARC) for people monitoring, lone workers and object tracking systems for security applications *(Alarmontvangstcentrale voor persoonsbeveiliging, alleenwerkers en object traceersystemen voor security doeleinden)*	K21023 enkel indien het aangesloten platform gecertificeerd is conform K21023
Scopes category II	
Alarm Receiving Centre (ARC) for Fire Alarms Systems (FAS) *(Alarmontvangstcentrale voor branddetectiesystemen (FAS))*	TS 54-14*
Alarm Receiving Centre (ARC) for Fixed Firefighting Systems (FFS) *(Alarmontvangstcentrale voor brandblussystemen (FFS))*	EN 12094-1
Alarm Receiving Centre (ARC) for Social Alarm Systems (SAS) *(Alarmontvangstcentrale voor sociale alarmsystemen(SAS)*	TS 50134-7
Alarm Receiving Centre (ARC) for audio/video door entry systems *(Alarmontvangstcentrale voor audio/video toegangssystemen)*	EN 50518
Alarm Receiving Centre (ARC) for Video Surveillance Systems (VSS) for non-security applications (traffic flow) *(Alarmontvangstcentrale voor videotoezichtsystemen (VSS) voor niet-security doeleinden (verkeersstromen zoals weg, spoor, water, terreinen)*	EN-IEC 62676-4
Alarm Receiving Centre (ARC) for people monitoring, lone workers and object tracking systems for non-security applications *(Alarmontvangstcentrale voor persoonsbeveiliging, alleenwerkers en object traceersystemen voor niet-security doeleinden)*	K21023 enkel indien het aangesloten platform gecertificeerd is conform K21023
Alarm Receiving Centre (ARC) for lifts emergency systems *(Alarmontvangstcentrale voor lift noodsystemen)*	EN 81-28

Tabel 2 Scopes en categorieën EN 50518

2.1 Gerefereerde normen per scope

ARC's waren vroeger voornamelijk uitgerust om berichten van inbraak- en overvalalarmsystemen af te handelen. Door de jaren heen zijn de ARC's in staat om alle soorten berichten te verwerken die EN 50518: 2019 herkent met zijn categorieën en scopes. Om een goede afhandeling van al deze verschillende soorten scopes te organiseren, verwijst de EN 50518 naar andere Europese normen voor de afhandeling van berichten. Voorbeelden zijn:

De norm TS 50131-7 “Alarm systems - Intrusion and hold-up systems - Part 7: Application guidelines” geeft richting aan het ontwerp-, installatie- en inbedrijfstellingsproces van alarmsystemen.

De norm CEN/TS 54-14* gaat over Automatische brandmeldinstallaties - Deel 14: Richtlijnen voor het projecteren, ontwerpen, installeren, in bedrijf stellen, gebruik en onderhoud. Houd er rekening mee dat de norm EN54-2 voor Automatische brandmeldingsinstallaties - Deel 2: Brandmeldcentrale en aansluitnormen voor componenten verplicht zijn om te gebruiken volgens de Bouwproductenverordening (CPR) Verordening (EU) nr. 305/2011.

* Het toepassingsgebied EN 54-14 is alleen van toepassing wanneer er een volledig gecertificeerde installatie in het pand aanwezig is. Dit toepassingsgebied kan ook van toepassing zijn op woningen

op een lager niveau met rookmelders op basis van EN 14604. Deze aansluitingen en afhandeling wordt dan beoordeeld in EN 50518 artikel 9.1.5. Rookmelders op basis van EN 14604 zijn vereist.

Niet alle paragrafen van de genoemde normen zijn van toepassing. Bijlage 2 bevat de 'Matrix EN 50518 en relevante normen met aanvullende diensten'. Deze matrix bevat de van toepassing zijnde paragrafen van de normen waarnaar wordt verwezen. Indien van toepassing zou de ARC de markt kunnen voorzien van een breder portfolio van beveiligingsdiensten. Door deze normen te implementeren, kan de ARC voldoen aan de internationale behoeften op de markt voor beveiligingsdiensten met een hoge bedrijfscontinuïteit en een goede kwaliteit van de dienstverlening.

2.2 Monitoring van verbindingen door de Monitoring Centrale (MC)

Hoewel de EN 50518 officieel wordt genoemd als 'Monitoring and Alarm Receiving Centers' (MARC), worden de meeste MARC's alleen gebruikt als ARC. Het verschil is te zien in de definitie zoals omschreven in EN 50136-1 / A1:

Alarm receiving centre:
continuously manned centre to which information concerning the status of one or more AS is reported.

permanent bemand centrum waar informatie over de status van een of meer AS wordt gerapporteerd.

Monitoring and alarm receiving centre
continuously manned centre to which information concerning the status of one or more AS is reported, and additionally where the status of one or more ATS is monitored.

permanent bemand centrum waar informatie over de status van een of meer AS wordt gerapporteerd, en daarnaast waar de status van een of meer ATS wordt bewaakt.

Om het end-to-end monitoringgedeelte van de ARC te erkennen, kan Kiwa de ARC beoordelen als Monitoring Center (MC) en dit specificeren op hun certificaat. Om de erkenning te ontvangen, moet een beoordeling in combinatie met EN 50136-1 / A1 worden uitgevoerd volgens certificatieschema K21030. Binnen EN50136-1 / A1 zijn er vereisten voor de alarmtransmissiedienstverleners die de prestaties van een alarmtransmissiesysteem (ATS) end-to-end bewaken vanaf de doormeldeenheid (SPT) die is aangesloten op het alarmsysteem en de ontvanger (RCT) binnen de beveiligde muren van de ARC. Zie hoofdstuk 8 van dit document en / of K21030 voor meer informatie.

Opmerking: In dit document wordt er in benaming geen onderscheid gemaakt tussen een ARC en een MARC. Waar specifiek een MARC wordt bedoeld wordt ook een Monitoring Centre (MC) aangehaald.

2.3 De locatie van gegevensverwerkende apparatuur

Met de introductie van EN 50518: 2019 mogen ARC's hun gegevensverwerkingsapparatuur (zoals vermeld in clausule 5.8 EN 50518) opslaan op een veilige locatie anders dan hun eigen ARC. Twee mogelijkheden zijn:

- Een andere gecertificeerde ARC op basis van EN 50518 categorie I;
- een datacenter ontworpen en onderhouden volgens EN 50600 (beschikbaarheidsklasse 3 en beschermingsklasse 4 (EN 50136-1 / A1 clausule 4.1.38).*

De prestaties van de verbinding tussen deze twee ARC's of de ARC en het datacenter moeten een Dual Path (DP) 4 zijn volgens 50136-1 / A1 en moeten gecertificeerd zijn volgens de scope 'kritische transmissie' van certificatieschema K21030. In het geval dat een externe locatie van gegevensverwerkende apparatuur van toepassing is, zal Kiwa dit opnemen op het certificaat van de ARC.

*Uitleg bij EN 50600: de EN 50136-1/A1 stelt: “een datacenter ontworpen en onderhouden volgens EN 50600 (beschikbaarheidsklasse 3 en bescherming 4)”. Dit betekent niet dat het datacenter zelf een certificering heeft volgens EN 50600, maar dit is ook een optie.

De interpretatie van Kiwa is een verificatie van de externe locatie voor gegevensverwerkende apparatuur. Dit gebeurt met een beoordeling op basis van de hoofdprincipes voor EN 50600 beschikbaarheidsklasse 3 en beschermingsklasse 4, maar richt zich op het afgebakende gebied van de (M)ARC. Op deze manier controleert Kiwa of het datacenter is ontworpen en onderhouden volgens EN 50600.

Onderwerp van de beoordeling zijn:

- de toegangscontrole van het datacenter,
- het koelsysteem,
- redundantie,
- scheiding van stroom- en datalijnen,
- (nood)stroomvoorzieningen,
- brandblussysteem,
- inbraak- en camerasysteem.

Bovenstaande paragraaf beschrijft een situatie waarin alle gegevensverwerkende apparatuur door de (M)ARC zelf wordt beheerd. Kiwa komt steeds vaker situaties tegen waarin ook andere vormen van cloud computing worden toegepast. Om vast te stellen of deze optie binnen de betekenis van de norm valt, moet ook inzicht zijn in de specificaties van het cloud computing-platform en geografische locatie(s). De beoordeling is ook gebaseerd op de hoofdprincipes van EN 50600 en Kiwa zou ook 'een afgelegen locatie voor gegevensverwerkende apparatuur' kunnen verklaren op het EN 50518-certificaat van de (M)ARC.

Opmerking: EN 50518 hoofdstuk 5.8 beschrijft een situatie waarin apparatuur zoals ontvangers en spraakopnameapparatuur zich op een afgelegen locatie bevindt. Indien ook het Alarm Management Systeem zich op een externe locatie bevindt, is het certificatieschema K21046 Hosted Alarm Solution van toepassing. Dit om een gecertificeerde en veilige manier te implementeren om het AMS op een afgelegen locatie te plaatsen.

3 Bedrijfscontinuïteit van een (M)ARC “R”

Naast vele eisen in de norm EN 50518, zal de ARC twee hoofddoelen moeten vervullen om hun klanten op een goede manier te kunnen bedienen. Dit zijn:

- De beschikbaarheid van een ARC: 24/7/365;
- Het afhandelen van alarmen conform de reactietijden genoemd in de norm.

De M(ARC) voert een uitgebreide risicoanalyse uit. De risicoanalyse maakt deel uit van een risicobeheerproces en is een integraal onderdeel van het beheer en de besluitvorming en geïntegreerd in de structuur, activiteiten en processen van de organisatie. Het risicobeheerproces omvat de systematische toepassing van risico-identificatie, risicoanalyse, risico-evaluatie en risicobehandeling. Hoewel het risicobeheerproces vaak als opeenvolgend wordt gepresenteerd, zal het in de praktijk iteratief en continu zijn. Naast het potentiële risico zoals aangegeven in EN 50518, artikel 3.1.13 en 4.2, moet rekening worden gehouden met de typische bedreigingen die als voorbeeld worden gegeven in ISO 27005, bijlage C.

Het risiconiveau wordt vergeleken met risico-evaluatiecriteria en risico-aanvaardingscriteria met betrekking tot bedrijfscontinuïteit en omvat:

- Verlies van zakelijke en financiële waarde

- Wettelijke en regelgevende vereisten en contractuele verplichtingen

- Operationeel en zakelijk belang van beschikbaarheid, vertrouwelijkheid en integriteit

- Verwachtingen en percepties van belanghebbenden, en negatieve gevolgen voor goodwill en reputatie.

In de volgende alinea's worden enkele definities gegeven om verschillende oplossingen voor bedrijfscontinuïteit te erkennen. Bedrijfscontinuïteit van een ARC kan bovendien aanvullend worden beoordeeld volgens ISO 22301; Maatschappelijke beveiliging - Bedrijfscontinuïteitsbeheersystemen - Vereisten.

3.1 Een zelfstandige/standalone ARC zonder BC mogelijkheden

EN 50518-certificering van de ARC. De ARC vereist een beperkt DRP / BCM-beleid en moet daarom al hun klanten informeren tijdens de downtime. Desalniettemin moet de ARC nog steeds voldoen aan een beschikbaarheid van 99,9% volgens EN 50136-1 / A1.

3.2 Satelliet-ARC

Een operationele ARC die is aangesloten op een andere (vaak grotere) operationele ARC van dezelfde ARC-organisatie, die in een andere regio is gevestigd en een aantal alarmen afhandelt in geval van capaciteitsproblemen.

Voorwaarden; De satelliet-ARC wordt door de certificeringsinstantie (CI) als twee locaties behandeld en moet worden opgenomen in de EN 50518-beoordeling. De satelliet-ARC is niet opgenomen in het Business Continuity Plan (BCP) van de grotere ARC omdat de andere ARC niet in staat is om alle alarmen in geval van nood af te handelen. De verbinding tussen deze twee ARC's moet een DP4 zijn volgens 50136-1/A1 en moet gecertificeerd zijn volgens schema K21030 scope ‘kritische transmissie’.

3.3 Twin ARC

Een operationele ARC aangesloten op een andere operationele ARC in een andere regio die alarmen afhandelt. Twin ARC's voldoen aan de BCP voor beide ARC's.

