

Verbeterde Risicoklassenindeling Definities beveiligingsmaatregelen

Document D03/385

Versie: 1.4

Publicatiedatum: 3 maart 2014

De Verbeterde Risicoklassenindeling wordt beheerd door:

het Centrum voor Criminaliteitspreventie en Veiligheid
Postbus 14069
3508 CS Utrecht

Alle rechten voorbehouden. Niets uit deze uitgave mag worden verveelvoudigd, opgeslagen in een geautomatiseerd gegevensbestand, of openbaar gemaakt, in enige vorm of op enige wijze, hetzij elektronisch, mechanisch, door fotokopieën opnemen, of enige andere manier, zonder voorafgaande schriftelijke toestemming van de uitgever.

Voorzover het maken van kopieën uit deze uitgave is toegestaan op grond van artikel 16B van de Auteurswet 1912 jo het besluit van 20 juni 1974, St.b. 351, zoals gewijzigd bij het besluit van 23 augustus 1985, St.b. 471 en artikel 17 Auteurswet 1912, dient men de daarvoor wettelijk verschuldigde vergoedingen te voldoen aan de Stichting Reprorecht (Postbus 882, 1180 AW Amstelveen). Voor het overnemen van gedeelte(n) uit deze uitgave in bloemlezingen, readers en andere compilatiewerken (artikel 16 Auteurswet 1912) dient men zich tot de uitgever te wenden.

All rights reserved. No part of this book may be reproduced, stored in a database or retrieval system, or published, in any form or in any way, electronically, mechanically, by print, photoprint, microfilm or any other means without prior written permission from the publisher.

Ondanks alle aan de samenstelling van deze uitgave bestede zorg, kan het Centrum voor Criminaliteitspreventie en Veiligheid geen aansprakelijkheid aanvaarden voor eventuele schade die zou kunnen voortvloeien uit enige fout die in deze uitgave zou kunnen voorkomen.

REVISIEOVERZICHT

<i>nr</i>	<i>hoofdstuk</i>	<i>paragraaf</i>	<i>ingangsdatum</i>	<i>beschrijving</i>
14/01	6 (gehele hoofdstuk)	--	1-1-2014	Hoofdstuk 6 geheel gereviseerd, aansluiting gemaakt tussen de niveaus (AL0 t/m AL3) voor de alarmtransmissie trajecten en de indeling in ATS categorieën en Security Grades die worden gehanteerd in de Nationale en Europese normen
14/02	Gehele document	--	1-1-2014	Verwijzingen als gevolg van de wijziging van hoofdstuk 6
14/03	Gehele document	--	3-3-2014	Verwijzingen naar nieuwe versies VRKI documenten maart 2014
14/04	6 (gehele hoofdstuk)	--	3-3-2014	Paragraafnummers aangepast
14/05	6 (gehele hoofdstuk)	--	3-3-2014	Categorie DP2 toegevoegd voor risicoklasse 3 voor bedrijven
14/06	6	6.4.1	3-3-2014	Tabel 3 aangepast
14/07	6	6.4.3	3-3-2014	Adviezen om de testmelding op 2 uur i.p.v. 25 uur in te stellen geschrapt
14/08	6	6.4.6	3-3-2014	Uitvoering van de verification of performance gewijzigd voor de categorieën DP2, DP3 en DP4: verification of performance conform de NEN-EN 50136-1:2012, verduidelijkt waarvoor de installateur verantwoordelijk is
14/09	6	6.4.7	3-3-2014	Uitvoering van de verification of performance gewijzigd voor de categorieën DP2, DP3 en DP4: verification of performance conform de NEN-EN 50136-1:2012
14/10	6	6.4.9.1	3-3-2014	Toelichting bij tabel 4 aangepast
14/11	6	6.6	3-3-2014	Adviezen om de testmelding op 2 uur i.p.v. 25 uur in te stellen geschrapt

INHOUDSOPGAVE

Revisieoverzicht	1
Inhoudsopgave	2
1. Inleiding.....	5
1.1 Definities	5
1.2 Maatregelen en risicoklassen	6
1.3 Partiële beveiliging bij bedrijven.....	6
1.4 Volledige beveiliging met maatwerk	6
1.5 Gelijkwaardigheid.....	7
1.6 Afwijkend beveiligingsplan	7
1.7 Afwijkend voldoen aan de eisen	7
1.8 Beoordelen van gelijkwaardigheid.....	7
1.9 Programma van eisen (PvE).....	8
1.10 Risicoanalyse	8
1.11 Beveiligingsplan.....	8
2. Organisatorische maatregelen.....	9
2.1 Indeling in niveaus	9
2.2 Niveau en omvang van de Organisatorische maatregelen	9
2.2.1 Niveau O1.....	9
2.2.2 Sleutelbeheer en -gebruik	10
2.2.3 Sluitronde.....	10
2.2.4 Merken en registreren van waardevolle zaken	10
2.2.5 Zichtbare afwezigheid voorkomen.....	10
2.2.6 Beveiligingsverlichting.....	10
2.2.7 Gebruik van compartimenten	10
2.2.8 Buren en omwonenden	10
2.2.9 Huisregels en discipline	11
2.2.10 Opklimmogelijkheden	11
2.2.11 Tuinaanleg.....	11
2.2.12 Toegangscontrole.....	11
2.2.13 Gegevensbeveiliging	11
2.2.14 Wijzigingen en omstandigheden	12
2.2.15 In - en Uitschakelregistratie bij de PAC	12
2.2.16 Up en Downloaden	12
2.2.17 Logboek	12
2.3 Niveau O2.....	13
3 Bouwkundige beveiligingsmaatregelen	13
3.1 Omvang van de bouwkundige beveiligingsmaatregelen	13
3.2 Het niveau van de bouwkundige beveiligingsmaatregelen.....	13
3.2.1 Niveau B0	13
3.2.2 Niveau B1	13
3.2.3 Niveau B2	14
3.2.4 Niveau B3	14
3.2.5 Glasafscherming / glasvervanging	14
3.2.6 Tralies, hekwerken en strekmetaal	15
4 Elektronische maatregelen	15

4.1	Omvang van de Elektronische maatregelen	15
4.2	Ontwerp en aanleg	15
4.3	Het niveau van de Elektronische maatregelen	15
4.3.1	Ed niveau	16
4.3.2	E1 niveau	16
4.3.3	E2 niveau	17
4.3.4	E3 niveau	18
4.3.5	Eisen aan alarmapparatuur:	19
4.3.6	Brandpreventie (brand) rookmelders.	20
4.3.7	Beveiligingsverlichting.....	21
4.3.8	Camerasystemen	22
4.3.9	Toegangscontrole.....	22
4.3.10	Buitendetectie	22
5.	Compartimentering en /of Meeneembeperkende maatregelen (C/M).....	22
5.1	Inleiding.....	22
5.2	Attractieve goederen	23
5.3	Normstelling.....	23
5.4	Conclusie	24
5.5	Pictogrammen, uitleg en voorbeelden	24
5.6	C/M 1 niveau prestatie-eis 3 minuten inbraakvertraging	24
5.6.1	Verplaatsen.....	24
5.6.2	Koppelen.....	24
5.6.3	Verankeren	25
5.7	C/M 2 niveau prestatie-eis 5 minuten inbraakvertraging	25
5.7.1	Kisten of kasten	25
5.7.2	Vitrines.....	26
5.7.3	Hekwerken.....	26
5.8	C/M 3 Niveau prestatie-eis 10 minuten inbraakvertraging	26
5.8.1	Compartimenten.....	26
5.8.2	Kluizen en safes	28
5.8.3	Mistgeneratoren	28
6	Alarmering.....	29
6.1	Voorgeschiedenis	29
6.1.1	Gebruikte afkortingen	29
6.2	Europese normen	30
6.3	Kenmerken	31
6.4	Aanvullende bepalingen	32
6.4.1	Alarm over IP.....	33
6.4.2	secundaire transmissieverbinding	34
6.4.3	Prestatieniveau transmissiesysteem.....	34
6.4.4	Alarmtransmissie via mobiele netwerken	34
6.4.5	VoIP / VoDSL	34
6.4.6	Verificatie van prestaties	35
6.4.7	Beschikbaarheid	35
6.4.8	Voorkeurschakeling	36
6.4.9	Indeling alarmtransmissiesystemen in de VRKI	36
6.4.9.1	Woningen enkelpadig alarmtransmissiesysteem.....	36

6.4.9.2	Woningen dubbelpadig alarmtransmissiesysteem	37
6.4.9.3	Bedrijven enkelpadig alarmtransmissiesysteem	38
6.4.9.4	Bedrijven dubbelpadig alarmtransmissiesysteem	39
6.5	SP1 = optioneel (AL0) traject.....	40
6.6	SP2 en DP1 (AL1) traject	40
6.7	DP2 (voorheen AL1) traject.....	40
6.8	DP3 (AL2) traject	41
6.9	DP4 (AL3) traject.....	41
6.10	Tips om nodeloos alarm te voorkomen	41
6.10.1	Bij aanschaf	41
6.10.2	Nieuwe alarminstallatie in gebruik nemen	41
6.10.3	Toch nodeloos alarm?.....	42
6.10.4	Voorkom nodeloos alarm	42
7	Reactie (alarmopvolging)	42
7.1	Indeling in niveaus	42
7.2	R0 niveau	42
7.3	R1 niveau	42
7.4	R2 niveau	42
7.5	R3 niveau	42
7.6	Alarmverificatie	43
7.7	Alarmverificatie methoden	43
Bijlage 1	Modelformulier Programma van Eisen (PvE) informatief.....	44
Bijlage 2	Het belang van certificatie (INFORMATIEF)	46
Bijlage 3	Verwijzingen die direct of indirect verbonden zijn aan de VRKI (INFORMATIEF)	48

1. INLEIDING

De VRKI is een instrument om het risico op diefstal (eventueel met braak) te bepalen, met daaraan gekoppeld gestandaardiseerde maatregelen voor het verminderen van het risico, breed gedragen door beveiligingsbranche en verzekeraars.

In dit document worden de beveiligingsmaatregelen gedefinieerd en toegelicht die volgens de systematiek van de risicoklassen worden vereist voor de inbraakbeveiliging van een woning of bedrijf. Dit betreft de omschrijving van de O, B (C/M), E, A en R maatregelen en waaraan deze op de verschillende niveaus moeten voldoen. Allereerst wordt er echter op gewezen dat het mogelijk - en soms nodig of beter - is om 'afwijkingen' toe te passen. Want afwijkingen in de hier gehanteerde systematiek en in het voldoen aan de eisen zijn soms nodig of leiden tot betere oplossingen. In verband daarmee wordt het begrip 'gelijkwaardigheid' geïntroduceerd.

Het gebruik van de VRKI kan leiden tot afgifte van certificaten. Het belang van certificatie wordt nader toegelicht in bijlage 2.

1.1 DEFINITIES

Technische beveiligingsbedrijf

Een natuurlijke of rechtspersoon die een beveiligingssysteem gebaseerd op elektronische beveiligingen en bouwkundige beveiligingen ontwerpt uitvoert en/of onderhoudt.

Alarminstallateur

Een natuurlijke of rechtspersoon die een beveiligingssysteem gebaseerd op elektronische beveiligingen ontwerpt, uitvoert en/of onderhoudt.

Bouwkundig beveiligingsbedrijf

Een natuurlijke of rechtspersoon die een beveiligingssysteem gebaseerd op een bouwkundige beveiligingen ontwerpt, uitvoert en/of onderhoudt.

Alarminstallatie

Samenstel van componenten waarmee een onveilige situatie kan worden gesignaleerd en via telecommunicatie doorgegeven aan één of meer centrale punt(en), waar die signalen worden ontvangen en beoordeeld en van waaruit assistentie kan worden gevraagd aan derden. (noot)

Noot: Daar waarin dit document en andere publicaties wordt gesproken over Alarminstallatie moet ook worden verstaan: "elektronische beveiliging", inbraaksignalering(s)systeem, inbraaksignalering(s) installatie, inbraakalarmsysteem, inbraakalarminstallatie, alarmsysteem, (inbraak) alarmapparatuur e.d. Inhoudelijk wordt bedoeld:

Alarmapparatuur en componenten vormen samen een alarmsysteem voor het detecteren en signaleren van inbraak of pogingen daartoe, al dan niet tevens voor het signaleren van brand(rook) technische meldingen en/of een overval. Het gestelde in de Wet particuliere beveiligingsorganisaties en recherchebureaus is onverminderd van toepassing.

Beveiligingssysteem

Een samenhangend systeem van bouwkundige - mechanische -, compartimentering -, meeneembeperkende -, elektronische -, alarmerende - en reagerende maatregelen. Beveiligingsprocessen en procedures (organisatorische maatregelen) maken deel uit van het geheel. Een alarminstallatie is hiervan slechts een onderdeel.

PAC (particuliere alarmcentrale)

Een particuliere onderneming die in de uitoefening van beroep of bedrijf ten behoeve van derden in een centraal alarmmeldpunt, de door alarmapparatuur verzonden signalen ontvangt en beoordeelt en zonodig assistentie vraagt aan de politie, andere overheidsinstanties of particulieren. (noot)

Noot: Een PAC is een beveiligingsorganisatie zoals bedoeld in de Wet particuliere beveiligingsorganisaties en recherchebureaus, artikel 3, sub b. en een 'Alarm receiving centre' artikel 4.1.2 in de NEN-EN 50136-1 :2012

1.2 MAATREGELLEN EN RISICOKLASSEN

Voor iedere beveiligingsklasse wordt in de 'indeling in risicoklassen' een beveiligingsconcept gegeven in de vorm van een combinatie van de O, B, E en R maatregelen. De geleverde maatregelen zijn risicogebonden, alarminstallatiegebonden of objectgebonden.

Zie hiervoor ook de bijlage 1 in de documenten Verbeterde Risicoklassenindeling voor woningen, bijlage 2 van de Verbeterde Risicoklassenindeling voor bedrijven en bijlage 1 in de richtlijn inbraakbeveiliging onderwijsinstellingen.

1.3 PARTIËLE BEVEILIGING BIJ BEDRIJVEN

De risicoklasse wordt bepaald op basis van de categorie attractieve goederen in eigen gebruik, in winkel/showroom of in opslag/magazijn (zie tabel in bijlage 1 document D03/376 versie maart 2014) en voor welke waarde die goederen aanwezig zijn. Daarbij is het niveau van de E maatregel met betrekking tot schildetectie in de beveiligingsklasse 3, 3*, 4 en 4* ook gekoppeld aan de uitvoering van de Bouwkundige en C/M maatregelen (zie kolom 'voorwaarden' in tabel 2 in document D03/376 versie maart 2014).

Er kan echter ook worden besloten om een afwijkend beveiligingsplan op te stellen; dit is maatwerk.

De inschalingmethode die in de 'indeling in risicoklassen' wordt gehanteerd, is in feite niet bedoeld voor (zeer) grote of bijzondere objecten, want het optimale beveiligingsconcept kan hiervoor niet gemakkelijk gevangen worden in een standaard aanpak. Het opstellen van een beveiligingsconcept voor dit soort objecten is daarom meestal maatwerk. Bij het beveiligen van grote of bijzondere objecten kunnen zich twee situaties voordoen:

1. de attractieve zaken bevinden zich slechts in een beperkt deel van het object (bijvoorbeeld in het kantoor van een betonwarenfabriek) of een deel van het object valt in een hogere klasse (bijvoorbeeld magazijn/opslag);
2. het gehele object dient op een maatwerkmanier te worden beveiligd.

In het hiervoor genoemde eerste geval kan het voldoende zijn om alleen het meest risicovolle deel van het object te beveiligen. Er is dan in feite sprake van partiële beveiliging van het object, waarbij voor het bepalen van de beveiligingsaanpak in principe gebruik gemaakt kan worden van de systematiek volgens het deel 'indeling in risicoklassen'. Indien deze werkwijze wordt gevolgd, kan partiële beveiliging worden toegepast voor het beveiligde gebouw(gedeelte). Daarbij dient duidelijk te worden vastgelegd op welk gebouw(gedeelte) de beveiliging betrekking heeft. Voorwaarde is hierbij wel dat het gaat om een apart gebouw op het desbetreffende complex of om een afgescheiden gebouwgedeelte.

Bij een afgescheiden gebouwgedeelte dient de scheidingsconstructie (de scheidingswanden e.d.) met de rest van het gebouwcomplex te voldoen aan dezelfde bouwkundige (inbraakwerendheid)eisen als die gelden voor de buitengevels (daken etc.) van het beveiligde gedeelte. Inbraaktechnisch gezien dient het beveiligde gebouwgedeelte dus als zelfstandig gebouw te worden behandeld.

Indien de hiervoor bedoelde scheidingsconstructie ontbreekt of onvoldoende inbraakwerendheid bezit, kan de hier geschetste werkwijze niet worden gevolgd. Er dient dan een compleet beveiligingsplan (maatwerk) voor het geheel te worden gemaakt.

Een tweede mogelijkheid kan zich voordoen dat een gedeelte van het object waar zich concentraties van attractieve goederen bevinden (magazijn/opslag) die door de inschaling in een hogere risicoklasse valt dan het overige deel van het object (kantoren en/of productieruimten) in dat geval kan er voor de verschillende bouwdelen een op het risico afgestemd pakket van maatregelen worden vastgesteld.

1.4 VOLLEDIGE BEVEILIGING MET MAATWERK

Bij het opstellen van een maatwerk beveiligingsplan dient onderstaande procedure te worden gevolgd. Dit kan betrekking hebben op objecten in alle risicoklassen.

Het gaat er hierbij immers om dat geen standaardoplossing volgens de 'indeling in risicoklassen' wordt toegepast, maar dat een beveiligingsplan als maatwerk wordt opgesteld

Bij de procedure voor maatwerk is het van belang dat er van tevoren overeenstemming bestaat over het beveiligingsplan. Hiertoe dienen de uitgangspunten te worden vastgelegd in het programma van eisen. Beveiligingsmaatregelen en uitgangspunten die onder "Maatwerk" worden uitgevoerd moeten natuurlijk wel aan enkele uitgangspunten voldoen:

- De beveiligingsmaatregelen moeten op een gelijkwaardige manier worden uitgevoerd. Bijvoorbeeld: als u in klasse 4 voor maatwerk kiest mogen de E3 maatregelen onder maatwerk niet worden uitgevoerd als E2 of E1
- Kiezen voor "gelijkwaardige producten" en "gelijkwaardige oplossingen" mag geschieden op basis van *Goed vakmanschap*.
- Gelijkwaardigheid (maatwerk) hoeft in klasse 1-2-3 niet worden aangetoond met een verklaring van een Certificatie-instelling of gecertificeerd test- en/of keuringsinstituut.

- Uitgangspunt is wel dat uw oplossing (op een gelijkwaardige manier voldoet aan de geconstateerde klasse) door u verdedigbaar is.

Om te vermijden dat er verschillen van inzicht ontstaan, dienen alle betrokken partijen bij risicoklasse 4 en 4* schriftelijk te verklaren in te stemmen met (de uitgangspunten van) het beveiligingsplan.

Vooraf instemming van de desbetreffende verzekeraar is van belang. Desgewenst kan advies worden ingewonnen bij een inspectie-instelling. Indien één van de betrokken partijen dit wenst of eist kan worden afgesproken dat bij oplevering een opleveringsinspectie plaatsvindt door een inspectie-instelling op basis van ISO/IEC 17020-A.

1.5 GELIJKWAARDIGHEID

Ten aanzien van het begrip 'gelijkwaardigheid' doen zich twee situaties voor:

- het beveiligingsplan dat op een afwijkende, maar gelijkwaardige manier wordt ingevuld;
- de beveiligingsmaatregelen waaraan op een afwijkende, maar gelijkwaardige manier, wordt voldaan.

Beide 'afwijkingen' worden hierna nader toegelicht.

1.6 AFWIJKEND BEVEILIGINGSPLAN

In de risicoklassenindeling worden de vereiste beveiligingsmaatregelen in de beveiligingsklassen 1, 2, 3, 3*, 4 en 4* aangegeven met de letters O, B, E en R, waarbij het benodigde niveau wordt weergegeven door de cijfers 0, 1, 2 en 3. In de meest voorkomende gevallen wordt zo door een combinatie van letters en cijfers een adequaat pakket beveiligingsmaatregelen weergegeven voor het desbetreffende object of deel daarvan. Men dient er echter op bedacht te zijn dat er hierdoor sprake is van een zekere standaardisering die niet altijd tot een optimaal resultaat behoeft te leiden.

Voor zulke gevallen is het beter om een (iets) afwijkend pakket maatregelen samen te stellen. En dat is - in de hier gehanteerde systematiek - mogelijk door gebruik te maken van het beginsel 'gelijkwaardigheid'. Dat wil zeggen door het toepassen van maatregelen die samen leiden tot een resultaat dat 'gelijkwaardig' is aan dat van de maatregelen die in de desbetreffende beveiligingsklasse zijn voorgeschreven.

Het voorgaande is zeker van toepassing in de gevallen dat sprake is van een hoog inbraakrisico. Daarom is vermeld dat de vereiste beveiligingsmaatregelen ook volgens 'maatwerk' kunnen worden uitgevoerd. Dat wil zeggen dat een pakket maatregelen moet worden gekozen dat precies is toegesneden op het desbetreffende object. Hoe dat pakket eruit moet zien is niet gemakkelijk vast te leggen in een standaardoplossing.

Ook in dit opzicht echter is er sprake van 'gelijkwaardigheid', want het beveiligend vermogen van de maatwerkoplossing moet gelijkwaardig zijn aan hetgeen ten minste vereist is in de van toepassing zijnde beveiligingsklasse. De juiste invulling voor het desbetreffende object is echter een kwestie van maatwerk.

1.7 AFWIJKEND VOLDOEN AAN DE EISEN

De omschrijving van de beveiligingsmaatregelen gebeurt zoveel mogelijk in de vorm van prestatie-eisen. Dat wil zeggen dat niet precies wordt aangegeven op welke manier aan de eisen moet worden voldaan, maar wél welke prestatie geleverd moet worden. Dit geeft de mogelijkheid om voor een bepaald object de meest geschikte oplossingen te kiezen uit de (vele) verschillende mogelijkheden tot beveiliging.