Voorwaarden; De systemen lopen volledig parallel tussen de primaire ARC en de secundaire ARC. De primaire en secundaire ARC zijn volledig operationele ARC's. Het uitgangspunt is dat de ARC's hun eigen EN 50518-certificaat hebben, mogelijk worden de ARC's door de Certificatie Instelling als twee sites behandeld. De ARC's kunnen elkaar aanvullen of vervangen in het kader van hun BCP. Dit is getest door beide ARC's en moet beoordeeld worden door de CI bij beide ARC's. De verbinding tussen deze twee ARC's moet een DP4 zijn volgens 50136-1/A1 en moet gecertificeerd zijn volgens K21030 scope 'critical transmission' (Transmissie tussen ARC's).

3.4 Een standalone ARC met BC mogelijkheden

Een alarmontvangstcentrale met alle IT-infrastructuur op de eigen locatie die mogelijkheden heeft om de dienstverlening gedeeltelijk op een andere locatie voort te zetten dient te voldoen aan: EN 50518 certificering van de ARC inclusief managementsysteem.

Voor de ARC zijn DRP/BCM-procedures vereist en zij is genoodzaakt het deel van de klanten waar geen dienstverlening aan geleverd kan worden te informeren in geval van downtime. Dit neemt niet weg dat de ARC nog steeds moet voldoen aan de beschikbaarheidseisen zoals gesteld in EN50136-1 ten aanzien van het aangesloten ATS van de hoogste klasse (SP1 t/m DP4). Daarnaast kan de alarmcentrale haar dienstverlening tijdelijk* voortzetten vanaf een operationele back-up locatie. De afspraken met de exploiteur van de back-up locatie zijn geformaliseerd. De operationele back-up locatie is geschikt en minimaal gecertificeerd als EN50518- ARC-type II of wordt beveiligd door particuliere beveiligers tijdens het gebruik van de locatie.

3.5 Een ARC met externe IT-infrastructuur

Een alarmontvangstcentrale met externe IT-infrastructuur op een externe locatie, zijnde datacenter (EN50600/EN50518) kan bij verstorende gebeurtenissen haar dienstverlening voortzetten door tijdelijk* gebruik te maken van een operationele back-up locatie. De alarmontvangstcentrale dient te voldoen aan: EN 50518 certificering van de ARC inclusief managementsysteem en externe locatie ten behoeve van de IT-infrastructuur. Daarnaast voldoet de ICT-infrastructuur tussen beide locaties aan DP4 conform EN50136-1./K21030 scope 2. De ARC beschikt over DRP/BCM-procedures en kan haar dienstverlening tijdelijk* voortzetten vanaf de operationele back-up locatie. De afspraken met de exploiteur van de back-up locatie zijn geformaliseerd. De operationele back-up locatie is geschikt en gecertificeerd als EN50518- ARC-type II of wordt beveiligd door particuliere beveiligers tijdens het gebruik van de locatie.

3.6 Back-up ARC

Een secundaire ARC die, in overeenstemming met het Business Continuity Plan (BCP) van de primaire ARC, de processen van een primaire ARC kan overnemen, die mogelijk niet in staat is om te voldoen aan de prestatie-eisen een incident of een andere oorzaak.

Voorwaarden; De systemen lopen volledig parallel tussen de primaire ARC en de secundaire back-up ARC. De back-up ARC is geen volledig operationele ARC en is alleen operationeel in de back-upsituatie. De back-up ARC moet beoordeeld worden (bouw- en systeemeisen) en geëvalueerd door de CI binnen de beoordeling van de primaire ARC op basis van EN 50518. Mogelijk worden de ARC's behandeld als een twee-site door de Certificatie Instelling. De BCP moet worden getest door de ARC en geverifieerd door de CI.

Ook bestaat de mogelijkheid dat een aparte organisatie deze back-up ARC gaat organiseren. Deze situatie moet vervolgens worden beoordeeld door de CI binnen een afzonderlijk certificaat EN 50518, waarbij de BCP moet worden getest door de ARC en geverifieerd door de CI.

In elk van deze situaties moet de verbinding tussen deze twee ARC's een DP4 zijn volgens 50136-1 / A1 en gecertificeerd zijn volgens de K21030-scope 'kritische transmissie' (Transmissie tussen ARC's).

*** Tijdelijk**

Uitwijken naar een locatie om de dienstverlening voort te zetten kan uitsluitend een tijdelijk karakter hebben. Plannen om dit te bewerkstelligen dienen te allen tijde gemotiveerd te zijn in de risicoanalyse en uitgewerkt in een DRP en/of BCP. Om de tijdelijkheid transparant en meetbaar te maken zijn de volgende criteria opgesteld.

Tijdvak	Actie
< 48 uur	Op basis van het DRP/BCP wordt een uitwijk geïnitieerd. De besluitvorming voor uitwijken wordt vastgelegd als incident. Alle incidenten worden tevens geëvalueerd en meegenomen in de management review. In geval van thuiswerken dient per dienst te worden gemotiveerd, waarom er sprake is van thuiswerken. Dit dient tevens te worden vastgelegd en geëvalueerd.
> 48 uur	Na 48 uur dient een besluit te worden genomen over de continuering van de dienstverlening. Het besluit dient te worden vastgelegd. Alle besluiten worden tevens geëvalueerd en meegenomen in de management review.
< 1 week	Na 1 week uur dient een besluit te worden genomen over de continuering van de dienstverlening. Wanneer de dienstverlening voor langere tijd buiten de beveiligde schil (Type I) moet worden uitgevoerd, dient een plan van aanpak te worden opgesteld om binnen 2 maanden terug te keren binnen een beveiligde schil (Type I). Het plan van aanpak inclusief besluit(en) dient te worden vastgelegd. Alle besluiten worden tevens geëvalueerd en meegenomen in de management review.
< 2 maanden	Na 2 maanden dient de dienstverlening te worden gecontinueerd binnen een beveiligde schil (Type I). De wijze waarop de werkzaamheden binnen de beveiligde schil zijn hervat dient te zijn vastgelegd in een evaluatierapport. Het evaluatierapport wordt geëvalueerd en meegenomen in de management review.

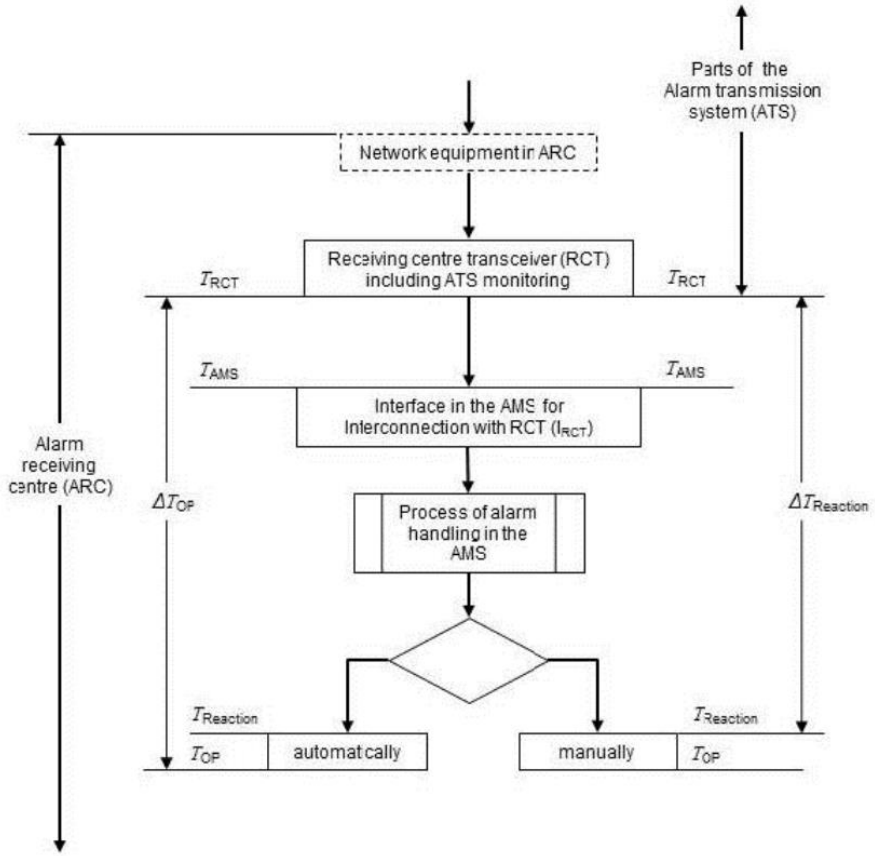
4 Statistieken van de MARC “G en R”

Een MARC heeft de volgende primaire functies:

- Adresseren en afhandelen van inkomende berichten als ARC volgens EN 50518.
- Adresseren en afhandelen van falende transmissieverbindingen:
  - van de doormeldeenheid (SPT) op de locatie van het alarmsysteem (AS) of
  - voor een Alarm Transmission Service Provider (ATSP) volgens EN 50136-1 / A1 & certificatieschema K21030 als Monitoring Center.

4.1 Voorbeeld alarmafhandeling - G

Een ARC moet zijn primaire prestatie-indicatoren (KPI's) controleren. In dit geval is de snelheid van het afhandelen van inkomende berichten volgens de norm. Om dit te doen heeft de ARC een functie nodig in haar Alarm Management Systeem (AMS) die de metadata in dit systeem analyseert, waardoor de ARC operators live inzicht krijgen of ze binnen hun verplichte KPI's werken. Het management van de MARC heeft deze statistieken nodig om corrigerende maatregelen te treffen als niet aan de KPI's wordt voldaan (bijvoorbeeld: om de operators extra te trainen in het effectiever uitvoeren van hun taak of om het aantal operators dat de alarmen verwerkt te vergroten). Deze statistieken zijn ook belangrijk om preventieve acties voor het ARC-management aan te pakken (bijvoorbeeld om piekperiodes te herkennen gedurende het jaar waarin meer alarmen binnenkomen en er extra operators nodig zijn).



Figuur 3

Voor het hebben van de juiste statistieken is de informatie van de RCT, die alarmen doorgeeft aan het AMS, nodig.

ΔTOP; tijd die verstrijkt tussen het moment van beschikbaarheid van het alarmbericht aan de uitgang van de RCT en het moment van eerste actie geïnitieerd door de ARC-operator of de AMS (ΔTOP = TOP - TRCT).

Voor een ARC is het belangrijk om te weten:

- Hoeveel alarmen komen de ARC binnen in de cue.
- Hoe snel worden deze alarmen erkend door het AMS. De acceptatie kan worden gedaan door een operator die het alarm op zijn monitor krijgt of een automatische handeling. De verwerkingstijd om het alarm door de operator te voltooien is niet relevant voor deze statistiek / KPI.

4.2 Best practice voor het voldoen aan de prestatiecriteria van berichtverwerking - G

Om zeker te zijn dat ze voldoen aan de KPI van prioriteit 1 voor overval, brand, vaste brandbestrijdingssystemen, personenbewaking en voor andere alarmen is overeengekomen dat ze van het hoogste prioriteitsniveau zijn: 30 s voor 80% van de ontvangen signalen en 60 s voor 98 , 5% van de ontvangen signalen.

De meeste MARC's gebruiken een drempel van 15 tot 25 seconden om aan de prestatiecriteria te voldoen. Hierdoor kunnen ze binnen de KPI opereren. De drempel van 15 seconden geeft de meeste zekerheid.

Een voorbeeld. Een MARC behandelt dagelijks 100 alarmen met prioriteit 1. De norm vraagt om een overeenstemming met bovenstaande criteria die over een voortschrijdende periode van twaalf maanden moeten worden bereikt. Dit leidt binnen 30 dagen tot de volgende criteria;

Aantal prio 1-alarmen per dag	**80% binnen 30 seconden**	**98,5% binnen 60 seconden**	**1,5% boven 60 seconden**
100	80 alarmen	18 alarmen	2 alarmen
Aantal prio 1-alarmen per week	**80% binnen 30 seconden**	**98,5% binnen 60 seconden**	**1,5% boven 60 seconden**
700	560 alarmen	129 alarmen	11 alarmen
Aantal prio 1-alarmen per 30 dagen	**80% binnen 30 seconden**	**98,5% binnen 60 seconden**	**1,5% boven 60 seconden**
3000 alarms	2400 alarmen	555 alarmen	45 alarmen

Tabel 3 Aantal prio 1-alarmen

Als de ARC een slechte dag heeft in het uitvoeren omdat veel alarmen naar de MARC worden gestuurd vanwege fouten in de AS, en bijvoorbeeld 19 alarmen met prioriteit 1 zijn hoger dan 60 seconden, voldoet de ARC niet aan zijn KPI.

In het voorbeeld van een week kan dit leiden tot het volgende voorbeeld. Als 601 alarmen met prioriteit 1 binnen een week boven 30 seconden worden afgehandeld, voldoet de ARC niet aan zijn KPI.

De 1,5% die boven de 60 seconden mag komen, is de basis voor verder onderzoek door de ARC om de KPI's van hun diensten te verbeteren.

4.2 Prioriteiten voor reactietijden – R

Hieronder volgt een tabel ter verduidelijking van EN 50518, hoofdstuk 9.2. Prioriteit 1, 2 en individuele diensten worden vermeld. Ook de mogelijkheid van automatische alarmbehandeling en vertraging zijn opgenomen in de tabel per alarmtoestand/-melding.

Prioriteit	EN 50518 art. 9.2	Automatische alarm afhandeling mogelijk	Vertraging mogelijk	Specifieke alarmtoestand/-bericht
1	Voor overval, brand, vaste brandblussystemen, personenbewaking en voor andere alarmen die als hoogste prioriteit zijn aangemerkt: 30 s voor 80 % van de ontvangen alarmen en 60 s voor 98,5 % van de ontvangen alarmen;	Nee Nee Nee Nee Nee Ja	Nee Nee Nee Nee Nee Ja/Nee	Overval Branddetectiesystemen Brandblussystemen Personenbewaking Sociaal - levensbedreigend Andere volgens klantcontract
2	Alle andere alarmcondities: 90 s voor 80 % van de ontvangen alarmen en 180 s voor 98,5 % van de ontvangen alarmen.	Ja Ja Ja Nee Nee Ja	Ja Ja Ja Ja Ja Ja	Inbraak Video - detectie Sociaal - niet levensbedreigend Sabotage Totaaluitval Andere volgens klantcontract
#	Individuele diensten op basis van een klantencontract NL 50518 9.1.5	Ja Ja Ja Ja Ja	Ja Ja Ja Ja Ja	Video Access Traffic Lift Failures also ATP Signals also technical

Tabel 4

Noot: voor reactietijdenvoorstel CCV PAC zie bijlage 4. Alle alarmen en meldingen dienen te worden gemeten in het AMS. Er mag geen negatieve invloed zijn vanuit scopes die niet onder certificatie zijn op de gecertificeerde scope. Er zijn geen uitsluitingen mogelijk. Daarnaast moeten ook automatische alarmafhandelingen separaat gemeten kunnen worden.

4.3 Monitoring van verbindingen (Monitoring Centre) - G

ATS-prestatiebewaking wordt doorgaans uitgevoerd door de ATSP (Alarm Transmission Service Provider). De ATSP kan de monitoring zelf uitvoeren of delegeren aan een Monitoring Center volgens EN 50518. Als de ATSP de monitoring zelf uitvoert, moet deze ook voldoen aan EN 50518. Voor meer informatie over ATSP's, zie ook hoofdstuk 8.

Een Monitoring Center (MC) kan een afzonderlijk centrum zijn of onderdeel zijn van een ARC. De oorsprong van prestatiebewaking is de verplichte vereiste in EN 50136-1. De taken van een Monitoring Center zijn het melden en loggen van storingen en beschikbaarheid. Deze taken moeten worden ondernomen om het vereiste prestatieniveau voor elke ATS van de desbetreffende categorie te behouden.

Het doel van prestatiebewaking is om snel ATS'en te identificeren die niet voldoen aan de overeengekomen prestaties voor de juiste categorie.

Het is om deze reden dat een MC / ATSP continu de belangrijke prestatieparameters moet bewaken, b.v. transmissie vertragingen, fouten en beschikbaarheid. Wanneer een fout wordt geïdentificeerd, moet de MC / ATSP een actie ondernemen om de fout te herstellen en de ATS in zijn volledig operationele staat te herstellen om te voorkomen dat de ATS en / of ATSN niet aan de vereiste gemiddelde vertragingen en beschikbaarheid voldoen.

Figuur 3 toont de 'ATS-monitoring' in het midden van de ATS tussen het alarmsysteem en de ARC. In theorie zou de monitoring ook in de ARC kunnen worden uitgevoerd als de ARC ook een ATSP en / of MC is.

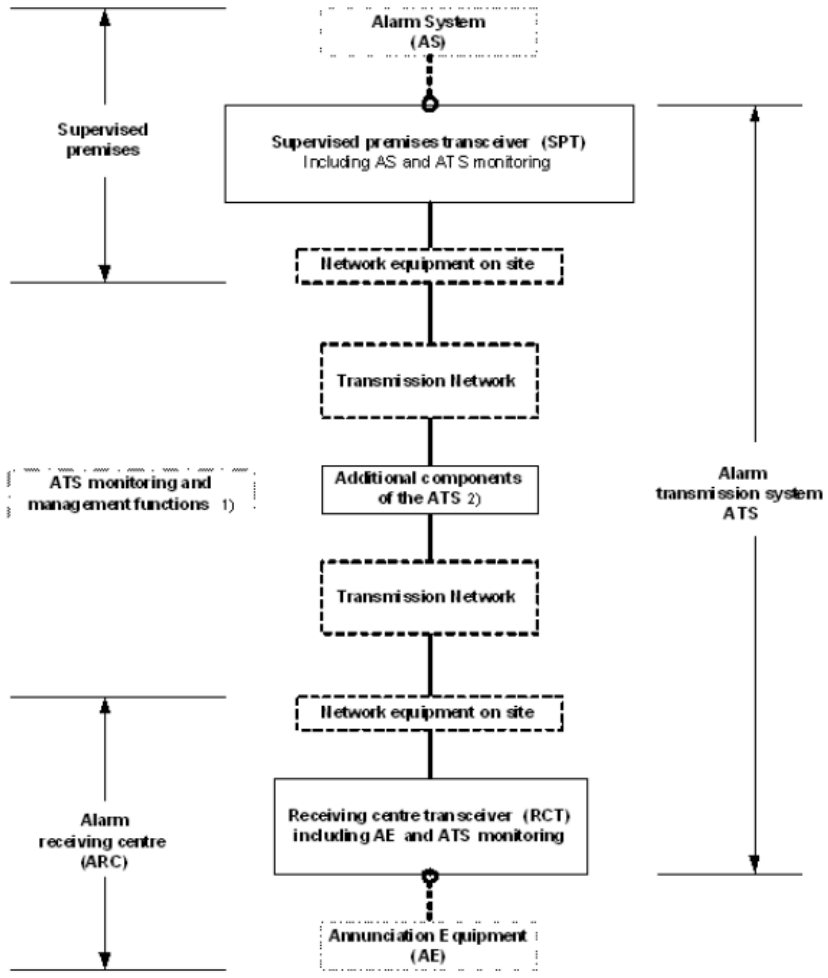


Figure 4

4.4 Lean ATSP - G

EN 50136-1 / A1 specificeert vereisten voor alarmtransmissiesystemen en bewaking van deze systemen in combinatie met EN 50518. De bevoegde autoriteit hiervoor is: wetshandhavings- en verzekeringspartijen. Ze vereisen een bewaakte alarmtransmissie op basis van prestatiecontrole.

EN 50136-1, -2 en -3 samen met EN 50518 stellen eisen aan dit bewakingsproces. In dit proces kan de Alarm Receiving Centre de functie van Monitoring Centrale (MC) uitvoeren. We zien dat de ARC's worstelen met dit proces om de rol als MC te vervullen. Het doel van Lean ATSP is om deze worstelende ARC's te helpen.

De ontvanger volgens EN 50136-3 verwerft de gegevens die nodig zijn om de rol voor transmissies met twee paden te vervullen. De ARC moet standaardactiepatronen hebben om zich te gedragen bij falende verbindingen.

Definities:
Polling
Een veelgebruikte methode voor het bewaken van alarmtransmissiepaden (ATP) en / of ATS-beschikbaarheid waarbij de term polling betekent dat er regelmatig statusberichten worden uitgewisseld tussen een SPT en een RCT. (EN 50136-7)

Rapportagetijd
Periode vanaf het moment dat er een fout optreedt in de ATS totdat de foutinformatie wordt gerapporteerd aan de RCT, het alarmsysteem op het bewaakte terrein of de zendontvanger van het bewakingscentrum (indien aanwezig) (EN 50136-1 / A1)

Polling- en rapportagetijd zijn dus niet hetzelfde! Zie norm EN 50136-7 voor meer informatie.

	DP4
Primaire ATP Rapportagetijd	90 seconden
Secundaire ATP Maximale periode wanneer de primaire operationeel is	5 uur
Alternative ATP Maximale periode wanneer primaire faalt	90 seconden
Falen van alle ATP's tegelijkertijd *	3 minuten
*Als een ATS twee of meer ATP's bevat, moet de rapportagetijd voldoen aan de vereisten van deze tabel	

Tabel 5 Maximale rapportage tijd DP4

Als een ATS operationeel blijft, wordt een enkele lijnpad fout aan de ATSP voorgelegd, maar kan deze worden vertraagd bij de AMS, indien overeengekomen tussen belanghebbenden. De maximale vertraging mag niet meer zijn dan 96 uur.

Met de bovenstaande informatie is hieronder een suggestie gedaan voor een standaardactie. Het doel van deze opzet is om zoveel mogelijk in het proces te automatiseren.

Andere categorieën vallen buiten het toepassingsgebied van dit voorstel.

DP 4	**90 seconden** EN 50136-1/A1	**30 minuten na RT** EN 50518	**25 uur na RT** EN 50518	**1 week na RT** EN 50518
Falende primaire verbinding	**Rapportagetijd (RT)**	**Automatische e-mail / sms**	**Automatische e-mail / sms**	**Telefoontje**
DP4	**5 uur** EN 50136-1/A1	**30 minuten na RT** EN 50518	**5 uur na RT** EN 50518	**1 week na RT** EN 50518
Falende secundaire verbinding Als primair faalt, is de alternatieve rapportagetijd 90 seconden.	**Rapportagetijd (RT)**	**Automatische e-mail / sms**	**Automatische e-mail / sms**	**Telefoontje**

DP 4	**3 minuten** EN 50136-1/A1	**90 seconden na RT** EN 50518
ATS fout	**Rapportage tijd (RT)**	**Automatische e-mail / sms <u>en</u> een telefoontje**
Zorg er bij het implementeren van deze tabel voor uw Monitoring Center voor dat deze wordt overeengekomen tussen geïnteresseerde partijen		
Een automatische e-mail / sms is een voorbeeld van een redundante vorm van communicatie naar de gebruiker / klant. Andere effectieve vormen zijn ook mogelijk.		
Alle tijden in deze tabel zijn de maximale tijden.		

Tabel 6 Lean ATSP DP4

De bovenstaande tabel schriftelijk:
DP4
Primair pad heeft een falende verbinding;

- Rapporteringstijd is 90 seconden. Na 30 minuten wordt automatisch een e-mail / sms * naar de client gestuurd met betrekking tot deze mislukte verbinding.
- Indien niet opgelost na 25 uur, wordt er automatisch een e-mail / sms * naar de client gestuurd met betrekking tot deze falende verbinding.
- Indien niet verholpen na 1 week, een telefoontje naar de klant over deze falende verbinding en dat de klant voldoet aan de vereisten van betrouwbare alarmoverdracht omdat de back-upsituatie niet functioneert.

Alternatief pad heeft een falende verbinding;

- Rapporteringstijd is 5 uur. Na 30 minuten wordt automatisch een e-mail / sms * naar de client gestuurd met betrekking tot deze mislukte verbinding.
- Indien niet verholpen na 5 uur, wordt er automatisch een e-mail / sms * naar de client gestuurd met betrekking tot deze mislukte verbinding.
- Indien niet verholpen na 1 week, een telefoontje naar de klant over deze falende verbinding en dat de klant voldoet aan de vereisten van betrouwbare alarmoverdracht omdat de back-upsituatie niet functioneert.

Zowel het primaire als het alternatieve pad hebben een falende verbinding;

- Rapporteringstijd is 90 seconden. Na 90 seconden wordt automatisch een e-mail / sms * naar de client gestuurd met betrekking tot deze falende verbinding en een telefoontje naar de client met betrekking tot deze falende verbinding en dat de client aan de vereisten voldoet en dat er een mogelijkheid bestaat voor een vijandige aanval op de verbindingen en bewaakte gebouwen.

Een automatische e-mail / sms is een voorbeeld van een redundante vorm van communicatie naar de gebruiker / klant. Andere effectieve vormen zijn ook mogelijk.