Bij het formuleren van prestatie-eisen wordt verwezen naar normen en voorschriften. Op basis daarvan kan worden geverifieerd of een bepaalde oplossing de gevraagde prestatie levert. Zulke normen en voorschriften bestaan echter niet op alle gebieden van inbraakpreventie en daarom wordt in een aantal gevallen omschreven hoe de gevraagde beveiligingsmaatregel eruit moet zien.

Het is daarbij uitdrukkelijk niet de bedoeling om alternatieve oplossingen uit te sluiten. Vooral niet als die tot een beter resultaat leiden! Bij het toepassen van alternatieve oplossingen dient daarom eveneens het begrip 'gelijkwaardigheid' te worden gehanteerd: de gekozen oplossing dient ten minste gelijkwaardig te zijn aan de voorgeschreven maatregel.

1.8 BEOORDELEN VAN GELIJKWAARDIGHEID

Door wie (of hoe) wordt de gelijkwaardigheid nu beoordeeld? Bij producten, constructies of installaties waarvoor genormaliseerde beproevingen of voorschriften bestaan, ligt dat tamelijk eenvoudig.

De beoordeling kan hier plaatsvinden aan de hand van testresultaten of de desbetreffende voorschriften. In andere gevallen is dat niet mogelijk en zal de beoordeling moeten plaatsvinden op grond van vakkennis en ervaring. Het beoordelingsvermogen van de deskundige moet hierbij niet worden onderschat, maar dit sluit de mogelijkheid niet uit dat andere deskundigen tot andere conclusies komen.

Bij de toepassing van het beginsel van gelijkwaardigheid is het daarom altijd van belang dat de direct betrokkenen vooraf tot overeenstemming komen. Dit moet middels het vastleggen van de maatwerkoplossingen in het PvE (programma van eisen) waarin de eisende partijen zich akkoord verklaren.

1.9 PROGRAMMA VAN EISEN (PVE)

Het bedrijf legt, in overleg met de opdrachtgever, het programma van eisen voor het beveiligingsplan vast in een document, genaamd Programma van Eisen (PvE), zie modelformulier bijlage 1 (informatief).

Het PvE bevat:

NAW gegevens van de klant (opdrachtgever) en de aanduiding van het object,
De geconstateerde risicoklasse, de gekozen combinatie van de beveiligingsmaatregelen in de vorm van een aanduiding van de individuele niveaus uitgesplitst in:

- O: Organisatorische maatregelen
- B: Bouwkundige maatregelen + indien van toepassing, de C/M maatregelen
- E: Elektronische maatregelen + Alarmering
- R: Reactie (alarmopvolging)

Indien de gekozen combinatie van beveiligingsmaatregelen voldoet aan de beveiligingsklasse die behoort bij de geconstateerde risicoklasse dan wordt een Beveiligingscertificaat verstrekt.

Indien de gekozen combinatie van beveiligingsmaatregelen op een lager niveau wordt uitgevoerd dan wordt een Opleveringsbewijs afgegeven.

Bij afwijkingen wordt onder "maatwerk" een toelichting gegeven.

Een verwijzing naar het beveiligingsplan (voor zover dit in dit stadium reeds beschikbaar is)

De vermelding van het kwaliteitsdocument wat na oplevering wordt afgegeven.

Autorisatie van het ingevulde document.

Het PvE speelt ook een belangrijke rol bij eventuele aansprakelijkheid bij conflicten

Voorbeeld sjabloon PvE: zie bijlage 1

1.10 RISICOANALYSE

De risicoanalyse gaat minimaal uit van onderstaande gegevens:

Woningen

Attractieve zaken van de inboedel:

Audiovisuele en computerapparatuur: vastgestelde waarde €.....

Lijfsieraden en contant geld of waardepapieren: vastgestelde waarde €.....

Bijzondere bezittingen: vastgestelde waarde €.....

Immateriële zaken die van toepassing zijn op het risico waardoor de uitkomst in een hogere risicoklasse wordt ingeschaald dan de optelling van de attractieve zaken van de inboedel rechtvaardigen, alsmede specifieke risico's en maatregelen die in het beveiligingsplan zijn/worden uitgewerkt.

Bedrijven

Attractieve goederen categorie L: vastgestelde waarde €.....

Attractieve goederen categorie M: vastgestelde waarde €.....

Attractieve goederen categorie H: vastgestelde waarde €.....

Attractieve goederen categorie ZH: vastgestelde waarde €.....

Immateriële zaken die van toepassing zijn op het risico waardoor de uitkomst in een hogere risicoklasse wordt ingeschaald dan de uitkomst m.b.t. de attractieve goederen en bedrijfsuitrusting / inventaris rechtvaardigen, alsmede specifieke risico's en maatregelen die in het beveiligingsplan zijn of worden uitgewerkt.

1.11 BEVEILIGINGSPLAN

Het beveiligingsplan bevat:

- een aanduiding van het te beveiligen (deel van het) bouwwerk of terrein,
- een aanduiding van de doelstelling van de beveiliging, waarbij de materiële - en immateriële - attractieve zaken worden genoemd, waarop de beveiliging is toegespitst, de risicoanalyse en de uitkomst van de risicoanalyse met vermelding van de geconstateerde risicoklasse, en een aanduiding van de te treffen maatregelen volgens de, bij de risicoklasse behorende, beveiligingsklasse.

Indien de gekozen combinatie van beveiligingsmaatregelen voldoet aan de beveiligingsklasse die behoort bij de geconstateerde risicoklasse dan wordt een Beveiligingscertificaat verstrekt.

Indien de gekozen combinatie van beveiligingsmaatregelen op een lager niveau wordt uitgevoerd dan wordt een Opleveringsbewijs afgegeven.

Vastgelegd moet worden of de beveiliging moet geschieden op basis van een beveiligingssysteem of slechts bestaat uit een inbraakalarminstallatie.

Is het uitgangspunt een beveiligingssysteem dan bevat het beveiligingsplan voor alle maatregelen een specificatie van de te treffen O, B (+ indien van toepassing C/M), E (+ AL) en R maatregelen. Inclusief de projecteringstekening(en). Bij kleine objecten kan ook worden volstaan met een aanduiding in plaats van een projecteringstekening.

Het ontwerp van een beveiligingssysteem zegt niet alleen iets over de kwaliteit van de toegepaste componenten en de manier waarop ze zijn verwerkt, maar vooral ook over de samenhang en het beveiligend vermogen ervan. En dat alle, conform de bepaalde beveiligingsklasse vereiste beveiligingsmaatregelen, volgens de desbetreffende voorschriften worden uitgevoerd of daaraan gelijkwaardig is (maatwerk).

Is het uitgangspunt een alarminstallatie dan bevat het beveiligingsplan een specificatie van de E (+AL) en R alsmede de daarbij behorende organisatorische maatregelen. Inclusief de projecteringstekening(en) van de alarminstallatie. Bij kleine objecten kan ook worden volstaan met een aanduiding in plaats van een projecteringstekening. De geleverde maatregelen worden daarmee alarminstallatie gebonden in plaats van risico gebonden.

Is het uitgangspunt een bouwkundige beveiliging dan bevat het beveiligingsplan een specificatie van B, en eventuele C/M maatregelen alsmede de daarbij behorende organisatorische maatregelen. De geleverde maatregelen worden daarmee object gebonden in plaats van risico gebonden.

Leeswijzer:

Aanduiding: benaderende beschrijving

Specificatie: iedere maatregel op zichzelf noemen

2. ORGANISATORISCHE MAATREGELEN

2.1 INDELING IN NIVEAUS

Afhankelijk van de van toepassing zijnde beveiligingsklasse zijn niveaus in de organisatorische maatregelen voorgeschreven. We onderscheiden twee verschillende niveaus, O1, en O2.

Een deel van de eisen die voorheen werden vermeld bij de Elektronische maatregelen maar hoofdzakelijk van organisatorische aard zijn, zoals bijvoorbeeld het bewaken van in - en uitschakeltijden van de alarminstallatie, zijn nu bij de O maatregelen opgenomen.

2.2 NIVEAU EN OMVANG VAN DE ORGANISATORISCHE MAATREGELEN

2.2.1 NIVEAU O1

Standaard organisatorische maatregelen en voorlichting over preventie. Inbraakpreventie is niet alleen een kwestie van het treffen van bouwkundige en elektronische maatregelen. Om tot een sluitend geheel te komen zal de eigenaar of gebruiker van een beveiligde woning of gebouw moeten zorgen dat ook de nodige organisatorische maatregelen worden getroffen. Hierbij ligt het voor de hand dat de technische preventieve voorzieningen op de juiste manier gebruikt moeten worden, om deze het gewenste effect te laten sorteren. Daarnaast zal - om te zorgen dat dit ook in de toekomst het geval zal zijn - het onderhoud daarvan geregeld moet worden. En ten slotte zijn er tal van organisatorische maatregelen die het de inbreker moeilijk maken of die hem soms al van tevoren doen besluiten af te zien om van een poging tot inbraak of diefstal.

Het totale pakket organisatorische maatregelen zal van geval tot geval verschillen; het is sterk afhankelijk van de situatie. Er zijn voldoende publicaties voorhanden die aandacht besteden aan de volgende standaard onderwerpen. Deze behoren bij oplevering van een alarminstallatie of het beveiligingssysteem aan de gebruiker te worden overhandigd.

2.2.2 SLEUTELBEHEER EN -GEBRUIK

Een slot moet goed gebruikt worden, anders heeft het geen zin. In elk geval moet ervoor worden gezorgd dat alleen bevoegde personen in het bezit zijn van een sleutel en dat eventuele reservesleutels goed worden opgeborgen. Om het aantal in gebruik zijnde sleutels te beperken, kan gebruik gemaakt worden van gelijksluitende cilinders. De inbraakwerende eigenschappen van sloten zijn gebaseerd op een situatie dat het slot op het nachtslot zit en de sleutel uit het slot is gehaald, dit voorkomt ook dat door middel van flipperen (terugduwen van de dagschoot met behulp van bijvoorbeeld een betaalpasje) de deur kan worden geopend. Zelfs als de bewoners thuis zijn en bijvoorbeeld slapen. Bij bedrijven verdient het aanbeveling om te registreren wie een sleutel in gebruik heeft. Er dient, met name bij bedrijven, een meldingsplicht te zijn bij verlies van een sleutel.

2.2.3 SLUITRONDE

Bij het afsluiten van het gebouw - en eventueel het inschakelen van de alarminstallatie - dient te worden gecontroleerd of alle ramen en deuren zijn afgesloten. Maak daar een vaste afsluitronde van; dit beperkt de kans om een deur of raam te vergeten. Maak duidelijke afspraken over wie er verantwoordelijk is voor het afsluiten en wie er als plaatsvervanger optreedt. Bij zeer hoge risico's en bij objecten waar een bepaalde cultuur heerst dat niemand zich verantwoordelijk voelt (vergelijkbaar met scholen) kan mogelijk (O2) een gedwongen sluitronde worden ingevoerd: alle ruimtelijk werkende detectoren moeten zijn "uitgelopen" anders kun je niet inschakelen.

2.2.4 MERKEN EN REGISTREREN VAN WAARDEVOLLE ZAKEN

Voorzie de meest waardevolle zaken van postcode en huisnummer door middel van graveren, etsen of inbranden. Het markeren met een DNA spray valt hier ook onder. Registreer deze bezittingen op een lijst en maak er eventueel foto's van. Na een diefstal kan dit nuttig zijn voor herkenning en opsporing en voor het vaststellen van de schade.

2.2.5 ZICHTBARE AFWEZIGHEID VOORKOMEN

Vooral in vakantieperiodes is een bekend verschijnsel dat gesloten gordijnen, overvolle brievenbussen, niet gemaaid gazons en zelfs briefjes op de deur afwezigheid kunnen verraden. Deze signalen maken de keuze voor de inbreker er niet moeilijker op. Buren, kennissen of familieleden kunnen helpen om een huis bewoond te laten lijken. Het laten branden van enkele lichtpunten in het huis accentueert het bewoond uiterlijk. Door middel van instelbare schakelklokken kan met enkele lichtpunten - met energiezuinige lampen - in het huis een normaal bewoningspatroon worden gesimuleerd. Bij bedrijfspannen is nachtverlichting preventief en een maakt het tevens mogelijk voor alarmopvolgers zich te oriënteren.

2.2.6 BEVEILIGINGSVERLICHTING

Een inbreker wordt niet graag gezien. Vandaar dat beveiligingsverlichting langs de buitenkant van het gebouw preventief werkt indien de omgeving (sociale) controle toelaat en de inbreker inderdaad de kans loopt om gezien te worden. Beveiligingsverlichting kan door middel van een schemerschakelaar automatisch worden ontstoken en gedoofd. Het verlichtingsniveau dient - met name ter plaatse van deuren, ramen en opklimmogelijkheden - ten minste gelijk te zijn aan dat van de openbare verlichting. In bepaalde gevallen kan 'schrikverlichting' worden toegepast, die wordt ingeschakeld door een detector of door de alarminstallatie.

2.2.7 GEBRUIK VAN COMPARTIMENTEN

Indien in het gebouw een inbraakwerend compartiment is ingericht, dienen afspraken te worden gemaakt over het gebruik van deze ruimte. Maak duidelijke afspraken over wie er verantwoordelijk is voor het goede gebruik van het compartiment en wie als plaatsvervanger optreedt. Het voorgaande geldt eveneens voor de (veilige) opslag van vertrouwelijke documenten, databestanden e.d.

2.2.8 BUREN EN OMWONENDEN

Het verdient aanbeveling om met buren of omwonenden afspraken te maken over het in de gaten houden van elkaars gebouwen. In woonwijken kan dit worden georganiseerd in de vorm van buurtpreventie projecten. Bewoners kunnen zo, samen met de politie, zorgen dat inbrekers en vandalen minder makkelijk de kans krijgen hun slag te slaan. Op bedrijventerreinen en in winkelcentra wordt de bewaking in toenemende mate georganiseerd in samenwerking met particuliere beveiligingsbedrijven, gemeente en politie.

2.2.9 HUISREGELS EN DISCIPLINE

Hoe compleet de technische beveiliging ook is opgezet, alle techniek wordt tenietgedaan door gebrek aan discipline of het ontbreken van sluitende huisregels. Met name voor bedrijven is het van belang dat huisregels worden opgesteld die antwoord geven op de volgende vragen.

- Wie mag waar komen?
- Wie mag wanneer ergens komen?
- Welke andere beperkingen van de bewegingsvrijheid zijn nodig en voor welke mensen: personeelsleden, inleenkrachten, leveranciers, bezoekers etc.
- Welke gegevens zijn voor wie toegankelijk?
- Waar en hoe worden ze opgeborgen?
- Welke gegevens en andere zaken zijn moeilijk vervangbaar en dienen daarom diefstal - (en brand) werend te worden opgeborgen?

2.2.10 OPKLIMMOGELIJKHEDEN

Opklimmogelijkheden om het gebouw dienen zoveel mogelijk vermeden te worden. Inbrekers schrikken er niet voor terug om via opklimmogelijkheden, zoals afvalcontainers, afdaken, een stapel pallets, een ladder, de afdekkap van de zonwering e.d., naar boven te klimmen om te onderzoeken of ze niet makkelijker binnen kunnen komen via daklichten, dakramen, bovenlichten of balkondeuren.

Opklimmen kan worden bemoeilijkt door het toepassen van bijvoorbeeld getande beugels rond hemelwaterafvoeren en overklimbeveiliging op (lage) muren. Losse hulpmiddelen, zoals ladders, pallets, kratten, verrolbare containers e.d., dienen te worden opgeborgen of met een goed hangslot op hun - van het gebouw verwijderde - plaats te worden gefixeerd. Speciale aandacht verdienen in dit verband ook tijdelijke voorzieningen, zoals bijvoorbeeld de steiger van een schilder. Bij bedrijven is extra aandacht voor opklimmogelijkheden een must. Veel daders plegen inbraken via de daken. Na een veroorzaakt alarm kijkt een alarmopvolger vaak alleen na verbreking van de schil; het dak wordt zelden gecontroleerd. Inbrekers weten dit en maken hiervan handig gebruik.

2.2.11 TUINAANLEG

Bij de aanleg en het onderhoud van de beplanting rondom het gebouw dient ervoor te worden gezorgd dat het geheel overzichtelijk blijft. Het is van belang dat de inbreker niet ongezien te werk kan gaan door hoogopgaande begroeiing of zich hierin kan verschuilen. Het verdient aanbeveling om de hoogte van de begroeiing om het gebouw te beperken tot circa 1 meter. Het is goed om hiermee rekening te houden bij de keuze van de beplanting en ook om bij het tuinonderhoud het onderwerp inbraakpreventie niet uit het oog te verliezen. Toepassing van doornachtige beplanting kan de toegankelijkheid verminderen. Het toepassen van een hekwerk om het terrein maakt het betreden natuurlijk nooit geheel onmogelijk, maar een hek vormt wel een extra barrière. Ook voor vandalen en ook bij de eventuele afvoer van de buit. Bovendien vormt het hek een juridische afscherming. Iemand die je aantreft achter een hek is in overtreding, artikel 461 Sr.

2.2.12 TOEGANGSCONTROLE

Voor bedrijven verdient het aanbeveling om een vorm van toegangscontrole te organiseren om zoveel mogelijk te voorkomen dat onbevoegden het terrein of de gebouwen betreden. Enerzijds bestaan hiervoor technische hulpmiddelen, zoals speciale pasjes, anderzijds is het ook weer een kwestie van organisatie. Niet alleen via een portier of een receptioniste, maar ook via (de andere) personeelsleden die de instructie hebben om onbekenden aan te spreken en - zo nodig - te verzoeken het bedrijf te verlaten.

2.2.13 GEGEVENSBEVEILIGING

Belangrijke bedrijfsgegevens, zoals vertrouwelijke documenten, computerbestanden, tekeningen van op maat gemaakte machines, receptuur e.d., dienen zeker ook te worden gerekend tot de attractieve zaken die dienen te worden beveiligd tegen brand en diefstal. En niet te vergeten: vandalisme! Hiervoor geldt in principe alles wat is gesteld voor de beveiliging van andere attractieve zaken. En zelfs in versterkte mate indien de vermissing van belangrijke bedrijfsgegevens de bedrijfscontinuïteit in gevaar kan brengen.

2.2.14 WIJZIGINGEN EN OMSTANDIGHEDEN

Inbraakbeveiliging is in feite altijd maatwerk, want alle beveiligingsmaatregelen worden speciaal afgestemd op de gegeven situatie. Het verdient aanbeveling om dit steeds goed in het oog te houden, zodra er plannen worden gemaakt om iets te wijzigen. Bij plannen voor verbouwing, uitbreiding, het wijzigen van de indeling, de routing of de bestemming van ruimten, dient daarom steeds te worden nagegaan of het nodig is de beveiliging aan te passen.

Dat is beter dan af te wachten tot het beveiligingsbedrijf de noodzaak tot aanpassing constateert tijdens de uitvoering van het periodieke onderhoud. Hetzelfde geldt natuurlijk ook voor wijziging met betrekking tot attractiviteit. Het beveiligingsniveau moet daarop blijvend zijn afgestemd. En wat daarbij zeker niet uit het oog mag worden verloren is de acceptatie van de gebruiker van de beveiligingsmaatregelen. ($E = K \times A$)

2.2.15 IN - EN UITSCHAKELREGISTRATIE BIJ DE PAC

Bij gebruik van een inbraaksignaleringsysteem met aansluiting op een PAC dienen de in - en uitschakelingen te worden doorgemeld of van een (software) systeem te zijn voorzien waarbij de in - en uitschakelingen (status en tijdstip) bij een inbraakalarm worden meegezonden. Hiermee wordt bereikt dat de centralist bij een inbraakalarmmelding zicht heeft op status van de installatie. Bedieningsfouten waarbij een inbraakmelding wordt veroorzaakt zijn hierdoor herkenbaar. Een inbraakmelding die volgt binnen enkele minuten na de inschakeling zal niet worden doorgemeld naar de politie. Hetzelfde is van toepassing als er na een inbraakmelding een uitschakeling volgt naar de PAC. De centralist zal contact met het object zoeken en altijd alarmverificatie moeten toepassen alvorens de politie mag worden gewaarschuwd. Alarmverificatie is mogelijk met technische voorzieningen zoals camerabeelden, inluisteren/spreken of meerdere zones in alarm. Deze laatste optie lijdt tot negatieve alarmverificatie als er ook een in - of uitschakelmelding met een inbraakalarmmelding is binnengekomen. Als het alarm alsnog niet wordt afgemeld door de veroorzaker zal persoonlijke alarmverificatie worden aangestuurd. Dit kan overlast betekenen voor de sleutelhouder(s) of tot kosten van een particuliere bewakingsdienst.

2.2.16 UP EN DOWNLOADEN

Onder uploading wordt verstaan de procedure waarbij informatie uit de alarminstallatie (met inbegrip van de daarop aangesloten randapparatuur en alarm/datatransmissieapparatuur) wordt verzonden naar een beheercomputer. De informatie behelst instellingen van parameters of software zoals die in het systeem aanwezig zijn.

Bijvoorbeeld:

- het in - of uitgeschakeld staan van het systeem en
- in - en uitloopvertragingen en het servicegeheugen.

Via een uploading procedure kunnen uitsluitend gegevens, komende uit het systeem, worden uitgelezen. Het is met deze procedure niet mogelijk parameters te wijzigen of te verwijderen.

Downloading omvat de procedure waarbij via de beheercomputer commando's kunnen worden gegeven aan de centrale controle- en stuu eenheid (CCS), om de parameters of software te wijzigen.

Een downloading communicatieverbinding mag slechts tot stand komen na een bewuste handeling, die moet plaatsvinden in het beveiligde object.

De bewuste handeling dient door het systeem automatisch te worden gemeld en geregistreerd bij de Particuliere Alarmcentrale (PAC) De bewuste handeling kan bestaan uit reguliere download activiteiten, waarvoor vooraf toestemming is verleend door middel van een autorisatieformulier.

Na oplevering van een inbraaksignaleringsysteem dient een door de klant ondertekend autorisatieformulier met betrekking tot up- en downloading (indien van toepassing) in het dossier van de klant bij het beveiligingsbedrijf aanwezig te zijn.

2.2.17 LOGBOEK

Bij oplevering van de alarminstallatie wordt aan de gebruiker een logboek overhandigd.