5 Gebouw en constructie-eisen “R”

5.1 Algemeen

EN 50518 stelt eisen aan de constructie en systemen van ARC's. Dit hoofdstuk bevat interpretatie, extra informatie en uitleg over de eisen.

5.2 Weerstand tegen fysieke aanval - R

- Wanneer een (M) ARC geen testrapporten, productiespecificaties en / of bouwtekeningen heeft, moet destructief onderzoek worden uitgevoerd om aantoonbaar aan de norm te voldoen.
- Dit geldt ook voor kalkzandsteen waar de massa het belangrijkst is voor conformiteit.
- Als de dikte van de muur, vloer of plafond overeenkomt met de tabel in EN 50518 (behalve staal), is dit voldoende om te voldoen aan fysieke weerbaarheid, kogelwerendheid en brandwerendheid.

5.3 Glasoppervlakken - R

- Als het glasoppervlak kogelwerend is, kan er van uit worden gegaan dat het ook voldoende brandwerend is. In het geval van aangrenzende gebouwen heeft de brandwerendheid meer prioriteit.
- Het risico van gebouwen die dicht bij het ARC staan, wordt beoordeeld in de risicobeoordeling. Dit is ook het geval bij gebouwen met brandgevaar van vloer tot verdieping.
- Conformiteit voor weerstand tegen kogelaanvallen is ook van toepassing op een fysieke aanval. Niet andersom.
- Zichtbaarheid van de ARC: dit item moet worden behandeld in de risicobeoordeling. Wat kunnen andere mensen van buitenaf zien?

5.4 Weerstand tegen vuur en rook (constructie)- R

- Dit wordt geïnterpreteerd van buiten de beveiligde schil naar de binnenkant van de beveiligde schil en niet omgekeerd.
- Weerstand tegen vuur en rook is afhankelijk van nationale regelgeving.
- De beveiligde schil van de ARC moet een brandwerendheid hebben volgens EN 13501-2 "Brandclassificatie van bouwproducten en bouwelementen - Deel 2: Classificatie met gegevens van brandwerendheidstests, met uitzondering van ventilatiesystemen" met een minimum van 30 minuten. De norm vermeldt de volgende brandscenario's:
  - o De standaard temperatuur / tijd-curve (na flash-over brand);
  - o De langzame stooklijn (smeulend vuur);
  - o Het 'halfnatuurlijke' vuur;
  - o De externe brandblootstellingskromme;
  - o Constante temperatuuraanval.

- De minimaal geldende eis is E - Integriteit voor wand, plafond, vloer en deuren.
- Nationale bouwvoorschriften of het ontwerp van het gebouw kunnen meer prestatiekenmerken verkrijgen, zoals

  - o R - Draagvermogen,
  - o I - Isolatie,
  - o W - Straling, enz.

  Vergeet deze niet na te vragen bij de architect en / of de lokale bouwautoriteiten.

- Gewapend beton van minimaal 10 cm wordt geacht aan deze E30-eigenschap te voldoen conform de minimale dikte voor wanden genoemd in hoofdstuk 5 van de norm.

5.4.1 Weerstand tegen vuur en rook (service-inlaten en -uitlaten)

Doorvoerafdichtingen moeten voldoen aan de norm EN1366-3 “Brandwerendheidstests voor service-installaties; Deel 3: Doorvoerafdichtingen “en gecertificeerd volgens de ETAG 26-serie” -richtlijn voor Europese technische goedkeuringen voor brandwerende en brandwerende producten ”. De ETAG-richtlijnen zijn vervangen door EAD's;

- EAD 350141-00-1106; Lineaire voeg- en spleetafdichtingen;
- EAD 350454-00-1104; Penetratie-afdichtingen

Brandwerende producten moeten gecertificeerd zijn volgens de ETAG 18-serie. De ETAG-richtlijnen zijn vervangen door EAD's;

- EAD 350402-00-1106; Reactieve coatings voor brandbeveiliging van stalen elementen.
- EAD 350142-00-1106; Brandwerende plaat, plaat- en matproducten en -kits.
- EAD 350140-00-1106; Renderings en kits op basis van Renderings die bedoeld zijn om brandwerende toepassingen te vuren.

Brandkleppen in verwarmings-, ventilatie- en airconditioningsystemen moeten aan de norm voldoen:

- EN1366-2 "Brandwerendheidstests voor service-installaties - Deel 2: Brandkleppen" en
- Classificatie volgens EN13501-3 "Brandclassificatie van bouwproducten en bouwelementen - Deel 3: Classificatie op basis van gegevens van brandwerendheidstesten op producten en elementen die worden gebruikt in gebouwinstallaties: brandwerende kanalen en brandkleppen"

De installatie-instructies van de fabrikant moeten worden opgevolgd om dezelfde prestaties te garanderen als tijdens de eerste typetests van deze producten. De producten worden geïnstalleerd aan de binnen- of de buitenzijde van de schil van de ARC, afhankelijk van de instructies van de fabrikant. De kant van de schil is ook afhankelijk van wat beschermd moet worden. Houd er rekening mee dat brandkleppen meestal getest worden gemonteerd in de brandwerende muur.

5.5 Bescherming tegen blikseminslag - R

Alle daarvoor geschikte metalen installaties / onderdelen moeten een potentiaalvereffening hebben (elektrische onderlinge verbinding van metalen installaties / onderdelen), zodat in het geval van bliksemstromen geen metalen onderdelen een ander spanningspotentieel heeft van elkaar. Een bescherming kan ook worden bereikt door het gebruik van overspanningsbeveiligingsapparatuur (SPD's) waar de directe verbinding met verbindingsgeleiders niet geschikt is. Sommige delen van een constructie, zoals een afgeschermde ruimte, zijn van nature beter beschermd tegen bliksem dan andere en het is mogelijk om de meer beschermde zones uit te breiden door een zorgvuldig ontwerp van de bliksembeveiligingsinstallatie (LPS), aarding van metalen voorzieningen zoals water en gas, en bekabeling technieken. Het is echter de juiste installatie van gecoördineerde overspanningsbeveiligingsapparatuur (SPD's) die apparatuur beschermen tegen schade en de continuïteit van de werking ervan garanderen - cruciaal voor het elimineren van downtime. Daarom moet de juiste SPD-bescherming dienovereenkomstig worden geïnstalleerd wanneer de (M)ARC niet goed is afgeschermd.

Er moet een risicoanalyse worden uitgevoerd in overeenstemming met EN 62305-2 of nationale voorschriften en er moeten passende maatregelen worden genomen om de ARC te beschermen tegen de effecten van bliksem wanneer R1 => 1 (verlies van mensenlevens 1 op 100.000 (1 x 10- 5).

5.6 Sluis - R

- Alle sluisdeuren moeten naar buiten openen gezien vanuit de ARC.
- Een sluis zou ook drie deuren kunnen hebben die ook interlocked moeten zijn. Dit moet voldoen aan alle constructievereisten en alleen kunnen worden bediend vanuit het ARC.

- Key cards zijn niet toegestaan voor normale toegang. De deuren van de sluis mogen alleen vanuit de ARC bediend worden. Key cards worden geaccepteerd als re-entry. Of als multi-factor authenticatietool.

5.7 Ventilatie inlaat- en uitlaatopeningen - R

- Openingen in de structuur van een ARC voor ventilatiesystemen moeten voldoen aan de vereisten voor weerstand tegen fysieke aanvallen.
- Ventilerende inlaat of uitlaat hebben geschikte alarmdetectie-apparatuur nodig om elke poging om de ventilatie-inlaat binnen te gaan te detecteren.
- De ventilatie-inlaat- en uitlaatopeningen in de schil van de ARC moeten fysiek worden beschermd.
- Inlaat- en uitlaatopeningen voor ventilatie moeten worden beschermd met luchtdichte kleppen die van binnenuit in de ARC in de gesloten positie kunnen worden vergrendeld.
- EN 50518 specificeert geen maximumtijd voor het sluiten van de luchtdichte kleppen. Deze tijd moet worden gezien vanuit het perspectief van BCM en risicoanalyse en moet realistisch zijn. Kiwa beoordeelt de tijd en doet een trendanalyse.
- De brandklep moet op de brandscheiding worden gemonteerd. De gasklep hoeft niet precies op de brandscheiding te worden gemonteerd.

5.8 Alarmsystemen van de ARC

Om te voldoen aan de paragrafen genoemd in alarmsystemen van de ARC, moet de ARC gecertificeerde componenten gebruiken voor hun alarmsysteem, brandalarmsysteem, gas, overvalknoppen en videobewakingssysteem. Het basis- en detailontwerp moet ook gebaseerd zijn op Europese normen: EN 50131, EN 54 en IEC 62676-4.

5.9 Alarm transmissie

Het alarmtransmissiesysteem voor het alarmsysteem van de (M)ARC voor EN 50518: 2019 moet minimaal voldoen aan EN 50136-1 categorie SP4 of DP3.

Het eigen alarmsysteem (en) van de ARC, inclusief het ATS, moeten worden bewaakt en getest op correcte werking. Voor de juiste werking wordt het volgende getest en de resultaten geregistreerd:

- Test hold-up knoppen (driemaandelijks)

- Open de nooddeur en beide deuren van de entreehal tegelijkertijd (driemaandelijks)

- Ontkoppel primaire ATP (maandelijks)

5.10 Branddetectiesysteem

De delen van het gebouw die worden ingenomen door het bedrijf dat de (M) ARC exploiteert, worden beschermd door een branddetectiesysteem en omvatten akoestische en optische waarschuwingsapparatuur in overeenstemming met nationale vereisten en veiligheid met componenten die zijn gecertificeerd volgens de EN 54-serie. Het branddetectiesysteem dient zodanig te zijn dat minimaal alle vitale ruimtes voor bedrijfscontinuïteit waar activiteiten worden ondergebracht zoals: technische ruimtes, dataruimtes, ups ruimtes, generator ruimtes, patch ruimtes worden beveiligd. De ontruimingsalarmsystemen moeten voldoen aan de wettelijke vereisten die door een nationale overheid noodzakelijk worden geacht en moeten zodanig zijn dat de zoemer een geluid afgeeft dat 6 dB boven het omgevingsgeluid ligt en, indien gebruikt, optische waarschuwingsapparatuur in de (M) ARC zichtbaar zijn voor de operators in de ARC.

Speciale aandacht voor vluchtwegbewaking bij evacuatieroutes.

6 Operatie van de ARC

6.1 Algemeen

EN 50518 stelt eisen aan de bediening van (M) ARC's. Dit hoofdstuk bevat extra interpretatie, extra informatie en uitleg over eisen..

6.2 Dagelijkse testen - G

Een ARC moet op zijn minst de binnenkomende communicatielijnen en alle kritieke componenten in de ARC zoals de AMS, ontvangers en databases bewaken om de beschikbaarheid van de ARC vast te stellen. Deze monitoring moet zo geautomatiseerd mogelijk zijn. Wanneer componenten worden gedupliceerd, en slechts 1 component faalt en de ARC blijft draaien op de andere component, is de beschikbaarheid nog steeds 100%. Kiwa zal deze beschikbaarheid verifiëren met rapporten volgens EN 50136-1 voor een wekelijkse, maandelijkse en jaarlijkse beschikbaarheid.

6.3 Communicatie - R

Alle ontvangers, die niet gecertificeerd zijn volgens EN 50136-3, moeten functioneel getest worden door de ARC zelf. Voor het functioneel testen heeft de ARC de leverancier nodig. Toegangsniveau 4 kan niet worden getest zonder de leverancier.

Vooral de primaire communicatiekabel moet fysiek worden beschermd en beschermd tegen vuur. De tweede communicatiekabel is de redundantie.

6.4 Stroomvoorziening - R

Om conformiteit met de norm vast te stellen, is Kiwa verplicht om minimaal één keer per jaar getuige te zijn van het testen van de noodstroom voorziening en de werking daarvan.

6.5 Toegangsbeleid - G

De norm specificeert de volgende vereisten:

- Bezoekers van het (M) ARC dienen altijd vergezeld te worden door een medewerker van het ARC;
- Onderhoud van kritieke apparatuur moet altijd onder toezicht staan van een medewerker van de ARC.

6.6 Alarm verificatie - G

Voor alarmverificatie kijkt Kiwa naar andere standaard voor aangesloten systemen zoals EN 50131, EN 50134, EN 54 etc. Het systeem moet op een correcte manier worden geïnstalleerd en getest om een goede alarmverificatie te kunnen doen. De ARC moet zich daarvan bewust zijn.

De standaard TS 50131-9 geeft methoden en principes voor alarmverificatie van inbraak- en overvalalarmsystemen. Contact opnemen met het risico-adres voor alarmverificatie kan worden gebaseerd op de risicobeoordeling van het bewaakte pand. Deze verificatiemethode kan te traag zijn om de indringer aan te houden.

Er zijn verschillende verificatie opties:

- Sequentiële verificatie van inbraakalarmen;
- Sequentiële verificatie van overvalalarmen;
- Hoorbare alarmverificatie;
- Visuele alarmverificatie;
- ATS-fouten.

7 Managementsysteem van de ARC

7.1 Algemeen

De EN 50518 beschrijft managementtools die in de ARC aanwezig moeten zijn. Dit hoofdstuk geeft interpretatie, extra informatie en uitleg over de aansluiting met ISO 27001.

7.2 ICT-security - G

Van toepassing zijnde paragrafen EN 50518:2019

Paragraaf	Onderwerp	Korte referentie
8.2	Time synchronization of equipment	Tijdsynchronisatie is vereist. Evenals foutenlogboeken en rapportage.
9.1.1	Procedures – General	Gedocumenteerde SOP's en KPI's vereist.
9.1.3	Message Handling	Statistieken worden gemaakt en geanalyseerd. Voor zowel handmatige als automatische berichten.
9.1.7	Unexpected increase in alarms	Hoe gaat MARC hiermee om?
9.1.8	Alarm transmission path failures	Alarmtransmissiepadfouten van de MARC moeten worden gesignaleerd in de MARC.
9.1.9	Controls to maintain quality of service	Hoe kan het MARC te allen tijde de kwaliteit van de dienstverlening handhaven?
9.1.10	Installation, maintenance, protection, removal and reuse of assets under the control of the ARC	Het assetbeheer moet worden uitgevoerd.
9.1.11	Monitoring and testing of equipment	Alle apparatuur moet worden gecontroleerd en regelmatig getest
9.1.12	Fault procedures and reporting	Rapportage is nodig wanneer apparatuur of software faalt.
9.1.13	Information management	Procedure voor het veilig omgaan met de benodigde informatie.
9.1.14	Data back-up	Back-up procedure nodig. Wanneer worden de back-ups gemaakt en wanneer worden ze getest?
9.1.15	Confidentiality and classification of information	Autorisatiematrix is vereist. Labelling van informatie en een clear desk beleid is benodigd
9.1.16	Relationships with essentials suppliers	Leveranciers moeten worden gescreend en er moeten afspraken worden gemaakt over data
9.1.18	Physical Access	De toegang tot de ARC en kritieke componenten moet worden beperkt. Er moet een autorisatiematrix worden getoond.
9.1.19	Remote access	Als externe toegang wordt gebruikt, moet dit veilig zijn.
9.1.20	Operational continuity and emergencies	Risico- en continuïteitsbeheer. We verwachten een beoordeling op basis van ISO 31000 (ISO 27005). Minstens 2 aansluitingen, aparte kabel apart lopen, redundante ontvangers, CIA, binnen de ARC zijn de paden van data en energie gescheiden. AMS is een apart systeem met redundante bekabeling en aparte kabeldoorvoer. (EN 50136), Fysieke beveiliging ook buiten alarmcentrale (datacenter, generator), logische toegang. Vuile connecties? Veilige toegang op afstand van leveranciers. Uw serverruimte koelen. Worden PEN-tests uitgevoerd?
10.4	Risk and contingency management	Het beheer van IT-systemen en IT-beveiliging moet worden georganiseerd. (Zie onder eisen ivm ICT beveiliging) Daarnaast moet worden voldaan aan de eisen zoals gesteld met betrekking tot GDPR.
10.4	Information management	Zie normatieve bijlage A van ISO 27001

Tabel 7

7.3 Mapping ISO 27001 bijlage A controls met EN 50518 – R

Onderstaande tabel is een mapping van de controls van ISO 27001 bijlage A met de eisen genoemd in EN 50518. Waar van toepassing zijn de hoofdstukken uit de EN 50518 toegevoegd. Waar de koppeling naar EN 50518 ontbreekt, zal dit aanvullend moeten worden aangetoond tijdens de audit.

	Normatieve bijlage A van ISO/IEC 27001:2013/2017 mapping met EN 50518	**EN 50518**
5	Informatiebeveiligingsbeleid	
5.1	Aansturing door de directie van informatiebeveiliging *Doelstelling: Het verschaffen van directieaansturing van en -steun voor informatiebeveiliging in overeenstemming met bedrijfseisen en relevante wet- en regelgeving.*	10.4 & 9.1
6	Organiseren van informatiebeveiliging	
6.1	Interne organisatie *Doelstelling: Een beheerkader vaststellen om de implementatie en uitvoering van de informatiebeveiliging binnen de organisatie te initiëren en te beheersen.*	10.4 & 9.1
6.2	Mobiele apparatuur en telewerken *Doelstelling: Het waarborgen van de veiligheid van telewerken en het gebruik van mobiele apparatuur.*	Nvt
7	Veilig personeel	
7.1	Voorafgaand aan het dienstverband *Doelstelling: Waarborgen dat medewerkers en contractanten hun verantwoordelijkheden begrijpen en geschikt zijn voor de functies waarvoor zij in aanmerking komen.*	10.4 & 9.1 & 10.5
7.2	Tijdens het dienstverband *Doelstelling: Ervoor zorgen dat medewerkers en contractanten zich bewust zijn van hun verantwoordelijkheden op het gebied van informatiebeveiliging en deze nakomen.*	10.4 & 9.1
7.3	Beëindiging van het dienstverband *Doelstelling: Het beschermen van de belangen van de organisatie als onderdeel van de wijzigings- of beëindigingsprocedure van het dienstverband.*	10.4 & 9.1
8	Beheer van bedrijfsmiddelen	
8.1	Verantwoordelijkheid voor bedrijfsmiddelen *Doelstelling: bedrijfsmiddelen van de organisatie identificeren en passende verantwoordelijkheden ter bescherming definiëren.*	10.4 & 9.1
8.2	Informatieclassificatie *Doelstelling: Bewerkstelligen dat informatie een passend beschermingsniveau krijgt dat in overeenstemming is met het belang ervan voor de organisatie.*	10.4 & 9.1
8.3	Behandelen van media *Doelstelling: Onbevoegde openbaarmaking, wijziging, verwijdering of vernietiging van informatie die op media is opgeslagen voorkomen.*	10.4 & 9.1
9	Toegangsbeveiliging	
9.1	Bedrijfseisen voor toegangsbeveiliging *Doelstelling: Toegang tot informatie en informatieverwerkende faciliteiten beperken*	10.4 & 9.1
9.2	Beheer van toegangsrechten van gebruikers *Doelstelling: Toegang voor onbevoegde gebruikers bewerkstelligen en onbevoegde toegang tot systemen en diensten voorkomen.*	10.4 & 9.1
9.3	Gebruikersverantwoordelijkheden *Doelstelling: Gebruikers verantwoordelijk maken voor het beschermen van hun authenticatie-informatie*	10.4 & 9.1
9.4	Toegangsbeveiliging van systeem en toepassing *Doelstelling: Onbevoegde toegang tot systemen en toepassingen voorkomen*	10.4 & 9.1
10	Cryptografie	
10.1	Cryptografische beheersmaatregelen *Doelstelling: Zorgen voor correct en doeltreffend gebruik van cryptografie om de vertrouwelijkheid, authenticiteit en/of integriteit van informatie te beschermen*	Aanvullend
11	Fysieke beveiliging en beveiliging van de omgeving	
11.1	Beveiligde gebieden *Doelstelling: Onbevoegde fysieke toegang tot, schade aan en interferentie met informatie en informatieverwerkende faciliteiten van de organisatie voorkomen.*	5 & 6
11.2	Apparatuur	5 & 6

	Doelstelling: Verlies, schade, diefstal of compromittering van bedrijfsmiddelen en onderbreking van de bedrijfsvoering van de organisatie voorkomen.	
12	Beveiliging bedrijfsvoering	
12.1	Bedieningsprocedures en verantwoordelijkheden *Doelstelling: Correcte en veilige bediening van informatieverwerkende faciliteiten waarborgen*	10.4 & 9.1
12.2	Bescherming tegen malware *Doelstelling: Waarborgen dat informatie en informatieverwerkende faciliteiten beschermd zijn tegen malware*	Aanvullend
12.3	Back-up *Doelstelling: Beschermen tegen het verlies van gegevens*	10.4 & 9.1
12.4	Verslaglegging en monitoren *Doelstelling: Gebeurtenissen vastleggen en bewijs verzamelen*	10.4 & 9.1
12.5	Beheersing van operationele software *De integriteit van operationele systemen waarborgen*	Aanvullend
12.6	Beheer van technische kwetsbaarheden *Doelstelling: Benutting van technische kwetsbaarheden voorkomen*	Aanvullend
12.7	Overwegingen betreffende audits van informatiesystemen *Doelstelling: De impact van auditactiviteiten op uitvoeringssystemen zo gering mogelijk maken.*	Nvt
13	Communicatiebeveiliging	
13.1	Beheer van netwerkbeveiliging *Doelstelling: De bescherming van informatie in netwerken en de ondersteunende informatieverwerkende faciliteiten waarborgen.*	10.4 & 9.1 & 5 & 6
13.2	Informatietransport *Doelstelling: Handhaven van de beveiliging van informatie die wordt uitgewisseld binnen een organisatie met een externe entiteit.*	Aanvullend
14	Acquisitie, ontwikkeling en onderhoud van informatiesystemen	
14.1	Beveiligingseisen voor informatiesystemen *Doelstelling: Waarborgen dat informatiebeveiliging integraal deel uitmaakt van informatiesystemen in de gehele levenscyclus. Hiertoe behoren ook de eisen voor informatiesystemen die diensten verlenen via openbare netwerken.*	Nvt
14.2	Beveiliging in ontwikkelings- en ondersteunende processen *Doelstelling: Bewerkstelligen dat informatiebeveiliging wordt ontworpen en geïmplementeerd binnen de ontwikkelingslevenscyclus van informatiesystemen.*	Nvt
14.3	Testgegevens *Doelstelling: Bescherming waarborgen van gegevens die voor het testen zijn gebruikt*	Nvt
15	Leveranciersrelaties	
15.1	Informatiebeveiliging in leveranciersrelaties *Doelstelling: De bescherming waarborgen van bedrijfsmiddelen van de organisatie die toegankelijk zijn voor leveranciers*	10.4 & 9.1
15.2	Beheer van dienstverlening van leveranciers *Doelstelling: Een overeengekomen niveau van informatiebeveiliging en dienstverlening in overeenstemming met de leveranciersovereenkomsten handhaven.*	10.4 & 9.1
16	Beheer van informatiebeveiligingsincidenten	
16.1	Beheer van informatiebeveiligingsincidenten en -verbeteringen *Doelstelling: Een consistente en doeltreffende aanpak bewerkstelligen van het beheer van informatiebeveiligingsincidenten, met inbegrip van communicatie over beveiligingsgebeurtenissen en zwakke plekken in de beveiliging.*	Aanvullend
17	Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer	
17.1	Informatiebeveiligingscontinuïteit *Doelstelling: Informatiebeveiligingscontinuïteit moet worden ingebed in de systemen van het bedrijfscontinuïteitsbeheer van de organisatie*	10.4 & 9.1
17.2	Redundante componenten *Doelstelling: Beschikbaarheid van informatieverwerkende faciliteiten bewerkstelligen*	10.4 & 9.1
18	Naleving	
18.1	Naleving van wettelijke en contractuele eisen *Doelstelling: Voorkomen van schendingen van wettelijke, statutaire, regelgevende of contractuele verplichtingen betreffende informatiebeveiliging en beveiligingseisen*	10.4
18.2	Informatiebeveiligingsbeoordelingen *Doelstelling: Verzekeren dat informatiebeveiliging wordt geïmplementeerd en uitgevoerd in overeenstemming met de beleidsregels en procedures van de organisatie*	10.4 & 9.1

Tabel 8

Deze matrix brengt de verschillende normen tot stand met betrekking tot serviceprocessen die de alarmcentrale aan haar klanten levert. Om de processen in een veilige operatie te archiveren, worden de standaarden voor het managen van de business en ICT-risico's links op de matrix gezet. De correlatie in de matrix geeft een overzicht van overlappende en aanvullende eisen tussen de verschillende standaarden en scopes. Het proces moet voldoen aan de eisen van "A.14.2 Beveiliging in ontwikkelings- en ondersteuningsprocessen" van ISO 27001 of de IEC 62443-4-1.