Het logboek bevat:

- Een instructie voor de gebruiker welk preventief onderhoud door gebruiker zelf periodiek dient uit te voeren.
- Een notitieblad waarop de gebruiker gebeurtenissen omschrijft, met name de ongewenste alarmeringen met vermelding van datum en mogelijke oorzaak.
- Een notieblad waarop de installateur de handelingen omschrijft bij bezoeken m.b.t. onderhoud en storingopheffing met vermelding van datum en naam van de monteur die deze werkzaamheden heeft uitgevoerd.

2.3 NIVEAU O2

Als O1 met aanvulling: omschrijving van de specifieke organisatorische maatregelen die zijn toegespitst op het risico. Voor bedrijven geldt bovendien: bij de PAC dient registratie plaats te vinden van de in- en uitschakeltijden van het systeem, alsmede van de controlemeldingen (ATS categorieën). Schriftelijk dient te worden overeengekomen dat een overschrijding van vooraf vastgestelde tijden door de PAC dient te worden onderkend en afgehandeld conform de hierover gemaakte afspraken.

3 BOUWKUNDIGE BEVEILIGINGSMATREGELEN

In de tabellen van de beveiligingsklassen voor woningen en bedrijven worden de vereiste bouwkundige maatregelen aangeduid met de letter B en een cijfer achter de B. Dit cijfer heeft betrekking op de aard en omvang (het niveau) van deze maatregelen.

3.1 OMVANG VAN DE BOUWKUNDIGE BEVEILIGINGSMATREGELEN

De complete bouwkundige beveiliging van een gebouw tegen inbraak moet alle inbraakgevoelige onderdelen aan de buitenzijde van een gebouw omvatten die voor inbrekers bereikbaar zijn.

Dit zijn dus alle buitendeuren, ramen, lichtkoepels, dakramen e.d.

Zie voor de bereikbaarheid van gevelelementen de NEN 5087:2013. Indien een gebouw toegankelijk is via een ruimte (zoals een garage, kruipruimte of berging) waarvan de toegangsmogelijkheden vanaf het openbare gebied niet voldoen of niet kunnen voldoen aan de eisen volgens B1 respectievelijk B2 of B3, dient de scheidingsconstructie tussen deze ruimte en de rest van het gebouw te voldoen aan de eisen volgens B1 respectievelijk B2 of B3

Opmerking:

Voor het bepalen van de bereikbaarheid kan in afwijking van de norm NEN 5087:2013 de definitie van bijlage 1 in het handboek PKVW bestaande bouw worden aangehouden.

Bron: <http://www.hetccv.nl/publicaties/webwinkel/PKVW/pkvw-bb-2011>

3.2 HET NIVEAU VAN DE BOUWKUNDIGE BEVEILIGINGSMATREGELEN

Hierna volgen de omschrijvingen van de eisen waaraan de buitenschil van een gebouw (de gevels, daken e.d.) moeten voldoen.

3.2.1 NIVEAU B0

Het aanwezige hang- en sluitwerk waarvan niet kan worden aangetoond dat deze producten of combinaties van producten voldoen aan de BRL 3104 of niet voldoen aan weerstandsklasse 2 van de NEN 5096:2012. "Kortom, het bestaande hang- en sluitwerk handhaven"

In voorkomende gevallen (zie tabel beveiligingsklasse in document D03-376 Risicoklassenindeling bedrijven en document D03-375 Risicoklassenindeling woningen) zijn hiervoor aanvullende E en/of C/M maatregelen vereist. Het niveau B1 heeft de voorkeur, B0 is een uitwijk mogelijkheid.

3.2.2 NIVEAU B1

Alle bereikbare gevelelementen dienen te voldoen aan de eisen volgens weerstandsklasse 2 van de NEN 5096:2012 (nl) waarmee een inbraakvertraging wordt beoogd van 3 minuten.

Voor bestaande bouw is de NEN 5089:2009 nl. Inbraakwerend hang- en sluitwerk en de aanvullende eisen volgens: "BRL 3104 (12-07-2012)" van toepassing. Hierbij kan gebruik worden gemaakt van de PKVW Beveiligingsrichtlijn Bestaande Bouw, meest recente uitgave, van het Centrum voor Criminaliteitspreventie & Veiligheid (CCV) Een lijst van goedgekeurde producten en productcombinaties voor deuren en beweegbare ramen en ventilatieopeningen die volgens recente beproevingen aan deze eisen voldoen is ook te vinden op de website van de SKG (www.sterrenwijzer.nl)

Ventilatieopeningen of -ramen (die in het gebruik vaak open staan) met een dagmaat van minder dan 15 cm behoeven niet te worden beveiligd. Bij een grotere dagmaat dient een beveiliging tegen inklimmen te worden aangebracht.

Van kelderramen beneden het maaiveld dienen de lichtschachten te zijn afgedekt met een rooster dat met speciale beugels aan de onderzijde is vastgezet. Kelderramen boven het maaiveld kunnen het beste worden afgeschermd met traliewerk of strekmetaal. Lichtkoepels dienen, indien ze niet gemaakt zijn van slagvaste kunststof, aan de onderzijde voorzien te worden van traliewerk of strekmetaal. Slagvaste lichtkoepels dienen te zijn vastgezet met beveiligde schroeven en/of moeren.

In afwijking van de norm voor de bereikbaarheid van gevelelementen kan de gewijzigde definitie worden aangehouden conform bijlage 1 in het handboek PKVW bestaande bouw.

Bron: <http://www.hetccv.nl/publicaties/webwinkel/PKVW/pkvw-bb-2011>

3.2.3 NIVEAU B2

Alle bereikbare gevelelementen dienen te voldoen aan de eisen volgens weerstandsklasse 3 van de NEN 5096:2012 (nl) waarmee een inbraakvertraging wordt beoogd van 5 minuten.

Voor bestaande bouw kan deze eis mogelijk ook worden bereikt door toepassing van veiligheidsbeglazing voor vaste gevelelementen weerstandsklasse 4 NEN-EN 356 P4 of zwaar traliewerk. Voor beweegbare gevelelement geldt afscherming door middel van rolluiken type O1/G1 en O2/G2 genoemd in de tabel 1 (matrix gevelafscherming) van document 002757 augustus 2001 versie 2 Handboek Beveiligingstechniek.

In afwijking van de norm voor de bereikbaarheid van gevelelementen kan de gewijzigde definitie worden aangehouden conform bijlage 1 in het handboek PKVW bestaande bouw.

Bron: <http://www.hetccv.nl/publicaties/webwinkel/PKVW/pkvw-bb-2011>

Opmerking:

Het niveau B2 kan bij winkels, showrooms en bedrijven worden gebruikt als inbraakvertragend gevelelement voor buit die direct voorhanden is en deze buit om praktische redenen niet in een compartiment is op te bergen. Het uitgangspunt is: eerst signaleren, dan vertragen. Toepassing van B2 vraagt dus altijd ook om schildetectie. Zonder deze samenhang wordt niet het gewenste resultaat behaald. Toepassing van C/M maatregelen of mistgenerator geniet de voorkeur.

3.2.4 NIVEAU B3

Alle bereikbare gevelelementen dienen te voldoen aan de eisen volgens weerstandsklasse 4 van de NEN-EN 1627:2011 waarmee een inbraakvertraging wordt beoogd van 10 minuten.

De bouwkundige beveiliging op niveau B3 is bedoeld voor de toepassing in bedrijfsmatige objecten in de risicoklasse 4. Gelet op de aard van deze objecten moet rekening worden gehouden met 'zwaardere' aanvalsmethoden dan de gebruikelijke methoden van de gelegenheidsinbreker.

Voor bestaande bouw kan deze eis mogelijk ook worden bereikt door toepassing van veiligheidsbeglazing voor vaste gevelelementen weerstandsklasse 4 NEN-EN 356 P5 of extra zwaar traliewerk. Voor beweegbare gevelelement geldt afscherming door middel van rolluiken type O3/G3 en O4/G4 genoemd in de tabel 1 (matrix gevelafscherming) van document 002757 augustus 2001 Handboek Beveiligingstechniek.

Voor objecten in de risicoklasse 4 en 4* dient de invulling van de eisen volgens B3 te geschieden op basis van de risicoanalyse voor het desbetreffende object. Het PvE bevat een aanduiding van de aldus bepaalde bouwkundige maatregelen. Het beveiligingsplan bevat een specificatie van alle uit te voeren bouwkundige maatregelen.

In afwijking van de norm voor de bereikbaarheid van gevelelementen kan de gewijzigde definitie worden aangehouden conform bijlage 1 in het handboek PKVW bestaande bouw.

Bron: <http://www.hetccv.nl/publicaties/webwinkel/PKVW/pkvw-bb-2011>

Opmerking 1:

Het niveau B3 kan bij winkels, showrooms en bedrijven worden gebruikt als inbraakvertragend gevelelement voor buit die direct voorhanden is en deze buit om praktische redenen niet in een compartiment is op te bergen. Het uitgangspunt is: eerst signaleren dan vertragen. Toepassing van B3 vraagt dus altijd ook om schildetectie. Zonder deze samenhang wordt niet het gewenste resultaat behaald. Toepassing van C/M maatregelen of mistgenerator geniet de voorkeur.

Opmerking 2: Bij toepassing van bouwkundige maatregelen op niveau B1, B2 en B3 dienen cilinders te worden toegepast conform de klasse van het slot. Voor deuren van compartimenten geldt: cilinders (sleutels) met certificaat. Voor de (hoofd)toegangsdeuren is dit een advies.

3.2.5 GLASAFSCHERMING / GLASVERVANGING

De afscherming van beglazing in ramen en deuren kan worden uitgevoerd door het aanbrengen van voorzieningen als tralies, hekwerken of strekmetaal.

Een andere vorm van 'glasafscherming' is het aanbrengen van rolluiken, waarmee in feite een gehele pui wordt afgeschermd. Voor nadere informatie over rolluiken wordt verwezen naar document 002757 Installatievoorschriften voor rolluiken, rolhekken en schaarhekken, augustus 2001 versie 2

In plaats van het toepassen van 'glasafscherming' kan de beglazing worden vervangen door inbraakwerende beglazing. Van toepassing is: document D03/394: Inbraakwerende beglazing, september 2003 versie 2.

3.2.6 TRALIES, HEKWERKEN EN STREKMETAAL

Bij het toepassen van tralies e.d. gaat het er om dat een inbreker - na het verwijderen/breken van de beglazing - niet makkelijk door de ontstane opening kan binnendringen. Het is van belang dat de onderlinge afstand tussen de staven van traliewerk of hekwerken zodanig klein is dat binnendringen praktisch onmogelijk wordt gemaakt. Over het algemeen is dit het geval als de ontstane openingen - na het verwijderen van het glas - een dagmaat hebben die kleiner is dan 150 mm. Een belangrijke voorwaarde is daarbij wel dat de opening door buigen - met mankracht - niet makkelijk is te vergroten. Met andere woorden dat de staven van traliewerk e.d. niet makkelijk zijn te verbuigen. Hierbij is het tevens van belang dat de aangebrachte voorzieningen niet makkelijk vanaf de buitenzijde zijn te verwijderen en dat de bevestiging voldoende stevigheid biedt.

Er bestaan geen separate richtlijnen om het hiervoor genoemde te beoordelen, zodat de beoordeling dient plaats te vinden op basis van de vereiste inbraakvertraging volgens de bouwkundige niveaus B1, B2 en B3 en document 002757 augustus 2001 versie 2: Installatievoorschriften voor rolluiken, rolhekken en schaarhekken, en in document D03/394 september 2003 versie 2: Inbraakwerende beglazing; hoofdstuk 4 'producten om glas af te schermen'

4 ELEKTRONISCHE MAATREGELLEN

In de tabellen van de beveiligingsklasse voor woningen en bedrijven worden de vereiste elektronische maatregelen aangeduid met de letter E en een letter of cijfer. De toevoeging achter de 'E' heeft betrekking op omvang en het niveau van deze maatregelen.

4.1 OMVANG VAN DE ELEKTRONISCHE MAATREGELLEN

In het op te stellen beveiligingsplan dient te worden bepaald welke typen detectoren in welke ruimten en op welke plaatsen moeten worden aangebracht. De zwaartepunten in het beveiligingsplan worden hierbij gevormd door de plaatsen waar zich de attractieve goederen bevinden. Bij het opstellen van het beveiligingsplan zal echter ook nagegaan moeten worden welke andere - eventueel verbindende - ruimten in het bewaakte gebied moeten worden opgenomen.

Uit het voorgaande volgt dat het bewaakte gebied zich niet alleen beperkt tot ruimten op de begane grond, maar zich in bepaalde gevallen ook uitstrekt tot ruimten in de kelder of op de verdiepingen.

Dit zijn in principe alle ruimten die voor een inbreker bereikbaar zijn vanaf het openbare gebied.

Het voorgaande betekent tevens dat bepaalde ruimten niet tot het bewaakte gebied gerekend behoeven te worden. Dit betreft bijvoorbeeld een toiletruimte op de begane grond met een ventilatieraampje met een dagmaat van minder dan 15 cm. Daarnaast kunnen ook andere ruimten van het bewaakte gebied worden uitgezonderd indien dit in overeenstemming is met de verdere invulling van het beveiligingsplan.

4.2 ONTWERP EN AANLEG

De alarminstallatie dient te worden ontworpen, aangelegd en onderhouden volgens de Installatievoorschriften voor alarmapparatuur document 002080 juli 2000 versie 2 en de Voorschriften beheer en onderhoud alarmapparatuur document 002079 juli 2000 versie 2.

Voor de detectie dient gebruik gemaakt te worden van een - op het risico afgestemde - combinatie van ruimtelijke - en omtrek detectie. De status van het systeem in het beveiligde object moet steeds afleesbaar zijn. Bij toepassing van mistgeneratoren is bijlage 2 van document D01/026 oktober 2001 versie 2 van toepassing.

4.3 HET NIVEAU VAN DE ELEKTRONISCHE MAATREGELLEN

Hierna volgen de omschrijvingen van de eisen waaraan de elektronische maatregelen moeten voldoen. Alarmering: Zodra de alarminstallatie in alarm komt - dat wil zeggen dat één of meer detectoren in het bewaakte gebied de alarmstatus bereiken - dient er een alarmering plaats te vinden. De eisen daaraan zijn opgenomen in hoofdstuk 6: "Alarmering" in dit document.

4.3.1 ED NIVEAU

Inleiding: aan de basis van de elektronische inbraaksignaleringsystemen voor woningen staat het E1 niveau. Dit E1 niveau dient altijd op een erkende BORG Particuliere Alarmcentrale (PAC) te worden aangesloten. In bepaalde gevallen kunnen er voor gebruikers en verzekeraars redenen zijn om genoegen te nemen met een inbraaksignaleringsstelsel zonder aansluiting op een PAC. Zij wensen echter wel de zekerheid dat de installatie uit goede componenten bestaat en deskundig is aangelegd. Bovendien willen zij graag dat aansluiting op een PAC in een later stadium altijd mogelijk blijft. Dit Ed niveau, wat uitsluitend geldt voor woningen in risicoklasse 1, is Ed genoemd. De 'd' staat daarbij voor domestic oftewel woonhuizen.

Eisen:

De installateur is verplicht gebruik te maken van gecertificeerde componenten die voldoen aan de Europese NEN-EN 50131-1:2006/A1:2009 en NEN-EN 50136-1:2012 of Technische Specificaties (TS'n). Van toepassing is security grade 2 / Klasse 2 (zie toelichting bij 4.3.5) Uitzondering hierop is dat de optische alarmgevers (flitsers) mogen worden toegepast die niet gecertificeerd zijn. Inbraaksignaleringsstelsel op het niveau Ed mogen ook volledig draadloos of gedeeltelijk draadloos worden aangelegd. Voor de alarmering is de ATS categorie SP1 (AL0) van toepassing.

De alarminstallatie dient te worden onderhouden en in overeenstemming te blijven met het niveau van het oorspronkelijke beveiligingsplan. Voor de controle hierop moet een onderhoudscontract worden afgesloten, dat voorziet in ten minste één onderhoudsbeurt per 2 jaar. Extra eisen bij toepassing van draadloze systemen: (zie niveau E1 eisen aan draadloze systemen)

Omvang projectie minimale eisen:

Voor alarmgevers zie artikel 6.6 en alarmtransmissie zie artikel 6.5 ATS categorie SP1 (AL0). Voor de alarmopvolging zie artikel 7.2 niveau R0

Indien een alarminstallatie van niveau Ed wordt aangesloten op een PAC moet worden voldaan aan de eisen onder E1, ATS categorie SP2 of DP1 (AL1) en R1.

4.3.2 E1 NIVEAU

De installateur is verplicht gebruik te maken van gecertificeerde componenten die voldoen aan de Europese NEN-EN 50131-1:2006/A1:2009 en NEN-EN 50136-1:2012 of Technische Specificaties (TS'n). Van toepassing is security grade 2 / Klasse 2 (zie toelichting bij 4.3.5)

Optische alarmgevers (flitsers) mogen worden toegepast die niet gecertificeerd zijn.

Inbraaksignaleringsstelsel op het niveau E1 voor woningen en bedrijven mogen ook draadloos worden aangelegd en dienen te worden onderhouden en in overeenstemming te blijven met het niveau van het oorspronkelijke beveiligingsplan. Voor de controle hierop moet een onderhoudscontract worden afgesloten, dat voorziet in ten minste één onderhoudsbeurt per jaar.

Extra eisen bij toepassing van draadloze alarmapparatuur:

1. Bij aansluiting op een PAC is doormelding van de beheers (supervisie)- en communicatiemeldingen (jamming) verplicht. De PAC moet op deze meldingen van een geactiveerd systeem reageren als bij een sabotagemelding. Het opnemen in computer log-files en achteraf rapporteren aan de installateur is onvoldoende. Er dient een schriftelijke overeenkomst met gebruiker en/of installateur te zijn, waarin is vastgelegd dat deze meldingen zo spoedig mogelijk aan klant en/of installateur worden doorgegeven, zodat adequate maatregelen getroffen kunnen worden.
2. De frequentie van onderhoud moet mede zijn gebaseerd op de levensduur/gebruiksdur van de batterijen met een minimum van één keer per jaar. De periode dat een batterij meegaat moet worden bepaald aan de hand van te verwachten activeringen. Batterijen moeten van het door de fabrikant voorgeschreven type zijn. Een batterij "laag" signaal dient vooraf door het stelsel lokaal te worden aangegeven. Indien de batterij niet tijdig wordt vervangen dient dit als laatste naar de PAC worden doorgemeld. Bij geen daadwerkelijke vervanging zal dit dan uiteindelijk leiden tot een zenderverlies signaal (1)

tabel 1

Woningen	Ed	E1	E2	E3
Volledig bedrade systemen	ja	ja	ja	ja
Draadloze systemen	ja	ja	ja	nee

Bedrijven	E1	E2	E3
Volledig bedrade systemen	ja	ja	ja
Draadloze systemen	Ja*	nee	nee

* wel in risicoklasse 1 en 2 en niet in risicoklasse 3, 3*, 4 en 4*

Omvang projectie minimale eisen:

- Ruimte detectie op plaatsen waar zich de attractieve goederen concentreren en op strategische plaatsen in het pand voor vroegtijdige detectie.
- Ruimte detectie voordat de CCS, en daartoe behorende delen, kunnen worden bereikt.
- Ruimte detectie ter plaatse van bediendelen.
- Ruimte detectie in ruimten met een waardeberging (safe) of wanneer daar meeneembeperkende maatregelen zijn toegepast.
- Openstand detectie op de entreeur(en) en nooduitgangen van het pand.

Met 'entreeur(en)' worden alleen de deuren bedoeld waar de bedieningspanelen zijn aangebracht die worden gebruikt om het pand te betreden of te verlaten. Deze indicatie geeft de uitloop- en inlooptijd aan.

Met 'nooduitgang(en)' worden de nooduitgangen bedoeld die door middel van vluchtwegaanduiding als zodanig herkenbaar zijn. Voor overige deuren wordt geadviseerd om deze deuren aan de buitenzijde van blind bouwbeslag te voorzien, om bedieningsfouten te voorkomen.

- Openstand detectie op rolluiken, rolhekken en schaarhekken met een beveiligingsfunctie.
- Openstand detectie op deuren van waardebergingen (compartimenten)
- Openstand detectie op de deur waarachter de CCS is opgesteld (meterkast)

Noot: Bij woningen kan het voorkomen dat de CCS niet altijd in de meterkast wordt geplaatst.

Bij bedrijven is het plaatsen van de CCS in een afgesloten ruimte wel een eis.

Voor de alarmering is de ATS categorie SP2 of DP1 (AL1) traject van toepassing, zie hiervoor de tabellen van de gekozen risicoklasse en beveiligingsklasse in document D03/375 (woningen) versie 1.4 (maart 2014) of D03/376 (bedrijven) versie 1.5 (maart 2014).

4.3.3 E2 NIVEAU

De installateur is verplicht gebruik te maken van gecertificeerde componenten die voldoen aan de Europese NEN-EN 50131-1:2006/A1:2009 en NEN-EN 50136-1:2012 of Technische Specificaties (TS'n). Van toepassing is security grade 2 of 3 / Klasse 2 of 3 (zie toelichting bij 4.3.5)

Optische alarmgevers (flitsers) mogen worden toegepast die niet gecertificeerd zijn.

Ruimtelijk werkende detectoren zijn van het type anti-masking. Voor woningen is dit geen eis.

Het is niet vereist dat de anti-masking signalering is ingeschakeld als de alarminstallatie is ingeschakeld. Maskering hoeft derhalve niet doorgemeld te worden. De maskering moet wel gesignaleerd worden en een afdekalarm veroorzaken. Een afdekalarm leidt ertoe dat de alarminstallatie niet ingeschakeld kan worden.

De alarminstallatie dient te worden onderhouden en in overeenstemming te blijven met het niveau van het oorspronkelijke beveiligingsplan. Voor de controle hierop moet een onderhoudscontract worden afgesloten, dat voorziet in ten minste één onderhoudsbeurt per jaar.

Inbraaksignaleringsstelsel op het niveau E2 voor woningen mogen ook draadloos worden aangelegd.