7.4 Kruisverwijzing ISO 9001 naar ISO/IEC 27001 en EN 50518 - G

EN-ISO 9001	ISO/IEC 27001	EN50518
Quality management systems – Requirements	**Information technology - Security techniques - Information security management systems - Requirements**	**Monitoring and alarm receiving centre**
4. Context of the organization	4. Context of the organization	1. Scope
5. Leadership	5. Leadership	10.1 General Principles leadership 10.2 Governance and Strategy 10.3 Legal and operational set-up
6. Planning - Actions to address risks and opportunities - Quality objectives and planning to achieve them - Planning of changes	6. Planning - Actions to address risks and opportunities - Quality objectives and planning to achieve them	Planning 4.1. Categorization 4.2. Site selection 10.4 Management System. - Risk and Contingency Management. - Information Management. - Complaint Handling. - Management of the Services Portfolio. - Management of Staffing. - Client Management. - Business Partner Management.
7. Support - Resources - Competence - Awareness - Communication	7. Support - Resources - Competence - Awareness - Communication	Support – Resources & Competence 5. Construction 6. Alarm systems of the ARC 7. Electrical power supplies 10.5.1. Staffing 10.5.2. Security screening and vetting 10.6 Training
8. Operation - Quality planning and control - Requirements for products and services - Design and development of products and services - Control of externally provided processes, products and services - Production and services provision - Release of products and services - Control of nonconforming outputs	8. Operation - Operational planning and control - Information security risk assessment - Information security risk treatment	Operation 8. Alarm Management System 9. Operation of the ARC 9.1 Procedures 1. General 2. Creation, modification & cancelation 3. Message handling 4. Communication with response services 5. Individual services provided by the ARC 6. Alarm verification 7. Unexpected increase in alarm signals 8. Alarm transmission path failures 10. Installation, maintenance, protection, removal and reuse of assets under the control of the ARC 11. Monitoring & testing of equipment 12. Fault procedures and reporting 13. Information management 14. Data back-up 15. Confidentiality and classification of information 16. Relationships with essential suppliers 17. Administrative procedures 18. Physical access 19. Remote access 20. Operational continuity and emergencies 21. Emergency evacuation and re-entry 22. Emergency entry

9. Performance evaluation - Monitoring , measurement , analyses & evaluation - Internal audit - Management review	9. Performance evaluation - Monitoring , measurement , analyses & evaluation - Internal audit - Management review	9.2 Performance criteria – message handling 9.1.9 . Controls to maintain QoS 9.1.23 KPI
10. Improvement	10. Improvement	

Tabel 9

7.5 Bedrijfscontinuïteit - G

De volgende paragrafen hebben betrekking op de bedrijfscontinuïteit van een MARC.

Clause	Subject
5.9.1	Communication cables
9.1.9	Controls to maintain quality of service
9.1.16	Relationships with essential suppliers
9.1.20	Operational continuity and emergencies
9.1.23	Key performance indicators
9.2	Performance criteria: Message handling
10.2	Governance and strategy
10.4	Management system

Tabel 10

8 Alarm Transmissie Service Provider

8.1 Algemeen - G

Een Alarm Transmissie Service Provider (ATSP) is de entiteit die verantwoordelijk is voor het bewaken van de prestaties van het Alarm Transmission System (ATS) volgens EN 50136-1 / A1. De taak voor de monitoring van de ATS wordt uitgevoerd door een Monitoring Centrale volgens EN 50518.

De ATSP houdt documentatie bij die voldoende is voor planning, installatie, inbedrijfstelling, service en bediening van de ATS.

Instructies voor alarmtransmissieapparatuur (ATE) moeten zodanig zijn gestructureerd dat ze de toegangsniveaus van het verschillende type gebruikers weerspiegelen. Zie de toegangsniveaus in EN50136-1 / A1 als weerspiegeling van de toegangsniveaus in EN50131-1.

De MC kan de ATSP assisteren bij de inbedrijfstelling, service en bediening van de ATS. De MC heeft een Alarm Management Systeem (AMS) om zijn taken uit te voeren. De MC ontvangt zijn informatie van de Receiving Center Transceiver (RCT). De functies van de RCT volgens EN50136-3 zullen gedeeltelijk worden vervuld door de AMS. Controleer deze functies volgens EN50136-3 binnen de AMS naast de vereisten van de AMS volgens EN50518.

Als de ATSP een gemeenschappelijk protocol volgens TS 50136-9 gebruikt, moet dit interageren met de vereisten in EN50136-1 / A1 over inbedrijfstelling en verbindingsinstellingen.

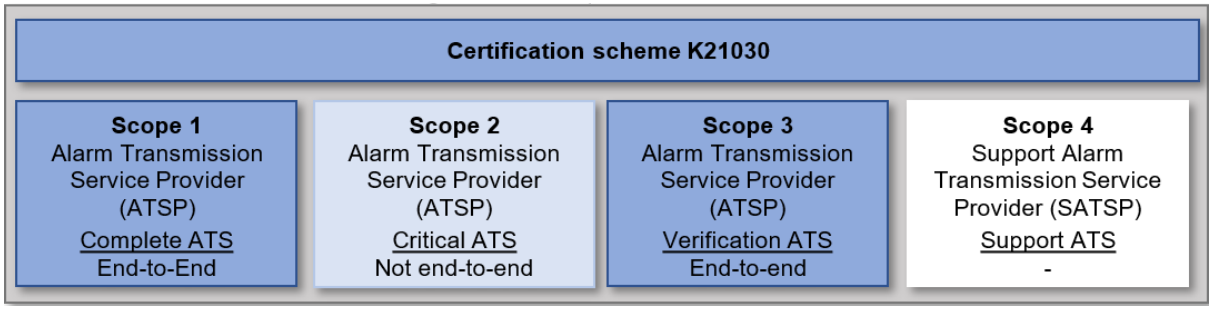
Onderstaande tabel geeft de relevantie weer tussen de standaarden die bij de uitvoering in acht moeten worden genomen.

EN 50136-1/A1	TS 50136-9	EN 50518:2019
5 General requirements		
6 System requirements	4 Objective 5 Messaging 6 Message types	8 Alarm Management System
7 Verification of performance		
8 Documentation sufficient for planning, installation, commissioning, service and operation	7 Commissioning and connection setup	9 Operation of the ARC 10.4 Complaint handling 10.4 Compliance audit 10.5 Staffing

Tabel 11 relevantie tussen de normen

8.2 K21030 Alarm Transmission Systems - Alarm Transmission Service Providers - G

Certificatieschema K21030 is gemaakt door Kiwa voor de certificering van alarmtransmissiesystemen en alarmtransmissiedienstverleners. De regeling is verdeeld in vier scopes. Zie voor meer informatie het certificatieschema K21030.



8.2.1 Scope 1

Scope 1 is de certificering van een compleet alarmtransmissiesysteem (ATS) van Supervised Premises Transceiver (SPT) naar Receiving Center Transceiver (RCT) en de volledige verantwoordelijkheid. Deze reikwijdte is end-to-end.

8.2.2 Scope 2

Scope 2 is de certificering van het critical alarm transmission system (ATS). Deze reikwijdte is voornamelijk toepasbaar in gehoste situaties en omvat de verbinding tussen de Receiving Centre Transceivier Hosted (RCT-H) en de Receiving Centre Transceiver in de ARC (RCT-A) en de volledige verantwoordelijkheid. Deze reikwijdte is niet end-to-end.

8.2.3 Scope 3

Scope 3 is de certificering van verificatie alarmtransmissiesystemen (ATS) van Supervised Premises Transceiver (SPT) naar Receiving Center Transceiver (RCT) en omvat alleen verificatie van prestaties en rapportage aan de klant. Deze reikwijdte is end-to-end.

8.2.4 Scope 4

Scope 4 is de certificering van ondersteuning geleverd aan een alarmtransmissiedienstverlener.

9 VSS Control Room / Videotoezichtcentrale

9.1 Hoofdstuk 12 - Control room configuratie - G

Zoals vermeld in hoofdstuk 2, verwijst EN 50518 naar EN-IEC 62676-4 voor videobewakingssystemen (VSS). Het doel van dit deel van IEC 62676 is om richtlijnen te geven over hoe ervoor te zorgen dat videobewakingssystemen (VSS) voldoen aan hun functionele en prestatie-eisen. Hoofdstuk 12 bevat de VSS-controlekamerconfiguratie.

De EN-IEC 62676-4 vermeldt het volgende:

If the VSS has a requirement for live viewing, camera control, system management, or any other human intensive tasks, a control room should be specified to house these functions. The 'control room' could be a single workstation, or a large operations centre.

Naast de configuratie van de werkstations vereist de norm ook back-up stroom en bliksem- en overspanningsbeveiliging. Beide items zijn al voorzien in EN 50518.

9.2 Het aansluiten van een VSS op een VSS control room - G

Bij het aansluiten op een VSS control room moeten het doel en de parameters van het videosysteem helder bepaald zijn. Deze informatie is benodigd voor de VSS control room voor een goede kwaliteit van de dienstverlening. De benodigde informatie is benoemd in hoofdstuk 4 en 5 van de EN-IEC 62676-4. Deze hoofdstukken zijn verplicht bij het aansluiten op een VSS control room.

9.2.1 Hoofdstuk 4 - General considerations - G

Dit hoofdstuk bevat algemene overwegingen voordat u een VSS gaat ontwerpen. Dit bevat:

- Risk assessment - risicoanalyse;
- Security grading – bepalen van de grade;
- Operational requirements – operationele eisen;
- Site survey - locatiebeoordeling;
- System design and site plan – systeem ontwerp en plattegrond;
- Developing the test plan – ontwikkelen van het testplan;
- Installation, commission and hand over - installatie, inbedrijfstelling en overdracht;
- Documenting the system - Documenteren van het systeem.

9.2.2 Hoofdstuk 5 - Operational requirements specifications - G

Dit hoofdstuk bevat operationele vereisten met betrekking tot de specificaties van de VSS. Het doel van deze operationele eisen is dat duidelijk wordt aangegeven wat de klant verwacht dat de functies van het systeem doen. Zonder duidelijk gedefinieerde operationele vereisten is er geen praktische methodologie om te beoordelen of het systeem aan het vereiste doel kan voldoen. De operationele vereisten omvatten:

- Basic objective/functionalities - basisdoel / functionaliteiten;
- Definition of surveillance limitations - definitie van surveillance beperkingen ;
- Definition of the site(s) under surveillance - definitie van de site (s) onder toezicht;
- Definition of activity to be captured - definitie van de vast te leggen activiteit;
- System/picture performance - systeem- / beeldprestaties;
- Period of operation – periode waarin het systeem in bedrijf is;
- Conditions at the location – voorwaarden op de locatie;
- Resilience – veerkracht;
- Monitoring and image storage - monitoring en beeldopslag;
- Exporting images – beelden exporten;
- Routine actions – routine handelingen;

- Operational response – operationele reactie;
- Operator workload – werklast van de operator;
- Training – opleiding;
- Expansions - uitbreidingen;
- Lijst met andere speciale factoren die niet onder het bovenstaande vallen
- Automation - Automatisering;
- Alarm response – alarm reactie;
- System response times – reactietijden van het systeem.

9.3 VSS control room beoordeling - R

Wanneer een beoordeling op basis van scope VSS in beveiligingstoepassingen gewenst is, zal Kiwa de VSS Control Room configuratie beoordelen op hoofdstuk 12. Aangesloten VSS zullen worden beoordeeld op basis van hoofdstuk 4 en 5. De beoordeling omvat een initiële steekproef van 2 en een opvolgingssteekproef van drie projecten. De steekproef van projecten is gebaseerd op de afgesproken documentatie en de beelden in de VSS Control Room. Er zijn geen locatiebezoeken nodig.

10 Guidance op remote access/apps en portals

10.1 Remote toegang en de risico’s

Het op afstand verkrijgen van toegang tot IT-systemen brengt ook potentiële risico's met zich mee als de inrichting en configuratie hiervan onvoldoende is. Enkele belangrijke risico's zijn:

1. Beveiligingslekken: Het openen van externe toegang kan mogelijk beveiligingslekken in IT-systemen introduceren, waardoor kwaadwillenden kunnen proberen toegang te krijgen tot gevoelige gegevens of schadelijke activiteiten kunnen uitvoeren.