Omvang projectie minimale eisen:

- Ruimte detectie op plaatsen waar zich de attractieve goederen concentreren en op strategische plaatsen in het pand voor vroegtijdige detectie.
- Ruimte detectie voordat de CCS, en daartoe behorende delen, kunnen worden bereikt.
- Ruimte detectie ter plaatse van bediendelen.
- Ruimte detectie in ruimten met een waardeberging (safe) of wanneer daar meeneembeperkende maatregelen zijn toegepast.
- Openstanddetectie op de voor inbrekers bereikbare gevelopeningen (ramen en deuren in de buitenschil van het pand, mits niet mechanisch afgeschermd)
- Openstand detectie op rolluiken, rolhekken en schaarhekken met een beveiligingsfunctie.
- Openstand detectie op deuren van waardebergingen (compartimenten)
- Openstand detectie op de deur waarachter de CCS is opgesteld (meterkast)

Noot: Bij woningen kan het voorkomen dat de CCS niet in de meterkast wordt geplaatst.

Bij bedrijven is het plaatsen van de CCS in een afgesloten ruimte wel een eis.

Als gevelopeningen mechanisch zijn afgeschermd, dan is openstanddetectie bij E2 niet vereist. Voorbeelden van mechanische afscherming zijn: vaste afscherming: traliewerk, barrière stang(en), beweegbare gevelelementen: rolluik(en), rolhekken, schaarhekken.

Bij de toepassing van beweegbare gevelelementen dient de openstanddetectie wel op het rolluik, rolhek of schaarhek te zijn aangebracht.

Openstanddetectie en Schildetectie niveau 2: bij bedrijven in risicoklasse 3 waar geen C/M maatregelen worden getroffen geldt als extra eis: detectie en alarmering bij eerste aanval op bereikbare vaste en beweegbare gevelelementen die direct toegang geven tot de ruimten met de attractieve goederen.

Voorbeelden van detectiemethoden: glasbreukdetectie / trillingsdetectie / video bewaking met motion detectie / buitendetectie / inpandige ruimtedetectie aan de aanvalszijden e.d. Maatstaf bereikbaarheid gevelelementen is de NEN 5087:2013.

Opmerking:

Voor het bepalen van de openstanddetectie en schildetectie kan in afwijking van de norm voor de bereikbaarheid van gevelelementen NEN 5087:2013 de gewijzigde definitie worden aangehouden conform bijlage 1 in het handboek PKVW bestaande bouw.

Bron: <http://www.hetccv.nl/publicaties/webwinkel/PKVW/pkvw-bb-2011>

Voor de alarmering is de ATS categorie SP2 of DP1 (AL1) of de ATS categorie DP3 (AL2) traject van toepassing, zie hiervoor de tabellen van de gekozen risicoklasse en beveiligingsklasse in document D03/375 (woningen) versie 1.4 (maart 2014) of D03/376 (bedrijven) versie 1.5 (maart 2014).

4.3.4 E3 NIVEAU

De installateur is verplicht gebruik te maken van gecertificeerde componenten die voldoen aan de Europese NEN-EN 50131-1:2006/A1:2009 en NEN-EN 50136-1:2012 of Technische Specificaties (TS'n).

Van toepassing is security grade 3 / Klasse 3 (zie toelichting bij 4.3.5).

Optische alarmgevers (flitsers) mogen worden toegepast die niet gecertificeerd zijn.

Ruimtelijk werkende detectoren zijn van het type anti-masking.

Het is niet vereist dat de anti-masking signalering is ingeschakeld als de alarminstallatie is ingeschakeld. Maskering hoeft derhalve niet doorgemeld te worden. De maskering moet wel gesignaleerd worden en een afdekalarm veroorzaken. Een afdekalarm leidt ertoe dat de alarminstallatie niet ingeschakeld kan worden.

Voor de alarmering is de ATS categorie DP3 (AL2) of de ATS categorie DP4 (AL3) van toepassing, zie tabellen risicoklasse / beveiligingsklasse in documenten D03/375 versie 1.4 (maart 2014) en D03/376 versie 1.5 (maart 2014).

De alarminstallatie dient te worden onderhouden en in overeenstemming te blijven met het niveau van het oorspronkelijke beveiligingsplan. Voor de controle hierop moet een onderhoudscontract worden afgesloten, dat voorziet in ten minste één onderhoudsbeurt per jaar.

Omvang projectie minimale eisen:

- Ruimte detectie op plaatsen waar zich de attractieve goederen bevinden en op strategische plaatsen in het pand voor vroegtijdige detectie.
- Ruimte detectie voordat de CCS, en daartoe behorende delen, kunnen worden bereikt.
- Ruimte detectie ter plaatse van bediendelen.
- Ruimte detectie in ruimten met een waardeberging (safe) of wanneer daar meeneembeperkende maatregelen zijn toegepast.
- Openstand detectie op de voor inbrekers bereikbare gevelopeningen (ramen en deuren in de buitenschil van het pand, mits niet mechanisch afgeschermd).
- Openstand detectie op rolluiken, rolhekken en schaarhekken met een beveiligingsfunctie.
- Openstand detectie op deuren van waardebergingen (compartimenten)
- Openstand detectie op de deur waarachter de CCS is opgesteld (meterkast)

Noot: Bij woningen kan het voorkomen dat de CCS niet in de meterkast wordt geplaatst.

Bij bedrijven is het plaatsen van de CCS in een afgesloten ruimte wel een eis.

Als gevelopeningen mechanisch zijn afgeschermd, dan is openstanddetectie bij E3 niet vereist.

Voorbeelden van mechanische afscherming zijn: vaste afscherming: traliewerk, barrière stang(en), beweegbare gevelelementen: rolluik(en), rolhekken, schaarhekken.

Bij de toepassing van beweegbare gevelelementen dient de openstanddetectie wel op het rolluik, rolhek of schaarhek te zijn aangebracht.

Schildetectie niveau 2: bij bedrijven in risicoklasse 4 waar geen C/M maatregelen worden getroffen geldt als extra eis: detectie en alarmering bij eerste aanval op bereikbare vaste en beweegbare gevelelementen die direct toegang geven tot de ruimten met de attractieve goederen.

Voorbeelden van detectiemethoden: glasbreukdetectie / trillingsdetectie / video bewaking met motion detectie / buitendetectie / inpandige ruimtedetectie aan de aanvalszijden e.d.

Schildetectie niveau 3: bij bedrijven met de omschrijving attractieve goederen in magazijn in bijlage 1 van document D03/376 waar geen C/M maatregelen worden getroffen geldt als extra eis: detectie bij eerste aanval op bereikbare vaste en beweegbare gevelelementen, gevels, vloeren, daken en scheidingsconstructies die direct toegang geven tot de opslagruimten met de attractieve goederen.

Voorbeelden van detectiemethoden: glasbreukdetectie / trillingsdetectie / video bewaking met motion detectie / buitendetectie / inpandige ruimtedetectie aan de aanvalszijden e.d.

Voor de projectering van schildetectie op gevels geldt de definitie: schildetectie met een bereik tot een hoogte van 2,40 meter, de bereikbaarheid van vloeren omschrijft u in het PvE en hangt af of deze vloeren van onderaf toegankelijk zijn of het een aanvalszijde is. De schildetectie op daken wordt bepaald door de mate waarin door opklimmen het dak bereikbaar is.

Het dak moet dan vanaf maaiveld of gemeenschappelijk terrein bereikbaar zijn (maat van opklimbaarheid is 3,50 meter) of via doorklimmen vanaf een hoger gelegen bereikbaar werkvlak (2,40 meter) of door middel van duidelijke opklimmogelijkheden zoals schuttingen e.d.

Voor de alarmering is de ATS categorie DP3 (AL2) of de ATS categorie DP4 (AL3) van toepassing, zie hiervoor de tabellen van de gekozen risicoklasse en beveiligingsklasse in document D03/375 (woningen) versie 1.4 (maart 2014) of D03/376 (bedrijven) versie 1.5 (maart 2014).

4.3.5 EISEN AAN ALARMAPPARATUUR:

De toegepaste componenten dienen te voldoen aan de eisen van de NEN-EN 50131-1:2006/A1:2009 en NEN-EN 50136-1:2012 of Technische Specificaties (TS'n) Dit kan worden aangetoond door het overleggen van het productcertificaat, afgegeven door een voor het betreffende toepassingsgebied geaccrediteerde certificatie-instelling die tevens volledig lid is van de EA, of een verwijzing naar de lijst geregistreerde producten van de stichting REQ, NCP en CertAlarm.

Aan bovengenoemde eis kan ook worden voldaan door gebruik te maken van alarmapparatuur waarvoor een productcertificaat is afgegeven op basis een nationale norm, technische specificatie of productrichtlijn zoals bijvoorbeeld ANPI, Certec, VDS (klasse B=2 of C=3), NFA2P, IMQ vanaf klasse 2, etc. In de REQ lijst 'Overige producten' en de lijst NCP registratie wordt een overzicht gegeven van deze producten.

Toelichting: Bij periodiek onderhoud van projecten en bij hercertificatie hoeven de bestaande componenten waarvan de registratie is verlopen niet te worden vervangen.

In geval dat er in Nederland geen componenten beschikbaar zijn die voldoen aan de security grade of klasse voor het betreffende niveau kan gebruik worden gemaakt van componenten met een lagere security grade of klasse. Wanneer ook die ontbreken dient u zelf, op basis van goed vakmanschap, te bepalen of het product voldoet aan de duurzaamheid en functionele eisen die u hieraan stelt. Vermeldt afwijking op dit onderdeel in het PvE en het beveiligingsplan.

Het begrip Grade:

Security Grades: binnen de NEN EN 50131 / 50136 serie wordt uitgegaan van het niveau van de aanvaller (Inbreker / Overvaller)

Grade 1: (laag risico) Verwacht wordt dat aanvallers weinig kennis hebben van inbraak/overval detectiesystemen, en is gelimiteerd tot een beperkte set standaard gereedschappen. Ter indicatie VDS klasse A (geen sabotage circuit) Deze grade kan overeenkomen met de doe het zelf markt.

Grade 2: (laag tot gemiddeld risico) Verwacht wordt dat aanvallers gelimiteerde kennis hebben van inbraak/overval detectiesystemen en van vrij verkrijgbare gereedschappen en draagbare apparatuur waaronder o.a. multimeter.) Ter indicatie: ANPI, Certec, VDS klasse B. Deze grade kan overeenkomen met de particuliere markt.

Grade 3: (gemiddeld tot hoog risico). Verwacht wordt dat aanvallers bekend zijn met inbraak/overval detectiesystemen en hebben een uitgebreide set gereedschappen en draagbare elektronische

(meet)apparatuur. Deze grade kan gelden voor high-end particuliere markt, winkels en bedrijven.
Ter indicatie: ANPI, Certec, VDS klasse B en C

Grade 4: (hoog risico) Wanneer beveiliging voorrang heeft op alle andere factoren. Verwacht wordt dat aanvallers de middelen of vermogen hebben een inbraak tot in detail voor te bereiden en de beschikking hebben over een volledige set gereedschappen/ apparatuur inclusief mogelijkheden om vitale componenten van het inbraak/overval detectiesysteem te substitueren. Ter indicatie: VDS klasse C (Grade 4 kan gelden voor hoge risico's)

Environmental classes: binnen de EN 5013x wordt uitgegaan van het niveau van de aanvaller.

Class 1: (Binnen) Temperatuur goed geregeld, bijvoorbeeld particulier of kantoor.
(Temp: + 5C <-> + 40C, Rel. vochtigheid: 75%, niet condenserend)

Class 2: (Binnen generiek) Temperatuur minder goed geregeld, bijvoorbeeld onverwarmde magazijnen, gangen en trappenhuizen.
(Temp: - 10C <-> + 40C, Rel. vochtigheid: 75%, niet condenserend)

Class 3: (Buiten afgeschermd) Het product wordt blootgesteld aan buitentemperaturen, maar wordt is afgeschermd en wordt niet volledig blootgesteld aan het weer.
(Temp: - 25C <-> + 50C, Rel. vochtigheid: 75%, [30d] 85% <-> 95%, niet condenserend)

Class 4: (Buiten generiek) Het product wordt buiten volledig blootgesteld aan weer en wind.
(Temp: - 25C <-> + 60C, Rel. vochtigheid: 75%, [30d] 85% <-> 95%, niet condenserend)

4.3.6 BRANDPREVENTIE (BRAND) ROOKMELDERS.

In het Bouwbesluit 2003-artikel 2.146 worden niet ioniserende rookmelders met secundaire energievoorziening, aangesloten op het lichtnet, voor nieuwbouwwoningen en woningrenovatie verplicht gesteld (samengevat: gebouwen met een woonfunctie). Deze huisrookmelders moeten voldoen aan EN 14604 - NEN 2555. Voor bestaande woningen kan volstaan worden met rookmelder(s) met batterijvoeding. (Hier mogen ook rookmelder(s) met secundaire energievoorziening, aangesloten op het lichtnet worden toegepast). Ook de rookmelder voor bestaande woningen moet voldoen aan EN14604. Beide typen rookmelders moeten voorzien zijn van het KOMO keur.

Van toepassing is: bewoners dienen ingeval van rookontwikkeling tijdig gealarmeerd te worden door middel van een akoestisch signaal, waardoor de tijd om maatregelen te nemen en/of te vluchten aanzienlijk kan worden vergroot.

Maatregelen: In gebouwen met woonfuncties moeten in de verkeersruimten één of meerdere rookmelders geplaatst worden. Verkeersruimten zijn die ruimten waarop verblijfsruimten uitkomen; verkeersruimten zijn doorgangruimten die zich op alle verdiepingen in een woning bevindt (vluchtwegen) Voor projectering / plaatsing wordt verwezen naar het Bouwbesluit 2003- artikel 2.146 en NEN 2555- artikel 7. Hierbij gaat de voorkeur uit naar rookmelders met een secundaire energievoorziening die zijn aangesloten op het lichtnet. Hier mogen ook rookmelders met batterij voeding worden aangebracht.

Ter verhoging van de veiligheid wordt aangeraden de rookmelders onderling te koppelen. Installatie van rookmelders aangesloten op het lichtnet moet volgens de geldende voorschriften voor elektrotechnische installaties gedaan worden (NEN 1010). Daarnaast gelden de montagevoorschriften van de leverancier die bij elke rookmelder meegeleverd wordt. De gebruiksaanwijzing van de rookmelder moet, t.b.v. de bewoners, in de woning achtergelaten worden. Regelmatig dient de bewoner te controleren of de rookmelder nog naar behoren werkt. Door de testknop op de rookmelder in te drukken worden de functie van de rookmelder (en rookmelders in het geval deze gekoppeld zijn) getest. Bij doven en slechthorende bewoners is het zeer aan te bevelen een optische signalering aan te brengen en een trilwekker onder het kussen. Eenvoudige blusmiddelen kunnen als aanvullend advies worden opgenomen.

Aanbevelingen: het is toegestaan een rookmelder aan te sluiten op een alarminstallatie, mits er sprake is van aansluiting op een aparte 24-uurs groep van de Centrale Controle- en Sturingseenheid (CCS). De rookmelder(s) kunnen d.m.v. een potentiaalvrij contact op een dergelijke alarminstallatie aangesloten worden mits er geen wettelijke bepalingen zijn om een ontruimingsinstallatie in het gebouw aan te brengen. Anders wordt verwezen naar de bepalingen volgens NEN-EN 2535 en NEN-EN 2575.

Indien er sprake is van een onveilige situatie dient het specifieke signaal als zodanig herkenbaar bij de Particuliere Alarm Centrale (PAC) binnen te komen. Hierbij moet rekening worden gehouden met voorschriften van de alarmopvolgers. Dit betekent dat voor brandmelders aangesloten op een inbraakalarminstallatie ook altijd alarmverificatie moet plaatsvinden voordat de brandweer door de PAC, naar de woning mag worden gestuurd.

Bij bedrijven is branddetectie een apart aandachtsgebied en in de gebruiksvergunning mogelijk een eis. In dat geval verwijzen we naar de CCV certificatie- en inspectieschema's BMI, NEN-EN 2535 en NEN-EN 2575. Daar waar deze eisen niet van toepassing zijn, kan het aanbrengen van enkele brandmelders (rookmelders) op vitale plaatsen in het bedrijf zinvol zijn. Deze mogen onder voorwaarden worden aangesloten op het inbraaksignaleringssysteem.

Van toepassing is: additionele toepassingen zoals brand-, overval-, kluis- en technische alarmen mogen alleen op een aparte groep worden aangesloten op de CCS. De ontstane onveilige situaties worden als afzonderlijk herkenbare meldingen doorgemeld naar de PAC. Hierbij moet rekening worden gehouden met voorschriften van de alarmopvolgers. Dit betekent dat voor brandmelders aangesloten op een inbraakalarminstallatie ook altijd alarmverificatie moet plaatsvinden voordat de brandweer door de PAC, naar het object mag worden gestuurd. Zowel bij woningen als bedrijven geldt dat deze additionele toepassingen de goede werking van de alarmapparatuur nimmer nadelig zal beïnvloeden. Het brandalarm en het inbraaksignaleringssysteem mogen niet van hetzelfde akoestische signaal gebruik maken. Voor een rook/brandalarm wordt gebruik gemaakt van een zogenaamd slow-whoop-signaal.

4.3.7 BEVEILIGINGSVERLICHTING

Voor woningen is in het bouwbesluit en het Politie Keurmerk Veilig Wonen beveiligingsverlichting verplicht gesteld. Van toepassing is:

Bereikbare deuren van een woning, die vanuit openbaar gebied of andere woningen zichtbaar zijn. Deze dienen zodanig te zijn verlicht dat de bezoekers en bewoners bij schemer of donker in het licht staan.

Maatregelen:

Bij achter- en zijdeuren op de begane grond is een buitenlamp aangebracht. Bij (balkon)deuren op de eerste verdieping is een buitenlamp aangebracht, indien deze door opklimming bereikbaar is en er op de begane grond geen verlichting is.

Indien de voordeur van de woning in een portiek, nis of onder een overkapping is gelegen, is een buitenlamp aangebracht. Als er meer deuren in hetzelfde gevelvlak aanwezig zijn, kan worden gekozen voor een centraal aangebrachte buitenlamp, mits de lichtval op de deuren niet wordt onderbroken door verspruingen op of in de gevel.

Indien er sprake is van voldoende openbare verlichting ter plaatse van de bereikbare deuren is deze beveiligingsrichtlijn niet van toepassing.

De voorkeur gaat uit naar een vandalismebestendig armatuur (slagvaste kap en buiten bereik aangebracht) met schemerschakelaar, bewegingssensor of tijdschakelaar.

Installatie volgens de NEN1010 en de voorschriften van het gecontracteerde Energiebedrijf. Daarnaast gelden de bijgeleverde montagevoorschriften van de leverancier.

Toelichting:

Deze beveiligingsrichtlijn is zowel van toepassing op deuren op de begane grond van (flat)woningen als op (balkon)deuren op de eerste verdieping, indien deze door opklimming bereikbaar zijn.

Aanbevelingen:

Verlichting bij de voordeur op begane grond alsook op de galerij, geeft een verhoging van de sociale veiligheid. Bezoekers zijn duidelijk zichtbaar en herkenbaar, zowel vanuit de woning als vanuit de omgeving. Aanwezige struiken en bomen mogen de lichtval niet hinderen.

Indien de afstand tussen achter- of zijgevel van de woning en een aanwezige schuur, garage of berging beperkt is, kan een eventueel aanwezige buitenlamp op de gevel van deze bijgebouwen voldoende licht werpen op de deur. Verlichtingssterkte is minimaal 10 lux.

Bij bedrijven is beveiligingsverlichting een apart aandachtsgebied. Een inbreker wordt niet graag gezien. Beveiligingsverlichting langs de buitenkant van het gebouw werkt preventief.

Tenminste, indien de omgeving (sociale) controle toelaat en de inbreker inderdaad de kans loopt om gezien te worden. Aandachtpunten zijn: Verlichting van deuren en in afwijking van PKVW ook de ramen. De hoogte waarop de buitenlampen op de gevel van het gebouw en/of bijgebouwen bij voorkeur worden opgehangen is 2,7 meter. Wat is het doel van de verlichting? Sociale controle, preventie, beveiliging, cameratoezicht e.d.

Lichtreflectie-eigenschappen omgeving, hoeveelheid licht, kleur van het licht, kleurweergave index Ra waarde. Plaats en type van de lichtbron, soorten armaturen, energieverbruik, levensduur van lampen, wijze van in - uitschakelen, lichthinder, milieu en gezondheid, onderhoud e.d.

In een goed beveiligingsplan is de beveiligingsverlichting een belangrijk onderwerp.

Van toepassing is de NEN 1010 en aanwijzingen van de leverancier van het product.

4.3.8 CAMERASYSTEMEN

Camerasystemen spelen een steeds belangrijk wordende rol bij preventie.

In relatie tot de preventiewaarde kan een onderscheid worden gemaakt tussen camerasystemen waarvan de beelden binnen het bedrijfspand kunnen worden weergegeven. Denk aan overval preventie in winkels en toezicht op vitale plaatsen in het bedrijf

Er kan sprake zijn van beeldopslag en/of dat de camerabeelden worden verzonden naar een centraal punt PAC of service centrale.

Camerabeelden kunnen ook worden aangewend bij alarmverificatie.

Gebruik van videocameratoezicht (CCTV) is aan veel richtlijnen en wettelijke (ook Europese) regels gebonden. We noemen er slechts enkele zoals de Wet bescherming persoonsgegevens en de Wet heimelijk cameratoezicht, Een werkgroep buigt zich momenteel over de invulling van de technische - en procedurele eisen waaraan camerasystemen voor alarmverificatie moeten voldoen. Dit onderdeel wordt nog ingevuld in dit document en de installatievoorschriften voor alarmapparatuur.

4.3.9 TOEGANGSCONTROLE

Toegangscontrolesystemen en terreinafscheidingen (hekwerken)

Uitvoeringsnormen zoals bij inbraakbeveiliging zijn in Nederland niet beschikbaar.

Voor toegangscontrolesystemen geldt: de NEN-EN 50133 deel 1 t/m 7, CE aantekening van de fabrikant en RDR nummer voor RF apparatuur. Er zijn classificaties voor systemen (A, B en Ba) en voor toegangscontrole lezers (klasse 0 t/m 3)

Bij terreinafscheidingen gaat het om een substantiële belemmering voor inbrekers om het terrein te betreden. De preventiewaarde neemt toe naarmate deze afscheidingen zijn voorzien van schrikdraad, detectie tegen door - of overklommen en sabotage.

4.3.10 BUITENDETECTIE

Bij deze detectiemiddelen gaat het om systemen die het betreden van terreinen door personen of voertuigen detecteert. We onderscheiden E-veld systemen, schrikdraad gekoppeld aan detectie, drukdetectie, trillingsdetectie, magneetcontacten, actief infrarood, passief infrarood, radar, video-motion e.d. Het doel is: afschrikken, detecteren, vertragen, actie ondernemen en toegang verschaffen.

Buitendetectie systemen vragen altijd alarmverificatie, in combinatie met bijvoorbeeld alarmgestuurde dome-video-camera's bieden deze maatregelen een goede oplossing. De klimatologische omstandigheden waaronder deze systemen functioneren zijn niet te vergelijken met geveldetectie of ruimte detectie in een gebouw.

5. COMPARTIMENTERING EN /OF MEENEEMBEPERKENDE MAATREGELLEN (C/M)

5.1 INLEIDING

Een nog steeds groeiend aantal inbraken en diefstallen bij bedrijven en particulieren noopt tot het nemen van preventieve maatregelen. Inventarisatie van schadecijsers en modus operandi leiden tot de volgende stelling: inbraak - en diefstalpreventie blijft een absolute noodzaak, waarbij de aanpak met name dient te worden gezien vanuit de positie van de crimineel. Ofwel: welke voorziening sorteert het beste effect om een inbreker te slim af te zijn? Het is daarbij de kunst om de zichtbare drempel voor de inbreker zo hoog mogelijk te leggen, dat het voor hem niet de moeite loont een inbraak - of diefstalpoging te ondernemen. Ondanks soms uitgebreide preventieve maatregelen, worden goederen toch gestolen; vaak binnen een zeer kort tijdsbestek, de zogenaamde 'snelkraak'. Na het doorbreken van de bouwkundige schil van een gebouw (via raam, deur of wand) is de inbreker in staat om binnen zeer korte tijd voldoende waardevolle goederen te stelen om de inbraak 'lonend' te maken. Dit gebeurt ondanks de aanwezige alarmering, omstanders of bewoners.

Dat dit de praktijk is, blijkt uit de volgende redenen:

- de schil van een gebouw is zelden voorzien van elektronische detectie, waardoor er tot het moment van binnenkomst geen alarm zal zijn (er is dus vaak veel tijd om in te breken),
- de buitenzijde van een gebouw is veelal bouwkundig - door de omvang - moeilijk haalbaar inbraakvertragend te maken. Bovendien kunnen daders in alle rust (ontbreken van sociale controle) en met gebruik van zware inbrekersgereedschappen hun gang gaan. Buitendetectie om het gebouw is een zeldzaamheid,
- nadat men is binnengedrongen bestaan er, in pandig, doorgaans nauwelijks vertragingen meer,
- de inbreker weet dat een elektronisch alarm niet direct tot alarmopvolging leidt en dat hij vaak tien tot vijftien minuten de tijd heeft om goederen van zijn gading te vergaren. De praktijk wijst op aanrijtijden van een half uur of langer,
- de inbreker weet vaak, door een gedegen voorkennis, waar de bewuste goederen zich bevinden,
- attractieve goederen zijn veelal niet erg volumineus, waardoor er in een kort tijdsbestek goederen zijn te verzamelen en er snel sprake is van een relatief grote buit,
- de meeste attractieve goederen liggen vaak, vanwege de commercie, vóór in de winkel en/of aantrekkelijk uitgesteld voor het publiek. Dus meestal zó voor het grijpen,
- inbrekers worden steeds brutaler en lijken zich vaak niet te storen aan getuigen en/of omstanders in een alarmfase, sterker nog, deze worden nog al eens bedreigd.

5.2 ATTRACTIEVE GOEDEREN

Goederen zijn pas écht attractief als deze snel vervoerbaar, goed verhandelbaar en zonder directe pakkans voor de crimineel kunnen worden verkregen. De afzet en het transport ervan zijn, door voorkennis en inventiviteit vooraf, goed geregeld. Hoe groter de buit, hoe slimmer het 'gilde'!

Als het gaat om attractieve goederen zijn er drie situaties te onderscheiden, nl.;

- goederen voor eigen gebruik,
- verkoopgoederen in winkel en showroom
- goederen in opslag of in magazijn.

Voor een goed functioneren van alle meeneembeperkende maatregelen is een deugdelijke en tegen sabotage beveiligde alarminstallatie een voorwaarde. Samen met het direct ter plaatse ontstane optisch- en akoestisch signaal + de doormelding én de alarmopvolging kunnen we het gedrag van de crimineel dusdanig beïnvloeden dat de kans op diefstal van de attractieve goederen kleiner wordt.

Onderstaand worden in dit verband voor de drie situaties een paar voorbeelden gegeven bij een 9-tal symbolische pictogrammen. In feite moet men, door inventief te zijn en door rekening te houden met de meest geschikte materialen, zelf de beste aanpak bepalen. Om in showrooms en binnen kantoren een esthetisch verantwoorde voorziening te maken, kan gebruik worden gemaakt van inbraakwerende materialen als polycarbonaat, hout, geplastificeerd of gespoten traliewerk, roestvrij staal enz. Standaardvoorzieningen zijn verkrijgbaar om computers en randapparatuur te verankeren aan wand, vloer of bureau.

Veel standaard materialen en bouwkundige voorzieningen, zoals bijvoorbeeld stalen rolluiken, kunnen ook worden toegepast in binnensituaties. Stalen zee-containers kunnen dienst doen als -, c.q. binnen magazijn, of opslag.

Ook met alleen organisatorische maatregelen kan soms al een goed effect worden verkregen, immers door de attractieve goederen te verstoppen, zal het zoeken ernaar, in een alarmfase, te veel tijd vergen.

De verdere invulling en concretisering zijn aan de beveiligingsadviseur en de gebruiker zelf, waarbij rekening zal moeten worden gehouden met situering, materiaalsoort en -sterkte, esthetische eisen, bedieningsgemak en kosten. Tijdelijke en/of 'mobiele' voorzieningen vragen om veel discipline en organisatie, waarbij diverse handelingen elke keer bij winkelsluiting terugkeren en als hinderlijk kunnen worden ervaren. Daardoor is het gevaar groot dat men ze, zeker na verloop van tijd, achterwege zal laten en het meeneembeperkende effect nihil wordt. Heel essentieel is het effect van een bouwkundige barrière of voorziening binnen een elektronisch beveiligd gebied met een zeer deugdelijke en goed zichtbare preventieve uitstraling.

C/M maatregelen zijn ook zeer geschikt voor goederen met lage eigen waarde die wel goederen met een hoge waarde vertegenwoordigen. Denk daarbij aan sleutels en kentekenbewijzen voor auto's. Het compartimenteren van sleutels (kluis) is, samen met uitrijdbeveiliging een goed voorbeeld van C/M maatregelen.

5.3 NORMSTELLING

De enige norm die hier in feite telt is het tijdsbestek wat men wint door de toepassing van een goede meeneembeperkende maatregel nadat een elektronisch alarm is afgegaan.

Inventiviteit is hier troef, immers een potentiële inbreker komt overdag eerst kijken hoe het met alle maatregelen tegen inbraak gesteld is. Indien de genomen maatregelen overtuigend genoeg zijn, zullen deze maar zelden op hun sterkte worden beproefd opdat, als gezegd, ook inbraakpogingen waarschijnlijk achterwege zullen blijven. Afhankelijk van de duur van een alarmopvolging (in tijd gemeten) moet een oplossing voor de attractieve goederen of artikelen worden bedacht. Het gebruik van sterk materiaal, zwaar hang- en sluitwerk is uiteraard een eerste vereiste (zie BRL 3104 hang- en sluitwerk en BRL 9904 hangsloten), waarbij vooral de onderlinge samenhang van de toegepaste materialen telt. Tot slot kan elke functionele meeneembepurende maatregel individueel tot norm worden verheven als blijkt dat het voor een inbreker niet de moeite loont eraan te beginnen tijdens een alarmfase.

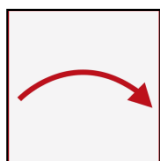
5.4 CONCLUSIE

Slechts enkele standaard oplossingen zijn hier aan te dragen, zodat met betrekking tot dit onderwerp een beroep wordt gedaan op het inlevingsvermogen van iedere adviseur, ondernemer of particulier. Een effectieve meeneembepurende maatregel zal zelden op zijn sterkte worden beproefd, immers een inbreker ziet (overdag reeds) waar hij tijdens een elektronisch alarm aan moet gaan beginnen. Inventiviteit blijft troef, waarbij de keuze voor materialen, vormgeving, opstelling en samenhang voor elke oplossing weer anders kan zijn. De mogelijkheden van vormgeving, uiterlijk, materiaaltoepassing en gebruikersgemak zijn legio, waardoor in feite voor elke situatie een meeneembepurende maatregel kan worden bedacht. Het zijn het inzicht in de materie en de wil om op deze manier inpandig te beveiligen die hierbij de doorslag geven. Veel goede oplossingen zijn inmiddels op een inventieve en creatieve manier gerealiseerd.

5.5 PICTOGRAMMEN, UITLEG EN VOORBEELDEN

Op de volgende pagina's zijn negen pictogrammen afgebeeld en situaties beschreven voor de toepassing van meeneembepurende maatregelen.

5.6 C/M 1 NIVEAU PRESTATIE-EIS 3 MINUTEN INBRAAKVERTRAGING



5.6.1 VERPLAATSEN

Eigen gebruik

Een verstopt artikel is moeilijk en niet snel vindbaar na een elektronische alarmering!

Winkel of showroom

Door het gebruik van een kelder- of bovenverdieping voor het etaleren van duurdere goederen is de weg naar deze goederen toe vaak te lang na het activeren van het elektronisch alarm. Ook de afvoer van de goederen neemt immers meer tijd in beslag. Deze oplossing is bepaald niet 'zaligmakend' en dient uitsluitend voor enkele kleinere gevallen, omdat de praktijk ook uitwijst dat het 'gilde' vaak zeer brutaal is en/of met meer personen tegelijk veel aandurft en veel aankan in een zeer kort tijdsbestek.

Magazijn of opslag

Door attractieve goederen hoog in de stellingen te plaatsen, ontstaat een grote handicap voor de inbreker, hij moet immers over een heftruck beschikken om de goederen naar beneden te halen. Binnen een elektronisch beveiligd gebied is dit bijna een onmogelijkheid. Wél is het zaak om de heftruck na sluitingstijd onklaar te maken! Niet zelden komt het voor dat de crimineel het eigen expeditievoertuig, welke soms al geladen staat met attractieve goederen, gebruikt voor de afvoer. Meeneembepurende maatregelen dienen dus niet alleen te worden toegepast op het product maar ook op bedrijfsmiddelen en gereedschappen die kunnen worden gebruikt voor het verbreken, verzamelen en vervoeren. Hiermee vergelijkbaar is de opslag op een entresol, waarbij het essentieel is dat een trap niet een, twee, drie de mogelijkheid biedt om boven te komen na inbraak.



5.6.2 KOPPELEN

Eigen gebruik

Een PC unit kan door middel van een stalen (standaard) kabel worden gekoppeld aan een bureau. Ook de steeds vaker voorkomende flatscreens in kantoren zijn op deze manier minder interessant te maken voor diefstal. Zie hiervoor de aanbevelingen

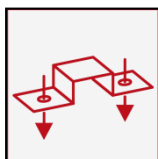
Meeneembepurende Producten op basis van SKG-KE 470 augustus 2005

Winkel of showroom

Door duurdere fietsen, scooters of bromfietsen onderling te koppelen met beugelsloten (eigen verkoop) en/of geplastificeerde staalkabels wordt snelkraak voorkomen. Een goed zichtbare drempel werkt op deze manier met name in een dagsituatie zeer preventief. De inbreker weet in dit geval dat hij na een elektronisch alarm nog met een volgend probleem te kampen krijgt!

Magazijn of opslag

Niet verpakte en grotere vaak verrijdbare handelsgoederen in magazijnen kunnen onderling met zwaardere geplastificeerde kabels onderling worden gekoppeld. Bijvoorbeeld onderling gekoppelde aanhangwagens of aggregaten zijn moeilijk snel aan te koppelen en mee te nemen. Indien dit binnen een elektronisch beveiligd gebied gebeurd is diefstal vrijwel onmogelijk binnen het tijdsbestek van de alarmopvolging.



5.6.3 VERANKEREN

Eigen gebruik Een antieke klok kan worden verankerd en tegen snelkraak beschermd door het vastzetten ervan met bijvoorbeeld een chemisch anker of keilbout. Zo zijn er ook speciale bevestigingen op de markt om schilderijen te verankeren. Aanhangwagens zijn moeilijk te ontvreemden en aan te koppelen als deze zijn verankerd door middel van het koppelen van de dissel aan een gefixeerde kogel aan het gebouw (denk aan een bouwmarkt)

Winkel of showroom

Door boormachines en/of ander elektrisch gereedschap te verankeren aan het schap, is snelkraak na elektronische alarmering moeilijk. Door de boorkop op gefixeerde stiften te plaatsen en/of de machines met kabels te beveiligen, wordt een goed effect verkregen.

Grotere machines als aggregaten, hogedrukreinigers en/of compressoren kunnen met behulp van een zware geplastificeerde kabel worden verankerd aan gefixeerde ankers in de betonnen vloer van de showroom.

Magazijn of opslag

Denk in dit verband ook aan het koppelen van aanhangwagens, grotere verrijdbare opslagen e.d. Elektrotechnische maatregelen zoals het spanningsloos maken van hefdeuren, rolluiken, verlichting, e.d. zijn feitelijk ook meeneembepurende maatregelen die na sluitingstijd effect sorteren.

5.7 C/M 2 NIVEAU PRESTATIE-EIS 5 MINUTEN INBRAAKVERTRAGING



5.7.1 KISTEN OF KASTEN

Eigen gebruik Een aannemersbedrijf kan na werktijd zijn elektrisch gereedschap verzamelen in een zelf gemaakte verrijdbare houten kist of grotere kast om inbraak en snelkraak te voorkomen. Let hierbij wel op dat de waardeberging zelf goed wordt gefixeerd, anders is de totale buit in één keer vertrokken. De andere machines in een werkplaats zijn groot en zwaar en dus veel minder attractief, zeker voor een snelkraker.

Een dergelijk beleid werkt ook een zekere mate van orde en netheid in de hand en komt het preventiebewustzijn ten goede.

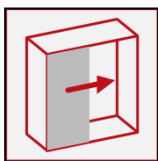
Winkel of showroom

De duurdere elektronica die bijvoorbeeld bij een verkoopadres van bootaccessoires aanwezig is, zoals navigatie - en sonarsystemen, kunnen in een fraaie maar goed afsluitbare houten of stalen kast worden geborgen die deel uitmaakt van de stellingwanden. Door deze kast in de dagsituatie simpelweg open te zetten ontstaat na sluitingstijd een gemakkelijk afsluitbare en effectieve preventieve voorziening tegen snelkraak. Ook tabaksartikelen zouden in een soortgelijke verkoopsituatie kunnen worden uitgesteld.

Magazijn of opslag

Alarm -, audio - en navigatiesystemen zijn bijvoorbeeld bij een grotere autodealer in het magazijn goed geborgen in deugdelijk afsluitbare houten (38 mm hechthout) of stalen kasten. Het hang- en sluitwerk daarvan moet voldoen aan niveau B2 zijn, evenals de bevestiging van bijvoorbeeld de overvalsluiting voor een hangslot. Standaard zwaardere archiefkasten of (tweedehands) grotere safes kunnen veelal dienst doen als opslag van inbraakgevoelige goederen.

5.7.2 VITRINES



Eigen gebruik Een vitrine is in deze situatie eigenlijk geen optie, of het zou zo moeten zijn dat het een verzameling betreft in de woning of op kantoor in een kast met beglazing waarbij gebruik gemaakt wordt van gelaagd glas (Swarowski kristal of antiek)

Winkel of showroom

Goederen als zonnebrillen, luxe artikelen, mobiele telefoons, digitale camera's, computerartikelen etc. kunnen worden gepresenteerd binnen een winkel in afgesloten schappen of vitrines (ook tegen diefstal overdag) Door gebruik te maken van lexan en/of gelaagde beglazing (norm NEN-EN 356) in een deugdelijk kader, met goed sluitwerk kan een beveiligde vitrine worden gerealiseerd. Veelal is het een eigen fabrikaat of zal het vernuft van een vitrinebouwer hierbij doorslaggevend zijn.

Magazijn of opslag

Niet van toepassing.



5.7.3 HEKWERKEN

Eigen gebruik Een cafébedrijf met audio-installatie en een flinke Cd-opslag achter de bar kan dit attractieve geheel eenvoudig tegen snelkraak beschermen door hiervoor na sluitingstijd consequent een raster of hekwerk te plaatsen en af te sluiten. Apparatuur met Cd's als inhoud en digitale PC-opslag van muziek moet niet worden onderschat qua

attractiviteit en vervangingskosten

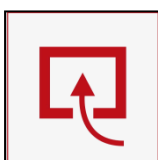
Winkel of showroom

Een inpandig rolluik, rol- of schaarhek (of soms zelfs bouwhek) kan in een hoek van een winkel dienst doen om een compartiment te vormen, waarachter na sluitingstijd de attractieve goederen worden gestald. Het is voor een inbreker de moeilijkste situatie om eenmaal in de winkel en tijdens een elektronisch alarm, een poging te ondernemen om dit hekwerk te slopen. De visuele drempel zal in dit geval ook al in de dagsituatie helpen voorkomen dat een inbreker zijn plannen voor inbraak voorbereidt. Denk in dit verband bijvoorbeeld aan leren motorkleding en accessoires in een motorshowroom en verkoopruimte.

Magazijn of opslag

Een schappengedeelte voor de opslag van attractieve materialen in een magazijn is tegen snelkraak beschermd door de gang - of looppaden te blokkeren met een inpandig hekwerk. Een goede afsluitmogelijkheid en een hek van afdoende hoogte en sterkte zijn dan essentieel. Een hekwerk tussen expeditie en magazijn doet in dit verband ook dienst om te voorkomen dat 'Jan en alleman' een kijkje in de keuken kunnen nemen! Als aandachtspunt geldt dat rekening moet worden gehouden met vluchtwegen.

5.8 C/M 3 NIVEAU PRESTATIE-EIS 10 MINUTEN INBRAAKVERTRAGING



5.8.1 COMPARTIMENTEN

Eigen gebruik Als voorbeeld kunnen laptops binnen afgesloten gebied worden geborgen in deugdelijk (en dus vaak met extra sloten) afgesloten inpandige ruimten. Een compartiment als dit is binnen het bedrijf vaak een ruimte waarin ook de server, een datasafe, aanwezige duurdere gebruikersgoederen (bijvoorbeeld laserapparatuur) of documenten kunnen worden geborgen of geplaatst. Een dergelijk compartiment dient geheel inpandig te zijn gesitueerd, waarbij een aanval in alle gevallen wordt voorafgegaan door een elektronisch alarm met opvolging. Alle 6 zijden (dus óók de boven - en onderzijde) van het compartiment moeten worden afgeschermd door elektronische detectie.

Winkel of showroom

Als voorbeeld kan hier een zonnebrillenstandaard (verrijdbaar?) worden genoemd in een optiekzaak die consequent na winkelsluiting wordt geplaatst binnen een extra afsluitbaar gemaakt gedeelte, zoals een inpandig kantoor of misschien zelfs een toiletruimte. Mobiele telefoons zijn als voorbeeld na winkel- sluiting goed geborgen in een, binnen de winkel of showroom gerealiseerd, compartiment (onder de toonbank, in een tweedehands safe of in een versterkte kast). Een dergelijk compartiment is te realiseren uit hout en/of staal met zwaar sluitwerk.

Magazijn of opslag

Attractieve goederen kunnen worden opgeslagen en/of geplaatst in een standaard of speciaal te realiseren compartiment uit vlechtwerkstaal, hout, baksteen, stekmetaal etc. Zwaar sluitwerk en een sabotagevrije elektronische detectie rondom zijn noodzakelijk. Alle aanvalszijden moeten goed onder de loep worden genomen, waarbij het essentieel is dat een aanval op het compartiment altijd eerst wordt voorafgegaan door elektronische alarmering. De braaktijd en dus de zwaarte van het compartiment, worden afhankelijk gesteld van de waarde van de op te bergen goederen. Met het oog op de alarmopvolging, die vandaag de dag gemakkelijk kan oplopen tot meer dan 15 minuten, zou de ondergrens op deze tijd moeten liggen, oplopend tot meer dan een uur. Standaard oplossingen met keurmerk zijn momenteel in de markt verkrijgbaar. Dit stalen compartiment wordt samengesteld uit modules en segmenten.

Opmerking bij 5.8.1; indeling in niveaus voor compartimenten

In de tabel van de beveiligingsklasse voor bedrijven wordt de vereiste compartimentering aangeduid met C1, C2 of C3. Bij C1 gaat het om een safe of inbraakwerende kast die geschikt is voor de op te bergen waarde.

Een compartiment op niveau C1 is een inpandige ruimte waarvan de deur voldoet aan B1 en de vloer, wanden en plafond een gelijkwaardige weerstand bieden. (prestatie-eis 3 minuten inbraakvertraging) C2 en C3 hebben betrekking op zwaardere bouwkundige compartimenten.

Voor de verschillende compartimenten worden de navolgende eisen gehanteerd.

Bij het inrichten of bouwen van een compartiment kan het gaan om één enkele ruimte of kast, maar ook om een samenstel van ruimten die samen één compartiment vormen.

Bij het inrichten of bouwen gelden de volgende eisen:

Alle bouwkundige afscheidende constructies van het compartiment dienen voldoende fysieke sterkte te bezitten om de vereiste inbraakvertraging te leveren. Dit wil zeggen dat er niet alleen eisen worden gesteld aan de wanden van het compartiment, maar ook aan de andere - mogelijke - aanvalszijden voor inbrekers. Dit betreft dus de vloer, het plafond of het dak van het compartiment, voor zover bereikbaar voor inbrekers.

Wanden: de inbraakwerendheid van de wanden van een compartiment (of vloer, plafond of dak) worden niet alleen bepaald door de dikte of het soort materiaal waaruit deze zijn geconstrueerd. Van belang zijn ook factoren als de verankering of de aanwezigheid van openingen.