2. Ongewenste toegang: Als de juiste beveiligingsmaatregelen niet worden geïmplementeerd, kan het op afstand verkrijgen van toegang het risico met zich meebrengen dat onbevoegde personen toegang krijgen tot systemen of gegevens.

3. Zwakke wachtwoorden: Slechte wachtwoordbeveiliging kan het risico vergroten dat kwaadwillenden wachtwoorden raden, kraken of onderscheppen om toegang te krijgen tot systemen.

4. Kwaadaardige software: Het op afstand verkrijgen van toegang kan de mogelijkheid bieden voor kwaadwillenden om schadelijke software te installeren of te activeren op het systeem, wat kan leiden tot gegevensverlies, systeemstoringen of andere vormen van schade.

5. Gegevensinbreuken: Als er geen passende beveiligingsmaatregelen zijn getroffen, kan het op afstand toegang krijgen tot IT-systemen leiden tot gegevensinbreuken, waarbij gevoelige informatie wordt blootgesteld aan ongeautoriseerde personen.

Om deze risico's te beperken, is het belangrijk om sterke beveiligingsmaatregelen toe te passen, zoals het gebruik van sterke wachtwoorden, tweefactorauthenticatie, regelmatige systeemupdates, firewalls en gegevensversleuteling. Daarnaast is het belangrijk om alleen betrouwbare en beveiligde verbindingen te gebruiken voor externe toegang en om de toegangsrechten zorgvuldig te beheren.

Voorbeeld van een hack op basis van remote toegang met consequenties:

Het fictieve bedrijf ABC had remote access tot zijn IT-systemen mogelijk gemaakt voor zijn leveranciers om op afstand service te kunnen uitvoeren. Helaas werd het bedrijf het slachtoffer van een hack die ernstige gevolgen had kunnen hebben.

In dit scenario maakte een kwaadwillende hacker gebruik van zwakke beveiligingsmaatregelen en een ongepatchte kwetsbaarheid / slecht ingericht Identity and Access Management (IAM) in de remote access-infrastructuur van het bedrijf. De hacker kon zo ongeautoriseerde toegang krijgen tot de interne systemen van het bedrijf, waaronder de XYZ.

De consequenties van een dergelijke hack kunnen significant zijn. Het kan leiden tot:

1. Gegevensdiefstal: De hacker kan toegang krijgen tot de klantendatabases en gevoelige gegevens stelen. Dit kan persoonlijke identificeerbare informatie (PII) van klanten, omvatten zoals namen, adressen, BSN-nummers en financiële transactiegegevens. Deze gegevensdiefstal brengt het risico met zich mee van identiteitsdiefstal en potentieel misbruik van klanten.

2. Financiële schade: De hacker krijgt toegang tot de financiële systemen van het bedrijf. Hierdoor kan hij frauduleuze transacties uitvoeren, geld overmaken naar externe accounts en de financiële integriteit van het bedrijf in gevaar brengen. Het bedrijf kan aanzienlijke financiële verliezen als gevolg van deze hack leiden.

3. Reputatieschade: Nieuws over een hack verspreidt zich snel, waardoor het vertrouwen van klanten en zakelijke partners in het bedrijf ernstig geschaad kunnen worden. Het bedrijf krijgt te maken met

negatieve publiciteit, klantverloop en verlies van nieuwe zakelijke kansen. De reputatieschade is aanzienlijk en kost het bedrijf veel tijd en moeite om het vertrouwen van de stakeholders te herstellen.

4. Regulatoire consequenties: Het bedrijf is onderhevig aan strikte regelgeving en nalevingsvereisten. De hack kan leiden tot schendingen van deze vereisten, wat resulteert in onderzoeken, boetes en mogelijke juridische procedures van toezichthoudende instanties.

Een dergelijk incident benadrukt het belang van robuuste beveiligingsmaatregelen, regelmatig patchen en monitoring van remote access-systemen (SOC, SIEM, SOAR, etc), evenals het belang van een adequaat responsplan voor incidenten.

Het bedrijf moet daarom zijn beveiligingsmaatregelen adequaat inrichten, extra beveiligingslagen implementeren en investeren in cybersecuritytraining en -bewustzijn om toekomstige hacks te voorkomen.

Het implementeren van ISO27001 kan hierbij als basis dienen.

10.2 Apps, appserver, webserver en webportals

Remote toegang beperkt zich niet tot de toegang van leveranciers en medewerkers, maar steeds vaker geven apps en portals ook remote toegang via servers. Waar hieronder wordt gesproken over apps en webportals, dienen ook de app- en webservers te worden beschouwd in de keten. Slecht ontwikkelde apps(servers), webservers en webportals kunnen verschillende risico's met zich meebrengen, waaronder:

1. Beveiligingskwetsbaarheden: Als een app of webportal slecht is ontwikkeld, kunnen er kwetsbaarheden in de code aanwezig zijn. Dit kan leiden tot beveiligingslekken, waardoor kwaadwillenden toegang kunnen krijgen tot gevoelige gegevens of schadelijke activiteiten kunnen uitvoeren.

2. Gegevensinbreuken: Slecht ontwikkelde apps en webportals kunnen leiden tot gegevensinbreuken, waarbij onbevoegde personen toegang krijgen tot persoonlijke of vertrouwelijke informatie. Dit kan ernstige gevolgen hebben, zoals identiteitsdiefstal of financiële schade.

3. Slechte gebruikerservaring: Als een app of webportal niet goed is ontworpen of onvoldoende gebruiksvriendelijk is, kan dit leiden tot frustratie bij gebruikers. Slechte prestaties, onduidelijke navigatie, trage laadtijden en andere usability-problemen kunnen ervoor zorgen dat gebruikers de app verlaten of de webportal niet meer gebruiken.

4. Instabiliteit en fouten: Slechte ontwikkelingspraktijken kunnen resulteren in instabiele apps en webportals die vaak crashen of fouten vertonen. Dit kan de bruikbaarheid van de app of webportal negatief beïnvloeden en het vertrouwen van gebruikers verminderen.

5. Slechte integratie en compatibiliteitsproblemen: Als een app of webportal niet goed is ontwikkeld met betrekking tot integratie met andere systemen of apparaten, kunnen er compatibiliteitsproblemen ontstaan. Dit kan leiden tot functionaliteitsverlies, gegevensverlies of verminderde prestaties.

Om deze risico's te verminderen, is het belangrijk dat apps en webportals worden ontwikkeld volgens best practices op het gebied van beveiliging, codekwaliteit, gebruikerservaring en compatibiliteit. Regelmatige beveiligingsaudits, code-reviews en testsessies kunnen helpen om kwetsbaarheden en fouten te identificeren voordat de app of webportal wordt uitgerold naar gebruikers. Bovendien is het van cruciaal belang om de privacy van gebruikers te waarborgen en te voldoen aan relevante wet- en regelgeving, zoals de Algemene Verordening Gegevensbescherming (AVG).

Maatregelen

Voor de beveiliging van apps, appservers, webportals en webservers moeten verschillende logische beveiligingsmaatregelen worden toegepast. Hier zijn enkele belangrijke maatregelen:

1. Authenticatie en autorisatie: Implementeer een robuust authenticatie- en autorisatiesysteem om ervoor te zorgen dat alleen geautoriseerde gebruikers toegang hebben tot de app of webportal. Gebruik sterke wachtwoorden, tweefactorauthenticatie en beperk de toegangsrechten op basis van de rol van de gebruiker. Zie EN 50518 9.1.19

2. Gegevensversleuteling: Versleutel gevoelige gegevens, zowel tijdens de opslag als tijdens de overdracht. Dit helpt de vertrouwelijkheid van de gegevens te waarborgen, zelfs als ze in verkeerde handen vallen.

3. Inputvalidatie: Voer strikte validatie van gebruikersinvoer uit om mogelijke aanvallen zoals SQL-injectie en cross-site scripting (XSS) te voorkomen. Dit voorkomt dat kwaadwillende gebruikers schadelijke code injecteren of misbruik maken van zwakke punten in de app of webportal.

4. Beperking van toegangsrechten: Beperk de toegangsrechten van de app of webportal tot wat strikt noodzakelijk is. Geef gebruikers alleen toegang tot de functionaliteiten en gegevens die ze daadwerkelijk nodig hebben om hun taken uit te voeren. Hierdoor wordt het risico van misbruik of ongeoorloofde toegang beperkt. Zie EN 50518 Annex B.

5. Beveiligde sessiebeheer: Implementeer beveiligd sessiebeheer om ervoor te zorgen dat sessies veilig worden geauthenticeerd en beheerd. Gebruik bijvoorbeeld unieke sessie-identificatoren, zorg voor een veilige overdracht van sessiegegevens en stel een tijdslimiet in voor sessies om inactiviteit te beheren. Zie EN 50518 Annex B.

6. Audit logs en monitoring: Implementeer logging en monitoring van activiteiten binnen de app of webportal. Dit helpt bij het detecteren van verdachte activiteiten, beveiligingsinbreuken of ongeautoriseerde toegang. Houd logs bij van gebruikersacties, fouten en beveiligingsgebeurtenissen voor analyse en forensisch onderzoek. Zie EN 50518 9.1.19

7. Reguliere updates en patches: Zorg voor regelmatige updates en patches van de app of webportal om beveiligingslekken te verhelpen en kwetsbaarheden aan te pakken. Houd de gebruikte softwareframeworks, bibliotheken en andere componenten up-to-date om bekende beveiligingsproblemen te vermijden. Zie EN 50518 9.1.13

Het is ook essentieel om de beveiligingsrichtlijnen en beste praktijken van relevante organisaties en standaarden te volgen, zoals OWASP (Open Web Application Security Project), om ervoor te zorgen dat de beveiligingsmaatregelen effectief en actueel zijn.

Het haakje voor de bovenstaande maatregelen zit in de EN 50518 artikel 9.1.19, die luidt:

The procedure shall describe how remote access to and from any system within the ARC and to the receiving data processing equipment (see 5.8) shall be controlled by a log-in / log-out procedure recording time and date, credentials of the person involved and actions performed. Remote access can only be granted by authorization of the ARC. See annex B for further information related to remote system access.

Laten we het artikel ontleden:

Wat is data processing equipment gebaseerd op EN 50518 5.8:

- Interface of the AMS for interconnection with the RCT (iRCT) *(Front end processor/signal processor);*
- Servers of the alarm management system (databases, storages);
- Voice recording equipment;
- Active network components (routers, switches);
- Passive network components (patch panels, cabling);
- Communication equipment (PABX)
- Internal transfer point LAN / WAN

Wat betekent: authorization of the ARC

De ARC kan werknemers en/of leveranciers autoriseren om toegang op afstand te krijgen door middel van:

- Hen te laten bellen naar het ARC om toegang te krijgen;

- Het maken van een contract/SLA met randvoorwaarden om toegang te krijgen tot de ARC onder bepaalde voorwaarden met beveiligingsafspraken;

Wat betekent: Log-in / Log-out procedure recording time and date, credentials of the persons involved and actions performed

De leverancier of werknemer moet geautoriseerd zijn door de ARC en het moet bekend zijn wanneer toegang op afstand wordt gebruikt. Dit moet worden vastgelegd in de applicatie of remote access server met vermelding van tijd en datum en de referenties.

Wat is: Annex B EN 50518 (informative)

EN 50518 annex B geeft handvatten voor het invullen van artikel 9.1.19 van de EN 50518 met ook het oog op ISO 27001 specifiek voor ARC data. Dit artikel is dus van toepassing bijvoorbeeld als een leverancier, installateur of klant toegang kan krijgen tot het AMS en de functies middels remote access, een app of portal. Let op: dit betreft een informatief artikel.

10.3 Guidance plan van aanpak remote access

1. Identificatie van bedrijfskritieke systemen: Het bedrijf identificeert eerst de systemen die van cruciaal belang zijn voor hun bedrijfsvoering. Dit omvat mogelijk servers voor gegevensopslag, interne communicatiesystemen, financiële systemen en klantendatabases.

2. Evaluatie van potentiële dreigingen: Het bedrijf analyseert de potentiële dreigingen waarmee ze te maken kunnen krijgen bij het openstellen van remote access. Dit omvat dreigingen zoals ongeoorloofde toegangspogingen, malware-infecties, phishing-aanvallen en datadiefstal.

3. Beoordeling van bestaande beveiligingsmaatregelen: Het bedrijf evalueert de huidige beveiligingsmaatregelen die al zijn geïmplementeerd om de IT-systemen te beschermen. Dit omvat zaken zoals firewalls, antivirussoftware, intrusion detection/prevention-systemen en gegevensversleuteling.

4. Identificatie van kwetsbaarheden: Het bedrijf voert een grondige beoordeling uit van de kwetsbaarheden in hun IT-infrastructuur. Dit omvat het identificeren van eventuele verouderde software, configuratiefouten, zwakke wachtwoorden en mogelijke misconfiguraties in de systemen.

5. Risicobeoordeling: Het bedrijf evalueert de geïdentificeerde dreigingen en kwetsbaarheden in termen van hun impact en waarschijnlijkheid. Hierdoor kunnen ze de potentiële risico's van remote access tot IT-systemen beter begrijpen en prioriteiten stellen voor risicobeheersing.

6. Risicobeheersing: Op basis van de risicobeoordeling neemt het bedrijf passende maatregelen om de geïdentificeerde risico's te beheersen. Dit omvat het implementeren van aanvullende beveiligingsmaatregelen, zoals sterke authenticatie, netwerksegmentatie, regelmatige systeemupdates, beveiligingsbewaking en bewustmakingsprogramma's voor medewerkers.

7. Periodieke evaluatie en herziening: Het bedrijf plant regelmatige evaluaties en herzieningen van de risico-inschatting om ervoor te zorgen dat de beveiligingsmaatregelen up-to-date blijven en in lijn zijn met de veranderende dreigingslandschappen en bedrijfsbehoeften.

Door deze risico-inschattingsaanpak kan Bedrijf XYZ de potentiële risico's van remote access tot IT-systemen begrijpen en de juiste maatregelen implementeren.

Bijlage 1: Matrix brandwerende doorvoeren - G

Om voldoende positief bewijsmateriaal te kunnen opschrijven, wordt er als voorbeeld een tabel per brandwerende doorvoer ingevuld.

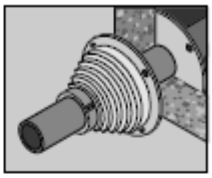
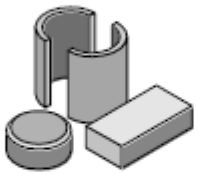
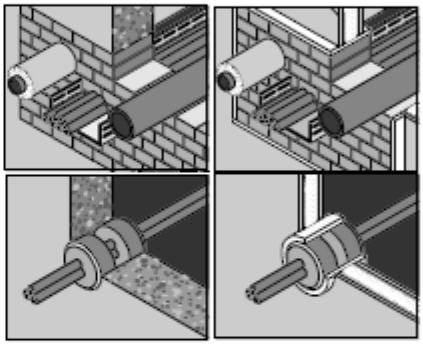
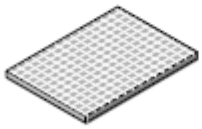
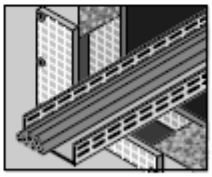
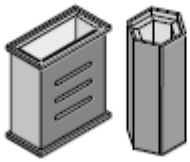
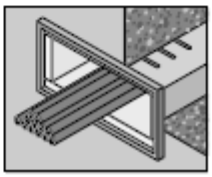
Doorvoer - Nummer		
Locatie	Locatie-identificatie vanaf de doorvoer op een kaart..	
Foto's	Voor het aanbrengen	Na aanbrengen
Originele scheiding	Materiaal en brandwerendheid.	
Doorvoer	Kabel (s) / buis (materiaal) / medium in buis..	
Type afdichting	Zie tabel 1-1 in ETAG26-2. Let op voor buismateriaal. Het moet duidelijk zijn dat het type penetratie-afdichting volgens de attestatie van het productcertificaat in staat is om deze in geval van brand uit te knijpen. Geef dit aan in de matrix door specifiek te verwijzen waar dit in het certificaat staat..	
Leverancier, product, certificaat	Noem de fabrikant, het product en welk certificaat het product heeft. EAD van ETAG-certificaat.	
Leveranciersrichtlijnen per brandwerende doorvoer	Geef aan waar dit specifiek staat vermeld in het certificaat en / of de montagehandleiding van de fabrikant. Besteed bijzondere aandacht aan de criteria voor de maximale afstand tussen de kabel (s) en / of buizen en de relevante originele muur en de montage-instructies voor de kabels / buizen. Maak ook duidelijk hoe ver de coating moet worden aangebracht op de kabels / buizen per specifieke penetratie..	
De persoon die de doorvoerafdichting heeft geïnstalleerd	Naam.	
De persoon die de juiste aanbreng heeft gecontroleerd	Naam.	

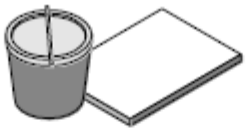
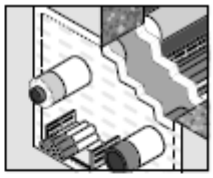
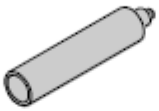
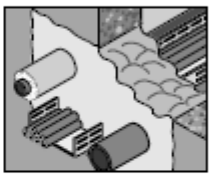
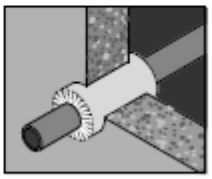
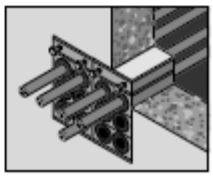
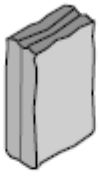
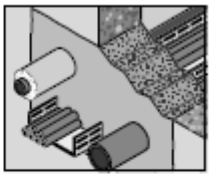
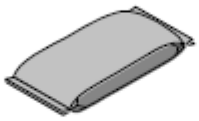
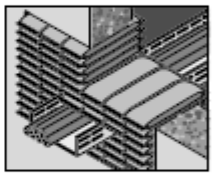
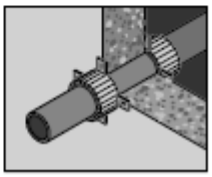
Zie tabel 1-1 in ETAG26-2. Let op voor buismateriaal. Het moet duidelijk zijn dat het type penetratie-afdichting volgens de attestatie van het productcertificaat in staat is om deze in geval van brand uit te knijpen. Geef dit aan in de matrix door specifiek te verwijzen waar dit in het certificaat staat.

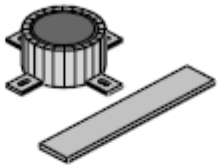
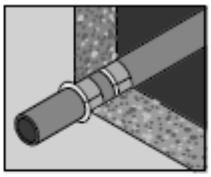
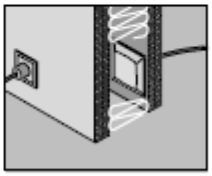
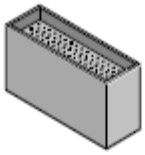
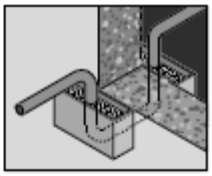
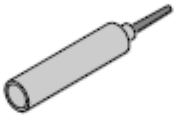
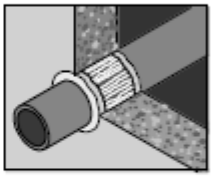
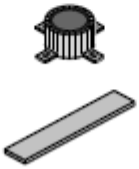
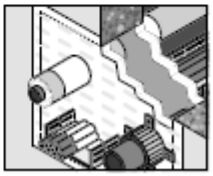
Belangrijk is de installatierichtlijn van de gebruikte producten. De instructies van de fabrikant moeten worden opgevolgd om dezelfde prestaties te garanderen als tijdens de test. Afhankelijk van de instructies van de fabrikant moet de applicatie aan de binnen- of buitenkant van de schaal worden gedaan.

Het is ook belangrijk dat de applicator wordt opgeleid in de context van de gebruikte producten. Ook moet de inschrijving van het onderwijs worden verstrekt.

Table 1.1 ETAG 26-2

Designation	Illustration [1] of the	
	product/component	penetration seal
Bellows seals		
Blocks, plugs		
Boards		
Cable boxes		

Coated mineral wool slabs (e.g. intumescent or ablative coating)		
Foams		
Mineral wool		
Modular systems		
Mortar		
Pillows (also referred to as "bags" or "cushions")		
Pipe closure devices		
• Collars (integrated into or outside the wall / floor)		

• Wraps (integrated into a wall or floor) including strips and composite strips		
• Mechanically actuated systems for pipes	variable	variable
Putties		
Sand gaskets		
Sealants/Mastics		
Combinations of the products named above		

Bijlage 2: Mapping matrix EN50518 en relevante normen met additionele toepassingen - G

European standard	EN50518	EN-IEC 62676-4: 2015	IEC 60839-11-2: 2014	K21023	EN50136-1/A1 K21030	CLC/TS 50134-7:	ISO/IEC 27039; 2015	TS54-14: 2004
Name of the standard	Monitoring and alarm receiving centre	Video surveillance systems for use in security applications - Part 4: Application guidelines	Alarm & electronic security systems - Part 11-2: Electronic access control systems - Application guidelines	Mobile Security – Security of mobile objects and persons	Alarm Transmission Service Provider	Alarm systems - Social alarm systems - Part 7: Application guidelines	Information technology - Security techniques - Selection, deployment and operations of intrusion detection systems (IDPS)	Fire Alarms Systems (FAS)
Paragraph	1. Scope	P1 Scope	P1 Scope	P1 Scope	P1 scope and Responsibilities	P1 Scope	P1 Scope	P1 Scope
Paragraph	Planning 4. Site selection							
Paragraph	Support – Resources & Competence 5. Construction 6. Alarm systems of the ARC 7. Electrical power supplies 4. Staffing	12 VSS control room configuration 12.1 Control rooms 12.2 Number, size and positioning of VSS video displays 12.3 Displays and screens mounted on or off the workstation 12.4 Recommended display sizes 12.5 Number of camera images per operator 12.6 Number of work stations 12.7 Equipment siting 12.8 Backup power supply provision 12.10 Lightning and surge protection		6 Product requirements 7 Requirements quality system	5 Requirements quality system	13 Sub-contract delivery of services 14 Staffing		
Paragraph	Operation 2013 P2: 4. Performance requirements P2: 5. Communication requirements P2: 6. Reception of signals P2: 7. Testing P2: 8. Data P2: 9. Data storage P2: 10. Availability and verification of performance of the ARC P2: 11. Contingency plan P3: 5. Operating procedures P3: 8. Data	12.9 Operating temperature	10.1 System operation	4 Performance requirements 5 Process requirements	5 Requirements quality system	8 Alarm receiving services 10 Response arrangements 12 Operational records 15 Risk management	6.4 Deployment 7 Operations	6.9 Signals to a fire alarm receiving station 8.2 Commissioning 11.2.2 Prevention of false alarms during routine testing

	2019 8. Alarm management system 9. Operation of the ARC 10. General principles, leadership, governance, management and staffing							
Paragraph	P3: 6. Auditing	13.3 Technical acceptance testing Annex B & C & E		7 Requirements quality system		9 Testing and maintenance		
Paragraph	P3: 7. Complaints procedure							

Bijlage 3: Reactietijden specifiek voor overgang CCV PAC

Omschrijving	Omschrijving 2	Reactietijd	Extra
Testmelding	24 uurs lijncontrole hersteld	25 uur	
Stroomstoring	Herstel stroomstoring	12 uur als er nog een backup stroom is	180s bij volledige uitval
Brandstoring	Herstel brandstoring	Zie NEN50131	
Sabotage detector	Herstel sabotage detector	prio 2	
Communicatieuitval	Herstel communicatieuitval	Eigen afspraken met klant	dubbele uitval is prio 2
Systeemstoring Algemeen	Herstel systeemstoring	180s	
Inschakeling Mislukt		180s	
Lage accuspanning	Accu laag herstel	25 uur	
Groep niet ingeschakeld	KTL (kiezer te laat)	180s	
Groep niet uitgeschakeld		180s	
Onregelmatige uitschakeling		prio 2	
Testmelding via backup		eigen afspraken met klant	
Uitloopfout		eigen afspraken met klant	
Te vroege uitschakeling		prio 2	
Zone niet hersteld		eigen afspraken met klant	
230 Volt uitval	230 volt herstel	eigen afspraken met klant	
Uitval GPRS		eigen afspraken met klant	bij dualpad 25 uur
Uitval IP		eigen afspraken met klant	bij dualpad 25 uur