De wanden van een C2 of C3 compartiment dienen te bestaan uit gewapend beton of uit metselwerk. Het metselwerk kan worden opgetrokken in baksteen, kalkzandsteen of betonblokken. Lichte blokken of stenen, zoals cellenbeton, lichtbeton, porisosteën e.d., zijn eveneens toepasbaar, mits een dikte wordt aangehouden die twee maal zo groot is als de hierna genoemde waarden.

De dikte van wanden van beton of metselwerk dient ten minste te bedragen voor C2: 100 mm en voor C3: 200 mm. Indien de hoogte van de wanden meer dan 3 meter bedraagt, dienen de genoemde dikten te worden verdubbeld. Uiteraard kunnen ook wanden worden toegepast die van andere materialen zijn geconstrueerd, mits daarmee een gelijkwaardige inbraakwerendheid wordt verkregen.

De wanden dienen afdoende aan de omliggende constructies te worden verankerd, waarbij de onderlinge afstand tussen de verankeringen niet meer dient te bedragen dan 500 mm.

De wanden dienen te worden opgetrokken tot - en goed aan te sluiten tegen - de bovenliggende vloer- of dakconstructie. In ruimten met systeemplafonds betekent het voorgaande dat de wanden dienen door te lopen tot boven het systeem plafond en aan te sluiten aan de bovenliggende vloer- of dakconstructie.

In de wanden dienen bij voorkeur geen ramen aanwezig te zijn. Als er ramen aanwezig zijn dienen ze voorzien te zijn van inbraakwerende beglazing dan wel glasafscherming.

Deuren: deuren in wanden van een C2 compartiment dienen te voldoen aan de norm NEN 5096:2012 weerstandsklasse 3 (prestaties is 5 minuten) of daaraan gelijkwaardig te zijn. Eventueel aanwezig glas in dergelijke deuren dient vervangen te worden door inbraakwerende beglazing dan wel voorzien van glasafscherming.

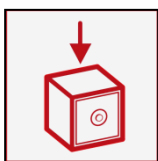
Deuren in wanden van een C3 compartiment dienen minimaal te voldoen aan de norm NEN-EN 1627:2011 weerstandsklasse 4 (prestaties is 10 minuten) of daaraan gelijkwaardig waarbij geen glas bezetting aanwezig dient te zijn. In het PvE kunnen nader gespecificeerde - en op het desbetreffende risico afgestemde - eisen worden gesteld.

Vloer, plafond of dak: de vloer en het plafond of dak maken eveneens onderdeel uit van het compartiment. Voor zover deze afscheidende constructies aan de buitenzijde van het compartiment voor inbrekers bereikbaar zijn, betekent het voorgaande dat ze voldoende inbraakwerend moeten zijn.

Indien het mogelijk is om met gebruik van handgereedschap, zoals plaatschaar, decoupeerzaag e.d., een opening te maken waardoor het compartiment betreden kan worden. Bij constructies, zoals een houten vloer of een dak van geprofileerde staalplaten, zullen daarom aanvullende maatregelen getroffen moeten worden. Dit heeft niet alleen betrekking op de elektronische bewaking, maar ook op het aanbrengen van een extra fysieke barrière aan de binnenzijde, bijvoorbeeld in de vorm van een doeltreffende beplating met staalplaat of strekmetaal.

Altijd inbraaksignaleringssysteem

Een compartiment is bestemd voor het opbergen van goederen of zaken die voor inbrekers zeer attractief zijn. De beveiligingstheorie is er daarom opgericht om een inbraak in het gebouw te detecteren nog vóór het compartiment wordt bereikt of aangevallen. Het betekent dat een compartiment altijd moet worden gecombineerd met een inbraaksignaleringssysteem in het gebied buiten het compartiment. Hierbij moet de beveiliging zich uitstrekken tot alle aanvalszijden van het compartiment (dus ook vloer en plafond of dak) Als door het volume van een C2 of C3 compartiment de kans bestaat op insluiting is ruimtelijke detectie ook IN het compartiment verplicht.



5.8.2 KLUIZEN EN SAFES

Eigen gebruik Om diefstal, en met name snelkraak, te voorkomen, kunnen kleine attractieve goederen in elke situatie worden opgeborgen in een safe of kluis. Essentieel is daarbij dat ook de safe zelf wordt verankerd! Het komt niet zelden voor dat de gehele voorziening verdwijnt; de kluis of safe vormt een wel heel attractief goed op zichzelf...

Het spreekt vaak tot de verbeelding van de potentiële crimineel dat het hier een aanzienlijk bedrag aan geld betreft. Ook wanneer dit niet het geval zou zijn en zelfs wanneer dat op de safe zou staan, zal een safe vrijwel altijd boven aan zijn 'verlanglijstje' staan. Het buiten het gezichtsveld plaatsen en/of betimmeren ervan is daarom aan te bevelen.

Winkel of showroom

Bijvoorbeeld een winkel in mobiele telefonie zou als display gebruik kunnen maken van een grotere tweedehands safe, desgewenst gespoten in de bedrijfskleuren. Na sluiting gesloten betreft het vervolgens een prima compartiment. Standaard safes en kluiskasten zijn verkrijgbaar als sigarettenopslag en verkoopkasten.

Magazijn of opslag

Luxe rookwaren en aanverwante artikelen van gerenommeerde merken kunnen binnen een groter magazijn worden opgeborgen in grotere safes. Ook soms aanwezige bouwkundige kluisen kunnen als geen ander dienst doen als goed compartiment voor de berging van hoogwaardige goederen als bijvoorbeeld horloges, laptops, computeronderdelen, software et cetera.

Opmerking bij 5.8.2; dekkingsindicatie

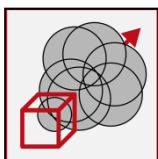
Safe: waardeberging met bescherming tegen inbraak, met een intern grond vlak van <math>< 2\text{m}^2</math> en

Kluis: waardeberging met bescherming tegen inbraak, met een intern grond vlak van >math>> 2\text{m}^2</math> die volgens de inschaling van de Vereniging Geld- en Waardeberging (VGW) geschikt is voor de op te bergen waarde. Van toepassing is: dekkingsindicatie Weerstandsklasse volgens NEN-EN 14 450 en de inbraakwering volgens NEN-EN 1143-1

Voor de berging van waardepapieren en digitale datadragers is de NEN-EN 1047-1 van toepassing.

Vrijstaande inbraakwerende kasten en safes die lichter zijn dan 1.000 kg vereisen een sterke verankering, zie voor de eisen daaraan het document van Vereniging Geld- en Waardeberging.

Voor safes en kluisen die zich binnen het ruimtelijk beveiligd gebied bevinden kan de dekkingsindicatie worden verdubbeld. Bij een safe of kluis geplaatst in een C2 of C3 compartiment kan de dekkingsindicatie worden verdrievoudigd (schillentechniek).



5.8.3 MISTGENERATOREN

Eigen gebruik Een kostbare particuliere inboedel, met daarin fraaie stukken, of een gelijke inventaris van een kantoor kunnen goed tegen snelkraak worden beschermd door middel van mist. Vooral wanneer de beveiliging van de bouwkundige schil geen uitkomst biedt en/of traliewerken om esthetische redenen niet toelaatbaar zijn. Een elektronische alarmering activeert de mistuitstoot, die tot soms wel 30 kubieke meter per seconde kan bedragen.

Winkel of showroom

Een winkel met bijvoorbeeld parfumerie, telefonie en/of ander zeer attractief kleingoed, kan met mistgeneratoren worden beveiligd. Een duidelijke zichtbare en fysieke drempel van rolluik en/of hekwerk ontbreekt hier, wat als een nadeel kan worden uitgelegd. De effectiviteit van een beveiliging met mistgeneratoren is echter groot.

Magazijn of opslag

Een apart gedeelte van een magazijn waar bijvoorbeeld de gehele voorraad elektrisch gereedschap staat opgeslagen, kan na elektronische detectie binnen de kortste keren in de mist worden gezet. De elektronische schakeling kan zo zijn opgebouwd dat pas een mistuitstoot volgt wanneer er daadwerkelijk wordt ingebroken en het detectieveld een toenadering van dit gedeelte van het magazijn 'ziet'. Duidelijk is dat het projecteren en toepassen van mistgeneratoren met veel zorg en vakkennis moet plaatsvinden. Met name omdat mist, bij de alarmopvolgers, geen verwarring mag geven met rook (brand). Zie hiervoor tevens het document D01/026 oktober 2001 versie 2: Mistgeneratoren.

6 ALARMERING

6.1 VOORGESCHIEDENIS

In de revisie van hoofdstuk 6 is een aansluiting gemaakt tussen de niveaus (AL0 t/m AL3) voor de alarmtransmissie trajecten en de indeling in ATS categorieën en Security Grades die worden gehanteerd in de Nationale en Europese normen. Afwijkingen van een norm op onderdelen zijn *curatief* weergegeven.

In het geval dat een inbraaksignaleringssysteem melding maakt van een onveilige situatie dient hiervan melding te worden gemaakt bij een ARC (particuliere alarmcentrale /PAC), van waaruit actie moet worden ondernomen. Na alarmverificatie mag de politie worden geïnformeerd.

Aangezien criminelen graag in de anonimiteit blijven proberen zij op tal van manieren te voorkomen dat zij ontdekt worden. Een van deze manieren is het saboteren van het alarmtransmissiesysteem tussen het bewaakte object en het ARC. Deze sabotage kan op een aantal punten in het gehele transmissietraject. Hierdoor moeten binnen het object maatregelen genomen worden dat bij een sabotage poging de melding hiervan altijd bij het ARC wordt gesignaleerd.

Daarnaast dient, zeker bij de hogere risico's, rekening te worden gehouden met het saboteren van de transmissiesysteem buiten het object. Om genoemde zaken te bewerkstelligen zijn functionele eisen opgesteld ten aanzien van ATS categorieën, te weten het SP1 t/m SP6 en DP1 t/m DP4.

De eisen voor deze trajecten zijn afkomstig uit de norm NEN-EN-50136-1:2012.

6.1.1 GEBRUIKTE AFKORTINGEN

In het kader van dit hoofdstuk en in de genoemde referentie documenten worden de volgende afkortingen gebruikt:

ADSL	- (Asymmetric Digital Subscriber Loop) standaard voor een digitale technologie die snellere datacommunicatie over een telefoonlijn toestaat
AL(..)	- Niveau alarmtransmissie traject
ARC	- (Alarm Receiving Centre) zie ook Particuliere Alarmcentrale / PAC
AS / AIS	- (Intruder Alarm System(s) alarmsysteem
ATK	- (Automatic phone dailer) automatische telefoonkiezer
ATP	- (Alarm Transmission Path) alarmtransmissiepad
ATS	- (Alarm Transmission System) alarmtransmissiesysteem
ATSN	- (Alarm Transmission Service Network) alarmtransmissieservicenetwerk
ATSP	- (Alarm Transmission Service Provider) alarmtransmissieserviceprovider
BAV	- Besloten alarmtransmissieverbinding
CIE	- (Control and indicatie equipment) besturings-, bedienings- en aanduidingsapparatuur (CCS)
DP(..)	- (Dual Paht) dubbelpadig alarmtransmissiesysteem
EN	- Europese Norm
GPRS	- (General Packet Radio Service) draadloos netwerk.
Grade	- (Security Grade) niveau waaraan moet worden voldaan
GSM	- (Global System for Mobile Communications) standaard voor digitale mobiele telefonie
ISDN	- (Integrated Services Digital Network) is een vorm van digitale telefonie
IP	- internetprotocol

- IPsec - (Internet Protocol Security) standaard voor het beveiligen van internetprotocol (IP) door middel van encryptie en/of authenticatie op alle IP-pakketten. IPSec ondersteunt beveiliging vanaf het 3e niveau van het OSI-model, namelijk de netwerklaag.
- IS-RA punt - Infrastructuur Randapparatuur, is het scheidingspunt tussen de apparatuur en bekabeling van de netwerkaanbieder en die van de abonnee.
- NEN - Nederlandse Norm
- NEN-EN - NEN Europese Norm
- NPR - Nederlandse Praktijk Richtlijn
- PAC - (Alarm Recieving Centre) Particuliere Alarmcentrale zie ook ARC
- Qos - (Quality of service) kwaliteit van de service geeft de mogelijkheid om de gegevensstromen in te delen naar hun belang voor de eigenaar/gebruiker, een netwerk dat QoS biedt, kan bepaald verkeer dus voorrang geven (in snelheid en/of capaciteit) boven andere applicaties.
- RCT - (Receiving Centre Transceiver) alarmontvanger in de PAC
- Shared line - Gedeelde lijnverbinding met andere gebruikers
- SP(..) - (Single Path) enkelpadig alarmtransmissiesysteem
- SPT - (Supervised Premises Transceiver) alarmoverdrager
- TN - (Transmission network) transmissienetwerk, netwerk tussen SPT en RCT
- TS - Europese Technische Specificatie
- UPS - Uninterruptible Power Supply (niet onderbreekbare voeding /noodstroomvoorziening)
- VC - Virtueel Circuit
- VoIP - (Voice over IP) hierbij wordt het internet of een ander IP-netwerk gebruikt om spraak te transporteren
- VOP - (Verification of performance) verificatie van prestaties
- VRKI - Verbeterde risicoklassen indeling

Tabel 1

Alarmtransmissie: minimaal vereiste ATS categorie						
Risicoklasse in de VRKI	Klasse 1	Klasse 2	Klasse 3	Klasse 3*	Klasse 4	Klasse 4*
Security Grade Eisen aan componenten	Grade 1 Grade 2	Grade 2 Grade 2	Grade 2 Grade 2	Grade 2 Grade 2	Grade 3 Grade 3	Grade 4 Grade 3
Woningen	SP1 (AL0) optioneel	SP2 (AL1)	SP2 (AL1)	n.v.t.	DP3 (AL2)	n.v.t.
Bedrijven	SP2 (AL1)	SP2 (AL1)	DP2 (voorheen AL1)	DP3 (AL2)	DP3 (AL2)	DP4 (AL3)

6.2 EUROPESE NORMEN

De functionele eisen zijn afgeleid van de Europese en ook in Nederland gehanteerde normen, te weten: NEN-EN 50131-1:2006/A1:2009 Alarmsystemen - Inbraak- en overvalsysteem - Deel 1: Systeemeisen. NEN-EN 50136-1:2012 en Alarmsystemen - Alarmtransmissiesystemen en -apparatuur - Deel 1: Algemene eisen voor alarmtransmissiesystemen. In deze norm staan eisen vermeld waaraan met name transmissietrajecten dienen te voldoen.

De genoemde normen geven een goed inzicht in de functionele en prestatie-eisen waaraan zowel het transmissiesysteem als de toe te passen apparatuur binnen de genoemde systemen dienen te voldoen.

In de VRKI zijn de niveaus van de elektronische maatregelen omschreven en gekoppeld aan projecteringseisen. Deze eisen in de VRKI wijken, op enkele onderdelen, af van de Europese - en Nationale regelgeving zoals vermeld in:

NEN-EN 50131-1:2006/A1:2009 Deel 1: Systeemeisen

NPR-CLC/TS 50131-7:2010, Alarmsystemen - Inbraak- en overvalsysteem - Deel 7: Richtlijnen voor de toepassing,

NEN-EN 50131-8 Mistgeneratoren, IEC 62642-8 (mistgeneratoren),

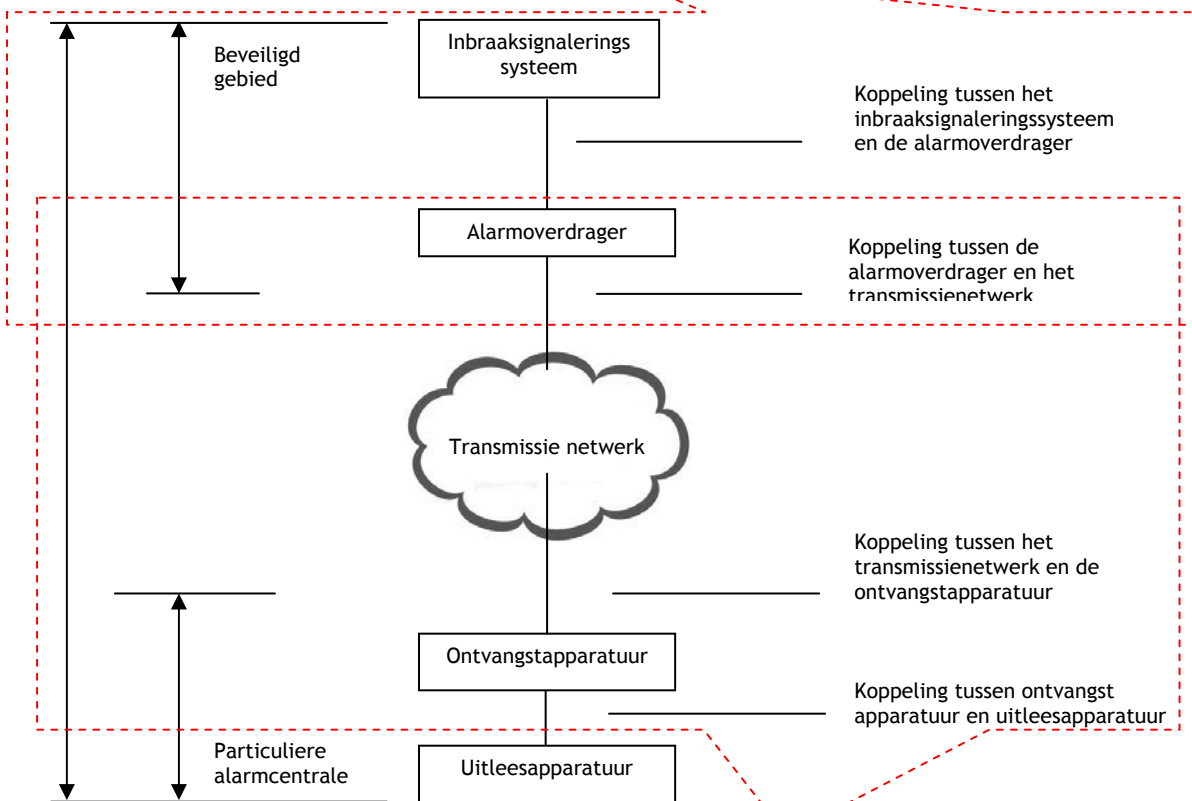
NEN-EN 50131-9 (alarmverificatie)

De brancheverenigingen hebben het initiatief genomen om tot een NEN 8131 voor alarminstallaties te komen. De ontwerpversie daarvan is op de website van NEN geplaatst en tot 1 maart 2014 kan daarop commentaar worden geleverd. Hoofdstuk 4 in dit document zal worden aangepast wanneer de definitieve versie van de NEN 8131 verschijnt.

De “Elektronische” maatregelen zullen in de NEN 8131 worden gedefinieerd op basis van Grade 1 t/m 4.

Figuur 1 schematische weergave relatie tussen de NEN-EN 50131 en NEN-EN 50136

NEN-EN 50131 van toepassing op de klantlocatie



NEN-EN 50136 van toepassing op het alarmtransmissiesysteem

In de NEN-EN 50136-1:2012 worden alleen eisen gesteld aan de alarmtransmissieapparatuur (alarmoverdrager en alarmontvanger) en aan het totale alarmtransmissiesysteem. Hoewel het transmissienetwerk een onderdeel is van een alarmtransmissiesysteem worden er geen normatieve eisen gesteld aan deze infrastructuur.

Het gebruikte transmissienetwerk kan daarom ook niet als zelfstandig onderdeel van een alarmtransmissiesysteem worden gecertificeerd.

6.3 KENMERKEN

De functionele eisen zijn vermeld in de tabel ATS klassen in de NEN-EN 50131-1:2006/A1:2009.

Het ligt de lijn van de verwachting dat deze tabel wordt vervangen door ATS categorieën.

De Europese normen NEN-EN 50131-1:2006/A1:2009 en NEN-EN 50136-1:2012 kennen t.o.v. de Nederlandse benadering een afwijkende systematiek en afwijkende prestatie-eisen.

In de NEN-EN 50131-1:2006/A1:2009 worden zes alarmtransmissieklassen gedefinieerd: ATS 1 t/m ATS 6

en in de NEN-EN 50136-1 worden tien categorieën gehanteerd: SP1 t/m SP6 en DP1 t/m DP4

SP is een enkelpadig transmissiesysteem (single path)

DP is een dubbelpadig transmissiesysteem (dual path)

De ATS categorieën die in de VRKI worden gehanteerd zijn:

Voor ATS1 (AL0) geldt: optioneel SP1

Voor ATS3 (AL1) geldt: SP2 of DP1

Voor ATS4 (voorheen bij bedrijven in klasse 3) geldt: DP2

Voor ATS5 (AL2) geldt: DP3

Voor ATS6 (AL3) geldt: DP4

Ook ander combinaties van ATS categorieën zijn toegestaan. Mits minimaal wordt voldaan aan de eisen in tabel 10 van de NEN-EN 50131-1:2006/A1:2009 en de minimale eisen in de VRKI documenten.

Het toegepaste alarmtransmissiesysteem is ook afhankelijk van de infrastructuur van de ARC.

Voor de genoemde categorieën gelden de hieronder vermelde waarden.

Tabel 2 – Specificaties ATS categorieën

	SP1	SP2	SP3	SP4	SP5	SP6	DP1	DP2	DP3	DP4
Rapportagetijd - primair ATP	32 dgn	25 h	30 min	3 min	90 s	20 s	25 u	30 min	3 min	90 s
Rapportagetijd - alternatief ATP	Op	Op	Op	Op	Op	Op	50 u	25 u	25 u	5 u
Rapportagetijd - alternatief ATP bij uitval primair ATP	Op	Op	Op	Op	Op	Op	25 u	30 min	3 min	90 s
Rapportagetijd ATS	32 dgn	25 u	30 min	3 min	90 s	20 s	50 u	60 min	6 min	3 min
Op	Optional (optie)									
dgn	dagen									

Voor de volledige tabel zie NEN-EN 50136-1:2012

6.4 AANVULLENDE BEPALINGEN

Voor de transmissiesystemen dienen maatregelen getroffen te worden ter voorkoming van het nabootsen van het transmissiesysteem in het beveiligde gebouw.

Bij SP2 en DP1 (AL1) is dit optioneel, *geadviseerd wordt hier de waarden (S1) en (I2) te hanteren. Zie artikel 6.4.1*

Bij DP2 (voorheen AL1), DP3 (AL2) en DP4 (AL3) dient dit te geschieden door: encryptie van een identiteit of een adres van alle uitgezonden signalen over het alarmtransmissiepad, Substitutie beveiliging conform NEN-EN 50131-1:2006/A1:2009 par. 8.6 tabel 11 (S2) en NEN-EN 50136-1:2012 par. 8.6.2 tabel 8 en tabel D.5 Substitution security

Ten aanzien van de informatiebeveiliging:

Conform NEN-EN 50131-1:2006/A1:2009 par. 8.6 tabel 11 (I2)

en NEN-EN 50136-1:2012 par. 6.8.3 tabel 9 en tabel D.6 Information security

6.4.1 ALARM OVER IP

Tabel 3

	Primaire verbinding T rapportagetijd	Secundaire verbinding T rapportagetijd standby	Secundaire Verbinding T rapportagetijd In bedrijf *	D	M	S	I	Beschikbaarheid ATSN	Beschikbaarheid ATS
								Op jaarbasis	Op weekbasis
SP1 (AL0)	Optioneel	n.v.t.	n.v.t.	Op	Op	Op	Op	Optioneel	Optioneel
SP2 (AL1)	T2 (25 uur)	n.v.t.	n.v.t.	Op	Op	Op	Op	Optioneel	Optioneel
DP1 (AL1)	T2 (25 uur)	T2 (50 uur)	T2 (25 uur)	Op	Op	Op	Op	Optioneel	Optioneel
DP2 (AL1)	T2 (30 min)	T2 (25 uur)	T2 (30 min)	D2	M2	S1	I2	99,5%	99,0%
DP3 9AL2)	T4 (3 min)	T2 (25 uur)	T4 (3 min)	D3	M3	S2	I3	99,9%	99,8%
DP4 (AL3)	T5 (90 sec)	T3 (5 uur)	T5 (90 sec)	D3	M3	S2	I3	99,9%	99,8%

* = indien primaire verbinding niet beschikbaar is.

Toelichting:

T = rapportagetijd conform NEN-EN 50131-1:2006/A1:2009 par. 8.6 - tabel 10 en 11 en NEN-EN 50136-1:2012 par. 6.3.3.3.1 - tabel 3

D = gemiddelde transmissietijd conform. NEN-EN 50131-1:2006/A1:2009 par. 8.6 - tabel 10 en 11 en NEN-EN 50136-1:2012 par. 6.3.2 - tabel 2
 D2 = gemiddelde transmissietijd: 60 sec. en 95% van alle transmissies: 90 sec.
 D3 = gemiddelde transmissietijd: 20 sec. en 95% van alle transmissies: 30 sec.

M = maximale transmissietijd conform. NEN-EN 50131-1:2006/A1:2009 par. 8.6 - tabel 10 en 11 en NEN-EN 50136-1:2012 par. 6.3.2 - tabel 2
 M2 = 120 sec.
 M3 = 60 sec.

S = substitutie beveiliging conform NEN-EN 50131-1:2006/A1:2009 par. 8.6 - tabel 10 en 11 en NEN-EN 50136-1:2012 par. 8.6.1 en 6.8.2 tabel 8
 S0 = geen maatregelen.
 S1 = toevoeging van een identiteit of adres aan elk via het alarmtransmissietraject verzonden bericht.
 S2 = toevoeging van encryptie van identiteit, of authenticatie door de fabrikant gespecificeerde methode.
 S3 = toevoeging van encryptie van identiteit, of authenticatie conform de in 6.8.1 (General security requirements) omschreven methode

I = informatie beveiliging conform NEN-EN 50131-1:2006/A1:2009 par. 8.6 - tabel 10 en 11 en NEN-EN 50136-1:2012 par. 6.8.3 tabel 9
 I0 = geen maatregelen.
 I2 = maatregelen ter voorkoming van ongeautoriseerde wijziging van verzonden informatie.
 I3 = maatregelen ter voorkoming van ongeautoriseerde wijziging en lezen van verzonden informatie.

Beschikbaarheid per 7 dagen en per 12 maanden van het totale alarmtransmissiesysteem conform NEN-EN 50136-1:2012 par. 6.7.5 tabel 6 (ATS availability recording) en par.6.7.6 tabel 7(ATSN availability)

Rapportagetijd:

Rapportagetijd is de tijd tussen het moment waarop een fout in het ATS optreedt en het moment waarop dit wordt gerapporteerd aan de zowel RCT/PAC als aan het AS/CCS in het beveiligde object. Voor de bewaking van het alarmtransmissiesysteem is gedefinieerd binnen welke tijd een verstoring aan het alarmtransmissiesysteem behoort te worden gerapporteerd. Het monitoren in de vorm van de end-to-end testberichten voldoet aan de desbetreffende rapportagetijden, zie tabel 3.

SP1 (ALO):

Alarmtransmissie naar een (mobiele) telefoon is één van de keuze opties. (zie artikel 6.5)

SP2 en DP1 (AL1):

Jaarlijkse beschikbaarheid voor alle actieve ATS'en (ATSN) = optioneel

Minimale wekelijkse beschikbaarheid voor elk actief ATS met betrekking tot foutlogging = optioneel

Aanbevolen wordt om voor de jaarlijkse beschikbaarheid 99,3 % en voor de wekelijkse beschikbaarheid 91,0 % als minimum te hanteren.

Substitutiebeveiliging = optioneel.

Informatiebeveiliging = optioneel

Aanbevolen wordt om substitutiebeveiliging (S1) en informatiebeveiliging (I2) toe te passen.

DP2 (voorheen bij bedrijven in risicoklasse 3: AL1):

Jaarlijkse beschikbaarheid voor alle actieve ATS'en (ATSN) = 99,5%

Minimale wekelijkse beschikbaarheid voor elk actief ATS met betrekking tot foutlogging = 99,0%

Substitutiebeveiliging = optioneel.

Informatiebeveiliging = optioneel

Aanbevolen wordt om substitutiebeveiliging (S1) en informatiebeveiliging (I2) toe te passen.

6.4.2 SECUNDAIRE TRANSMISSIEVERBINDING

Een aanvullend benodigde communicatieroute voor alarmoverdracht in het geval dat de primaire communicatieroute niet aan de prestatie-eisen kan voldoen. Gedurende de periode (stand-by) dat een secundaire communicatieroute niet in gebruik is als primaire communicatieroute, mag de rapportagetijd van de secundaire communicatieroute verschillen t.o.v. de primaire route.

6.4.3 PRESTATIENIVEAU TRANSMISSIESYSTEEM

Het prestatieniveau van het totale alarmtransmissiesysteem wordt bepaald door het component van het alarmtransmissiesysteem met het laagst (haalbare / ingestelde) prestatieniveau.

Voorbeeld: indien door toepassing van een conversieapparaat het prestatieniveau vanaf het conversieapparaat t/m de ontvangstapparatuur conform DP3 (AL2) is ingesteld en de toegepaste alarmoverdrager staat op SP2 of DP1 (AL1) ingesteld dan zal het prestatieniveau van de het totale alarmtransmissiesysteem uitkomen op SP2 of DP1 (AL1).

Noot:

Bij risicoklasse 3 voor bedrijven is DP2 van toepassing (rapportagetijd is dan 30 minuten in plaats van 25 uur). Uitval van het ATS wordt dan eerder gesignaleerd. Hiermee wordt tevens bereikt dat het grote verschil tussen de (oude AL1) met een testmelding op 24 uur en de (oude AL2) met een testmelding per 90 seconden wordt verminderd.

De oplossing die in de praktijk wordt gekozen zal afhankelijk zijn van de reeds aanwezige infrastructuur, ter plekke meest eenvoudige installatie en realisatie. Bovendien zal de oplossing afhankelijk zijn van de eenmalige en maandelijkse kosten voor de apparatuur en de netwerkaansluiting.

6.4.4 ALARMTRANSMISSIE VIA MOBIELE NETWERKEN

Ondanks het feit dat een technische oplossing op basis van een enkelvoudig transmissiepad via mobiele netwerken mogelijk is, wordt deze oplossing niet geadviseerd. Bij de keuze van de geadviseerde oplossingen is rekening gehouden met de sabotagegevoeligheid van mobiele netwerken (GSM-jammer). Voor lage risico's (SP1) risicoklasse 1 voor woningen en (SP2) in risicoklasse 2 en 3 voor woningen en risicoklasse 1 en 2 voor bedrijven is het gebruik van een GSM kiezer toegestaan.

6.4.5 VOIP / VODSL

Bij de geadviseerde oplossingen wordt expliciet nergens verwezen naar een oplossing op basis van VoIP, ADSL-routers met een POTS-poort voor internettelefonie (VoIP) en/of analoge terminal adapters. Geadviseerd wordt dan ook om deze oplossing niet toe te passen.

Telefonie via Internet Protocol. Bijvoorbeeld: InternetPlusBellen. VoDSL modems en VoIP kabelmodems zijn vaak voorzien van een aansluiting voor analoge telefonie randapparatuur. Deze aansluiting is echter niet geschikt voor analoge modems en analoge alarmkniezers! De conversie van analoge alarmmeldingen (zoals afkomstig uit traditionele analoge alarmkniezers) naar digitale IP datapakketten maakt de doormelding van alarmen onbetrouwbaar en voldoet niet aan de NEN-EN 50131-1:2006/A1:2009 en NEN-EN 50136-1:2012
Er dient bij gebruik van AoIP een IP kniezer/modem of IP converter te worden toegepast die op een Ethernetaansluiting van de router kan worden aangesloten.

6.4.6 VERIFICATIE VAN PRESTATIES

De toe te passen methoden voor verificatie van de prestaties van een ATS zijn beschreven in NEN-EN 50136-1:2012, hoofdstuk 7 Verification of Performance.
De installateur beschikt over de verificatie resultaten van de ATSP (Alarmtransmissie service provider).

Noot:

De verificatie van de prestaties van een ATS behoort te worden uitgevoerd door de ATSP. In Nederland betreft het in veel gevallen de PAC of een andere aanbieder van alarmtransmissiesystemen en/of -diensten. De verificatie van de prestaties van een ATS behoort de volgende aspecten te omvatten:
– verificatie dat het ATS functioneert conform de prestatie-eisen; hiertoe behoort het testen van de alarmdoormelding en de bewaking van het ATS;
–verificatie die nodig is om de beschikbaarheid van het ATS vast te stellen of te bevestigen.
De registraties van storingen en verificaties van prestaties van alle ATS'en en ATSN'en behoren te worden vastgelegd door de ATSP.
De registratie voor elke ATS-storing omvat:
– tijd en datum van de storing;
– tijd en datum waarop de storing is verholpen en het systeem weer normaal functioneerde.
De registraties behoren ten minste 3 jaar bewaard te blijven.

*In afwijking op de NEN-EN 50136-1 is het toegestaan bij SP1 (AL0) waarbij alarmmeldingen naar een (mobiele) telefoon worden gezonden geen verificatie van de prestaties uit te voeren.
Voor SP2 en DP1 (AL1) is het toegestaan geen verificatie van de prestaties uit te voeren. Volstaan kan worden met het bewaken van de controlemeldingen uit de CIE en/of SPT door de ARC (PAC).*

6.4.7 BESCHIKBAARHEID

De registratie van alle prestaties van een ATS en/of een ATSN behoort te worden gebruikt om de beschikbaarheid van het ATS en/of het ATSN vast te stellen.
Daarbij wordt onderscheid gemaakt tussen de beschikbaarheid van het ATSN (op jaarbasis) en elk individueel ATS (op weekbasis).
De calculatiemethoden en formules voor berekening van de beschikbaarheid zijn beschreven in NEN-EN 50136-1, 7.5.3 Calculations.
Registraties van de beschikbaarheid van elk ATS behoort op aanvraag aan de klant of installateur te worden verstrekt.

Transmissienetwerk:

Er bestaat een Nederlandse praktijkrichtlijn NPR 8136 (nl) Alarmtransmissie over IP-netwerken - Leidraad voor ontwerp, installatie, inspectie en onderhoud, gebaseerd op NEN-EN 50136-1:2012.
In deze NPR wordt melding gemaakt van criteria waaraan een besloten alarmverbinding (BAV) moet voldoen. De NEN-EN 50136-1:2012 stelt deze eis niet. In de VRKI wordt uitgegaan dat ieder netwerk kan worden gebruikt om de meldingen naar de ARC te sturen.

Opmerking: De beschikbaarheid van een ATS of ATSN de EN 50136-1:2012 dient niet verward te worden met de beschikbaarheid van een transmissienetwerk.

*In afwijking op de NEN-EN 50136-1 is het toegestaan bij SP1 (AL0) waarbij alarmmeldingen naar een (mobiele) telefoon worden gezonden geen beschikbaarheid te hoeven aantonen.
Voor SP2 en DP1 (AL1) is de verificatie van prestaties optioneel, volstaan kan worden met een overzicht van de controlemeldingen vanuit de CIE en SPT.
Indien een eisende partij stelt dat aanvullend op de NEN-EN 50136-1:2012 gebruik moet worden gemaakt van de NPR 8136 en/of de BRL K-21030 dient dit in het PVE te zijn opgenomen.*

6.4.8 VOORKEURSCHAKELING

Het alarmtransmissiesysteem dient zodanig te worden ingericht dat de alarmcommunicatie altijd voorrang heeft op de overige diensten/applicaties die gebruik maken van dezelfde netwerkaansluiting(en). Door gebruik te maken van bepaalde back-up routes voor alarmcommunicatie kan deze eis komen te vervallen tenzij de betreffende back-uproute zelf voorzien moet worden van een dergelijke voorkeurschakeling.

6.4.9 INDELING ALARMTRANSMISSIESYSTEMEN IN DE VRKI

6.4.9.1 WONINGEN ENKELPADIG ALARMTRANSMISSIESYSTEEM

Tabel 4

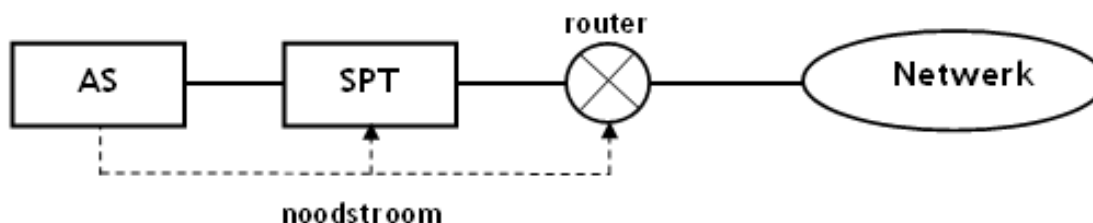
Alarmtransmissie over IP netwerken met enkelpadig alarmtransmissiesysteem voor woningen				
Risicoklasse	Klasse 1	Klasse 2	Klasse 3	Klasse 4
Security Grade Eisen aan componenten	Grade 1 Grade 2	Grade 2 Grade 2	Grade 2 Grade 2	Grade 3 Grade 3
Alarmtransmissiesysteem Prestatie-eisen conform artikel 6.4.1 t/m 6.4.8	SP1 (AL0) optioneel	SP2 (AL1)	SP2 (AL1)	<i>n.v.t.</i>
Noodstroomvoorziening netwerkcomponenten	optioneel	Ja ¹	Ja ¹	<i>n.v.t.</i>

¹ Toepassing van extra netwerkcomponenten tussen de SPT en IS-RA punt is toegestaan indien deze componenten zijn geplaatst in een beveiligde ruimte en - voor zover stroomverbruikend - zijn voorzien van een noodstroomvoorziening.
Indien een gescheiden noodstroomvoorziening wordt gebruikt voor deze componenten, behoort deze noodstroomvoorziening te worden aangesloten op dezelfde 230V eindgroep waarop de CIE is aangesloten en een uitval en een herstel van 230 V via het AS of de SPT door te melden naar een ARC. Doormelden netspanninguitval CIE binnen 2 minuten naar de ARC. *In uitzondering op artikel 9 in de NEN-EN 50131 "autonomietijd van de noodstroomvoorziening = 12 uur" mag een noodstroomvoorziening worden toegepast met een autonomietijd van minimaal 1 uur.*

Figuur 2

Schematische weergave van een ATS van categorie SP2 met noodstroomvoorziening van de router vanuit het AS.

Opmerking: de capaciteit van de accu in het AS (de CIE) dient toereikend te zijn voor een autonomietijd van minimaal 12 uur.



noot bij router:

De noodstroom geldt voor alle componenten tussen het AS en het IS-RA punt die gebruikt worden voor de alarmtransmissie, denk aan switches, omzeters glasvezel / koper etc..

Plaatsing in beveiligd gebied en een effectieve beveiliging tegen sabotage gelden ook voor alle apparatuur die voor het kunnen functioneren van de doormelding naar een ARC van belang is. alsmede voor de hierbij behorende noodstroomvoorziening(en).

De voeding voor de apparatuur van het ATS dient selectief te worden beveiligd ten opzichte van overige gebruikers die op een CIE zijn aangesloten. Voorkomen moet worden dat bij een kortsluiting in bijvoorbeeld een ruimtelijke melder of flitslicht de voeding van de apparatuur van het ATS wegvalt.

6.4.9.2 WONINGEN DUBBELPADIG ALARMTRANSMISSIESYSTEEM

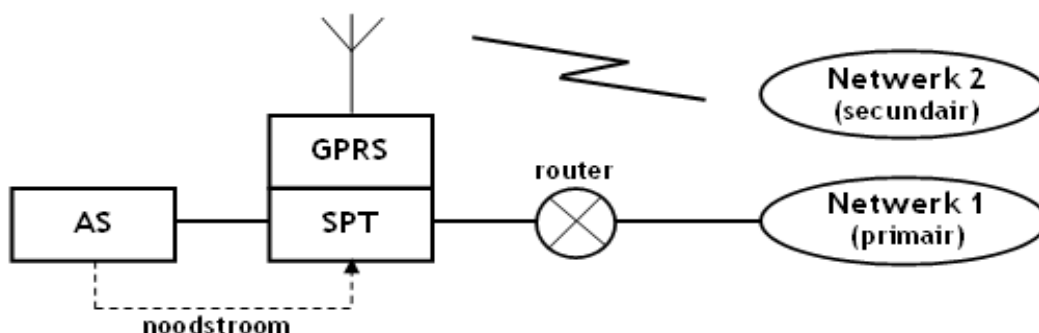
Tabel 5

Alarmtransmissie over IP netwerken met dubbelpadig alarmtransmissiesysteem voor woningen				
Risicoklasse	Klasse 1	Klasse 2	Klasse 3	Klasse 4
Security Grade Eisen aan componenten	Grade 1 Grade 2	Grade 2 Grade 2	Grade 2 Grade 2	Grade 3 Grade 3
Alarmtransmissiesysteem Prestatie-eisen conform artikel 6.4.1 t/m 6.4.8	n.v.t.	DP1 (AL1)	DP1 (AL1)	DP3 (AL2)
Noodstroomvoorziening Netwerkcomponenten voor de primaire transmissieverbinding (bijv. modem, router)	n.v.t.	Nee	Nee	Nee
Noodstroomvoorziening van de SPT voor de secundaire transmissieverbinding	n.v.t.	Ja ¹	Ja ¹	Ja ¹
¹ Voor de noodstroomvoorziening van de SPT en GPRS overdrager kan gebruik worden gemaakt van de noodstroomvoorziening van het AS. DP: Gescheiden transmissiewegen, Aanval op 1e transmissieweg leidt niet automatisch tot falen 2e transmissieweg.				

Het is tevens toegelaten het gebruik van het primaire en secundaire pad te verwisselen, bijvoorbeeld primair via GPRS en secundair via ADSL, of primair via ADSL en secundair via GPRS.

Figuur 2

Schematische weergave van een ATS van categorie DP1 en DP3 met noodstroomvoorziening van de SPT en de GPRS overdrager vanuit het AS.



noot bij de SPT en GPRS overdrager:

plaatsing in beveiligd gebied en een effectieve beveiliging tegen (sabotage) gelden ook voor alle apparatuur die voor het kunnen functioneren van de doormelding naar een ARC van belang is. Zie ook artikel 6.3.2.4 in de NPR 8136 met betrekking tot de antenne. De voeding voor de apparatuur van het ATS dient selectief te worden beveiligd ten opzichte van overige gebruikers die op een CIE zijn aangesloten. Voorkomen moet worden dat bij een kortsluiting in bijvoorbeeld een ruimtelijke melder of flitslicht de voeding van de apparatuur van het ATS wegvalt.

Opmerking: de capaciteit van de accu in het AS dient toereikend te zijn voor een autonomietijd van minimaal 12 uur.

6.4.9.3 BEDRIJVEN ENKELPADIG ALARMTRANSMISSIESYSTEEM

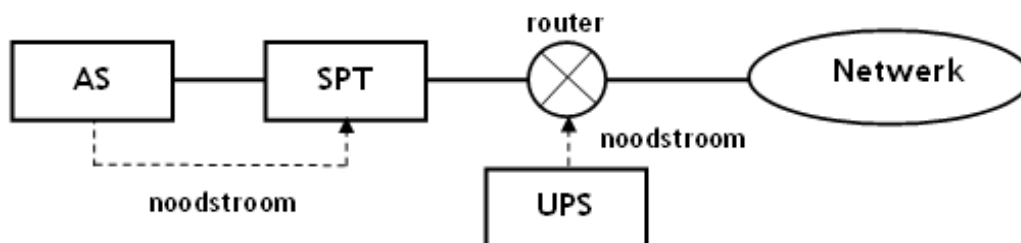
Tabel 6

Alarmtransmissie over IP netwerken met enkelpadig alarmtransmissiesysteem voor bedrijven						
Risicoklasse	Klasse 1	Klasse 2	Klasse 3	Klasse 3*	Klasse 4	Klasse 4*
Security Grade Eisen aan componenten	Grade 1 Grade 2	Grade 2 Grade 2	Grade 2 Grade 2	Grade 2 Grade 2	Grade 3 Grade 3	Grade 4 Grade 3
Alarmtransmissiesysteem Prestatie-eisen conform artikel 6.4.1 t/m 6.4.8	SP2 (AL1)	SP2 (AL1)	<i>n.v.t.</i>	<i>n.v.t.</i>	<i>n.v.t.</i>	<i>n.v.t.</i>
Noodstroomvoorziening netwerkcomponenten	<i>Ja</i> ¹	<i>Ja</i> ¹	<i>n.v.t.</i>	<i>n.v.t.</i>	<i>n.v.t.</i>	<i>n.v.t.</i>

¹ Toepassing van extra netwerkcomponenten tussen de SPT en IS/RA punt is toegestaan indien deze componenten zijn geplaatst in een beveiligde ruimte en - voor zover stroomverbruikend - zijn voorzien van een noodstroomvoorziening.
Indien een gescheiden noodstroomvoorziening wordt gebruikt voor deze componenten, behoort deze noodstroomvoorziening te worden aangesloten op dezelfde 230V eindgroep waarop het AS is aangesloten. Een uitval en een herstel van 230 V via het AS of de SPT door melden naar een ARC. Doormelden netspanninguitval van het AS binnen 2 minuten naar de ARC. *In uitzondering op artikel 9 in de NEN-EN 50131 "autonomietijd van de noodstroomvoorziening = 12 uur" mag een noodstroomvoorziening worden toegepast met een autonomietijd van minimaal 1 uur.*

Figuur 3

Schematische weergave van een ATS van categorie SP2 met noodstroomvoorziening van de router anders dan vanuit het AS.



noot bij router:

Indien mogelijk wordt de router, wanneer deze met 12 volt gelijkspanning kan worden gevoed, bijvoorkeur gevoed vanuit het AS. Als dat niet mogelijk is wordt een externe UPS toegepast.

De noodstroom geldt voor alle componenten tussen de SPT en het IS-RA punt die gebruikt worden voor de alarmtransmissie, denk aan switches, omzetter glasvezel / koper etc. plaatsing in beveiligd gebied en een effectieve beveiliging tegen sabotage gelden ook voor alle apparatuur die voor het kunnen functioneren van de doormelding naar een ARC van belang is, alsmede voor de hierbij behorende noodstroomvoorziening(en). De voeding voor de apparatuur van het ATS traject dient selectief te worden beveiligd ten opzichte van overige gebruikers die op een AS zijn aangesloten.

Voorkomen moet worden dat bij een kortsluiting in bijvoorbeeld een ruimtelijke melder of flitslicht de voeding van de apparatuur van het ATS wegvalt.

Er moeten maatregelen zijn genomen om het risico te beperken dat op de noodstroomvoorziening andere apparatuur wordt aangesloten waardoor de tijd dat de noodstroomvoorziening blijft werken niet meer aan de eis voldoet.

6.4.9.4 BEDRIJVEN DUBBELPADIG ALARMTRANSMISSIESYSTEEM

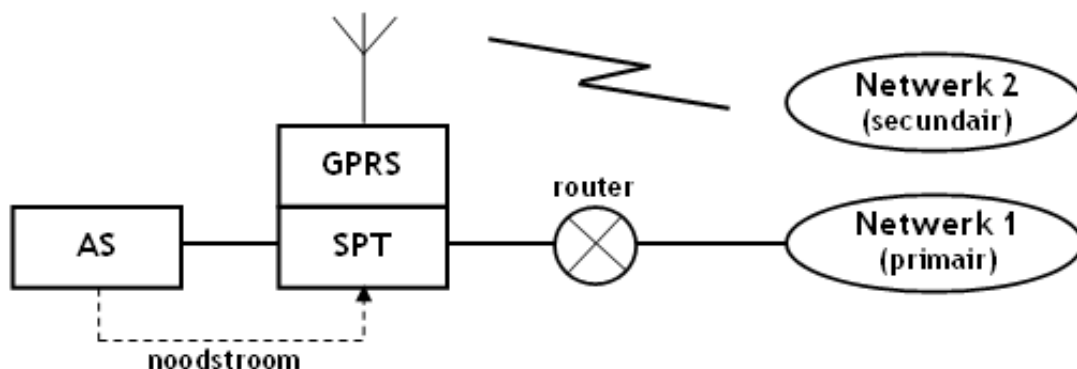
Tabel 7

Alarmtransmissie over IP netwerken met dubbelpadig alarmtransmissiesysteem voor bedrijven						
Risicoklasse	Klasse 1	Klasse 2	Klasse 3	Klasse 3*	Klasse 4	Klasse 4*
Security Grade Eisen aan componenten	Grade 1 Grade 2	Grade 2 Grade 2	Grade 2 Grade 2	Grade 2 Grade 2	Grade 3 Grade 3	Grade 4 Grade 3
Alarmtransmissiesysteem Prestatie-eisen conform artikel 6.4.1 t/m 6.4.8	DP1 (AL1)	DP1 (AL1)	DP2 (voorheen AL1)	DP3 (AL1)	DP3 (AL2)	DP4 (AL3)
Noodstroomvoorziening Netwerkcomponenten voor de primaire transmissieverbinding (bijv. modem, router)	Nee	Nee	Nee	Nee	Nee	Nee
Noodstroomvoorziening van de SPT voor de secundaire transmissieverbinding	Ja ¹	Ja ¹	Ja ¹	Ja ¹	Ja ¹	Ja ¹
¹ Voor de noodstroomvoorziening van de SPT en GPRS overdrager kan gebruik worden gemaakt van de noodstroomvoorziening van het AS. DP: Gescheiden transmissiewegen, Aanval op 1e transmissieweg leidt niet automatisch tot falen 2e transmissieweg						

Het is tevens toegelaten het gebruik van het primaire en secundaire pad te verwisselen, bijv. primair via GPRS en secundair via ADSL, of primair via ADSL en secundair via GPRS.

Figuur 4

Schematische weergave van een systeem met alarmtransmissie DP1
 In risicoklasse 3* en 4 DP3 en in risicoklasse 4* DP4



noot bij de SPT en GPRS overdrager:

Plaatsing in beveiligd gebied en een effectieve beveiliging tegen (sabotage) geldt ook voor alle apparatuur die voor het kunnen functioneren van de doormelding naar een ARC van belang is. Zie ook artikel 6.3.2.4 in de NPR 8136 met betrekking tot de antenne.

De voeding voor de apparatuur van het ATS dient selectief te worden beveiligd ten opzichte van overige gebruikers die op een CIE zijn aangesloten.

Voorkomen moet worden dat bij een kortsluiting in bijvoorbeeld een ruimtelijke melder of flitslicht de voeding van de apparatuur van het ATS wegvalt.

Voorkeurschakeling:

Indien een back-up route gebruik maakt van een shared line dan dienen aanvullende maatregelen te worden getroffen om de back-up alarmcommunicatie over deze shared line te borgen, dit kan middels een voorkeurschakeling onder controle van het alarmsysteem of overdrager of door toepassing van een beveiligde splitter welke wordt gevoed vanuit het alarmsysteem en rapporteert aan het alarmsysteem in de situatie dat er sprake is van het aanspreken van de beveiligingsfunctie m.b.t. de verstoring op de shared line. Opvolging door de ARC bij deze uitvalmeldingen dienen te worden opgevolgd conform daarover schriftelijk vastgelegde afspraken.

6.5 SP1 = OPTIONEEL (ALO) TRAJECT

Alleen van toepassing in combinatie met een alarminstallatie niveau Ed (Grade 1).

Alarmering:

Bij een alarmsituatie dient een alarm te worden gegenereerd.

Alarmering vindt plaats door middel van ten minste één van de volgende alarmeringsmogelijkheden:

1. akoestische alarmering binnen
2. akoestische alarmering buiten
3. optische alarmering
4. melding naar een (mobiele) telefoon

ISDN

Bij ISDN - aansluitingen vervalt bij niveau Ed de eis een voorkeurschakeling toe te passen voor de alarmoverdrager.

6.6 SP2 EN DP1 (AL1) TRAJECT

Bij een alarmsituatie dient binnen het gebouw een akoestisch alarm te worden gegenereerd, *alsmede een optische alarmering* die goed zichtbaar is vanaf de openbare weg.

Akoestische alarmgevers binnen, moeten zodanig zijn geplaatst dat binnen het beveiligde gebied het geluid ervan duidelijk is waar te nemen. *Met duidelijk wordt bedoeld een minimale geluidssterkte van 60 dB(A) gemeten ter plaatse waar zich de attractieve goederen normaliter bevinden.*

Dit is ook van toepassing op een sabotagealarm als het alarmsysteem in de in-fase staat. Bij sabotage van een luid-alarmgever dient minimaal *een tweede alarmgever te blijven functioneren.* (tenzij alarmgevers gelijktijdig worden gesaboteerd) het voorgaande is ook van toepassing bij deel-inschakeling van het alarmsysteem. *In de praktijk betekent dit dat er minimaal 2 luid-alarmgevers moeten zijn geïnstalleerd* waarvan deze ieder op een apart gezeekerde sirene-uitgang van het AS of uitbreidings-unit moeten zijn aangesloten. Het kortsluiten of onderbreken van een kabel naar een alarmgever mag dus niet leiden tot uitval van de tweede alarmgever.

Als een beveiligd object bestaat uit meerdere gebouwen is deze eis voor ieder afzonderlijk bouwdeel van toepassing. De eis is niet van toepassing in woningen in risicoklasse 1, 2 en 3, en bedrijven in klasse 1. Hier kan worden volstaan met één luid-alarmgever.

Met betrekking tot de alarmering dient voor het versturen van de alarmmelding de ATS categorie SP2 of DP1 te worden toegepast (AL1 traject). De alarmoverdracht dient te geschieden naar een door het ministerie van Justitie toegelaten ARC (particuliere alarmcentrale) Minimaal één keer per 24 uur dient ook een controlemelding vanuit de CIE plaats te vinden.

Aanvullend vereist bij gebruik IP met enkelvoudige verbinding

Bij gebruik van een UPS voor de router deze aansluiten op dezelfde 230V eindgroep waarop de CIE is aangesloten. Doormelden netspanninguitval/-herstel CIE binnen 2 minuten naar de ARC.

In uitzondering op artikel 9 in de NEN-EN 50131 "autonomietijd van de noodstroomvoorziening = 12 uur" mag een noodstroomvoorziening worden toegepast met een autonomietijd van minimaal 1 uur.

Actiepatroon ARC

Uitval van de CIE, de primaire verbinding, de secundaire verbinding en uitval van beide paden behoren te worden geconstateerd door de ARC (PAC) Opvolging door de ARC bij deze uitvalmeldingen dient te worden opgevolgd conform daarover schriftelijk vastgelegde afspraken. Zie ook artikel 6.4.7

6.7 DP2 (VOORHEEN AL1) TRAJECT

Zie voor de eisen aan de akoestische- en optische alarmgevers en voor de eisen voor het actiepatroon door de ARC bij uitval van de CIE en het ATS artikel 6.6

Met betrekking tot de alarmering dient voor het versturen van de alarmmelding een systeem te worden toegepast van de categorie DP2 (voorheen AL1). De alarmoverdracht dient te geschieden naar een door het ministerie van Justitie toegelaten ARC (particuliere alarmcentrale)
Minimaal één keer per 24 uur dient ook een controlemelding vanuit de CIE plaats te vinden.

6.8 DP3 (AL2) TRAJECT

Zie voor de eisen aan de akoestische- en optische alarmgevers en voor de eisen voor het actiepatroon door de ARC bij uitval van de CIE en het ATS artikel 6.6

Met betrekking tot de alarmering dient voor het versturen van de alarmmelding een systeem te worden toegepast van de categorie DP3 (AL2). De alarmoverdracht dient te geschieden naar een door het ministerie van Justitie toegelaten ARC (particuliere alarmcentrale)
Minimaal één keer per 24 uur dient ook een controlemelding vanuit de CIE plaats te vinden.

6.9 DP4 (AL3) TRAJECT

Zie voor de eisen aan de akoestische- en optische alarmgevers en voor de eisen voor het actiepatroon door de ARC bij uitval van de CIE en het ATS artikel 6.6

Met betrekking tot de alarmering dient voor het versturen van de alarmmelding een systeem te worden toegepast van de categorie DP4 (AL3). De alarmoverdracht dient te geschieden naar een door het ministerie van Justitie toegelaten ARC (particuliere alarmcentrale)
Minimaal één keer per 24 uur dient ook een controlemelding vanuit de CIE plaats te vinden.

Indeling in Grade ten aanzien van de eisen aan de alarmapparatuur

Bij het omzetten van de classificaties naar Europese standaarden: Grade 1 t/m Grade 4 moeten we ons de vraag stellen aan welke eisen de alarmapparatuur moet voldoen.

Een installatie conform Grade 1 moet ook worden uitgevoerd met gecertificeerde componenten.

Aangezien er vrijwel geen componenten volgens Grade 1 zijn gecertificeerd zal in de praktijk voor Grade 1 systemen de componenten worden toegepast conform Grade 2. Bij een eventuele wijziging van een (sub) systeem van Grade 1 naar Grade 2 voldoen daarmee de componenten al aan de eisen.

Een installatie conform Grade 2 moet worden opgebouwd uit componenten die gecertificeerd zijn conform Grade 2

Een installatie conform Grade 3 moeten worden opgebouwd uit componenten die gecertificeerd zijn conform Grade 3

Een installatie conform Grade 4 mogen worden opgebouwd uit componenten die gecertificeerd zijn conform Grade 3

In de huidige systematiek waar componenten worden weergegeven op lijsten van REQ / NCP en CertAlarm komen onvoldoende componenten voor die volgens Grade 4 zijn gecertificeerd soms wordt de Grade niet eens vermeld.

Grade 4 componenten zijn niet altijd beschikbaar (je kunt dus geen alarminstallatie ontwerpen met uitsluitend Grade 4 componenten), vandaar dat we uitgaan voor de eisen aan de alarmapparatuur van Grade 3.

6.10 TIPS OM NODELOOS ALARM TE VOORKOMEN

De meeste meldingen van alarminstallaties zijn nodeloos. In veel gevallen zijn bedieningsfouten daarvan de oorzaak. Nodeloos alarm geeft de politie handenvol werk. Met wat meer aandacht van de gebruiker is het mogelijk om hieraan iets te doen.

6.10.1 BIJ AANSCHAF

- Laat de installatie aanleggen door een installateur die voldoet aan de in de Wpbr gestelde eisen. Deze bedrijven werken volgens de installatievoorschriften voor alarmapparatuur.
- Let op de gebruikersvriendelijkheid: van belang is dat een bedieningsmogelijkheid wordt gebruikt die voor de omgeving, de situatie en de personen die deze moeten bedienen, het meest geschikt is.

6.10.2 NIEUWE ALARMINSTALLATIE IN GEBRUIK NEMEN

- Stel een oefenperiode in om met de nieuwe installatie te leren omgaan. Maak hierover een afspraak met de installateur en de alarmcentrale. Ga pas daarna op een definitieve aansluiting over.
- Houdt het aantal mensen dat de installatie kan in- en uitschakelen zo klein mogelijk. Zorg dat ze goed geïnstrueerd zijn.

6.10.3 TOCH NODELOOS ALARM?

Waarschuw onmiddellijk de alarmcentrale als u per ongeluk een alarm veroorzaakt. De centrale kan een doormelding aan de alarmopvolger dan wellicht nog voorkomen.

6.10.4 VOORKOM NODELOOS ALARM

- Maak met de alarmcentrale een afspraak over de manier waarop u hen bericht als u een fout maakt bij het in - of uitschakelen.
- Heeft u het telefoonnummer van de alarmcentrale bij de hand?
- Laat de installatie nazien als de oorzaak van een nodeloos alarm niet bekend is. Soms kan een kleine technische verandering herhaling voorkomen.
- Zorg dat iedereen die de installatie in - en uitschakelt ook weet wat er moet gebeuren, als hierbij een alarm wordt veroorzaakt.
- Maak voor het inschakelen altijd een afsluitronde. Overtuig u ervan dat alle ramen en deuren gesloten zijn. En denk aan eventuele huisdieren.
- Geef aan de alarmcentrale voldoende waarschuwadressen op. Controleer regelmatig of deze opgave van personen en hun telefoonnummers nog correct is.

7 REACTIE (ALARMOPVOLGING)

Alle elektronische maatregelen ten spijt, als de alarmopvolging faalt is het doel niet bereikt.

7.1 INDELING IN NIVEAUS

In de tabellen van de beveiligingsklasse voor woningen en bedrijven worden de vereiste procedures aangeduid met R0, R1, R1 of R3.

7.2 R0 NIVEAU

Alleen van toepassing bij een alarminstallatie van niveau Ed voor woningen.

In deze situatie kan de alarmering door het alarmsysteem gemeld worden naar een mobiele telefoon (spraak of sms bericht). Voor een adequate alarmopvolging is het belangrijk dat deze mobiele telefoon bereikbaar is. Er is geen garantie of controle of de melding tijdig de alarmopvolger bereikt. Ook kan de melding in een voice-mail terechtkomen. Alarmmeldingen van het niveau Ed mogen ook naar een servicecentrale (niet zijnde een PAC) worden doorgemeld. De alarmopvolging kan geschieden door persoonlijke verificatie door de eigenaar of sleutelhouder(s). Bij enkel luid- en/of optische alarmering geschiedt de opvolging door de bewoner, burens of passanten die reageren op de luid- en/of optische alarmgevers.

7.3 R1 NIVEAU

Reactie alarmopvolging: alarmopvolging door sleutelhouder(s) die door de PAC worden gebeld.

Bij de PAC dienen minimaal 2 sleutelhouders te zijn opgegeven. Bij een alarmmelding, waarbij alarmverificatie met technische middelen ontbreekt of leidt tot een negatieve verificatie, wordt de sleutelhouder gebeld. Het is dus belangrijk dat sleutelhouders bereikbaar zijn (gegevens actueel houden) en in staat om eerst persoonlijk te verifiëren of de alarmmelding niet nodeloos is.

De sleutelhouder dient bij mogelijk vermoeden ter plaatse dat het inbraakalarm door een criminele handeling is veroorzaakt de PAC daarvan op de hoogte te stellen of zelf 112 te bellen. Uitgangspunt is alarmopvolging binnen maximaal 20 minuten.

7.4 R2 NIVEAU

Reactie alarmopvolging: procedure als bij R1 met de aanvulling dat voor de alarmopvolging een contract dient te zijn gesloten met een door het ministerie van Justitie erkend particulier beveiligingsbedrijf, dat onder meer als sleutelhouder kan fungeren.

Sleutelhouder(s) dienen wel bij de PAC te blijven geregistreerd voor terugkoppeling bij calamiteiten. Uitgangspunt is alarmopvolging binnen maximaal 15 minuten. Voor woningen kan bij R2 ook worden gekozen voor R1 + technische alarmverificatie waarmee in plaats van alarmopvolging door een particuliere bewakingsdienst, alarmopvolging door een sleutelhouder samen met prioriteit 1 door de politie kan worden bereikt.

7.5 R3 NIVEAU

Reactie alarmopvolging: procedure als bij R2 (dus opvolging door een particulier beveiligingsbedrijf)

Minimaal dient ook één van de drie technische alarmverificatie mogelijkheden operationeel te zijn. Uitgangspunt is opvolgingstijd van maximaal 15 minuten door de bewakingsdienst en een prioriteit 1 van de politie. (15 minuten, na technisch alarmverificatie)
Indien niet haalbaar dan dient de vertragingstijd gelijkwaardig verhoogd te worden.
Sleutelhouder(s) dienen wel bij de PAC te blijven geregistreerd voor terugkoppeling bij calamiteiten.

7.6 ALARMVERIFICATIE

Op dit moment is het onderwerp alarmverificatie in een ontwikkelingsstadium. Een tekst voor dit onderdeel wordt nader ingevuld. Zie voor meer informatie de vigerende versie van Advies Projectering Alarmverificatie van de VvBO (<http://www.hetccv.nl/dossiers/Risicoklassenindeling/advies-projectering-alarmverificatie?reference=dossiers/Risicoklassenindeling/index/index>).

7.7 ALARMVERIFICATIE METHODEN

- 7.7.1 inkijken
- 7.7.2 inluisteren
- 7.7.3 dubbele zone
- 7.7.4 persoonlijke verificatie

BIJLAGE 1 Modelformulier Programma van Eisen (PvE) informatief

1: gegevens	
Projectnummer	:
Datum opmaak	:
Beveiligingsbedrijf Adres / Plaats Telefoonnummer	: : :
PvE ingevuld door	: naam:.....
Aanduiding object	: <input type="checkbox"/> woning <input type="checkbox"/> bedrijf <input type="checkbox"/> winkel / showroom <input type="checkbox"/> magazijn/opslag : <input type="checkbox"/> school lager onderwijs <input type="checkbox"/> school middelbaar en hoger onderwijs.
Bewoner / eigenaar / beheerder Adres / Plaats Telefoonnummer	: : :
Eisende partij(en)	: <input type="checkbox"/> bewoner / eigenaar / beheerder : <input type="checkbox"/> verzekeraar : <input type="checkbox"/> anders namelijk:
<input type="checkbox"/> Woningen	: <input type="checkbox"/> verzekerde waarde attractieve zaken €
Doel van de beveiliging: <input type="checkbox"/> inbraak en diefstalbev. <input type="checkbox"/> brandbeveiliging <input type="checkbox"/> informatiebeveiliging. <input type="checkbox"/> overvalbeveiliging <input type="checkbox"/> toegangsbeveiliging <input type="checkbox"/>	: <input type="checkbox"/> bedrijven : attractiviteit goederen, bedrijfsuitrusting/inventaris : <input type="checkbox"/> Laag verzekerde waarde €..... : <input type="checkbox"/> Midden verzekerde waarde €..... : <input type="checkbox"/> Hoog verzekerde waarde € : <input type="checkbox"/> Zeer Hoog verzekerde waarde € : <input type="checkbox"/> Meewegen immateriële zaken <input type="checkbox"/> ja <input type="checkbox"/> n.v.t.
Geconstateerde risicoklasse:	conform document D03-375 of D03-376 versies maart 2014 <input type="checkbox"/> klasse 1 <input type="checkbox"/> klasse 2 <input type="checkbox"/> klasse 3 <input type="checkbox"/> klasse 3* <input type="checkbox"/> klasse 4 <input type="checkbox"/> klasse 4*
Gekozen combinatie van Beveiligingsmaatregelen <input type="checkbox"/> Noot: bij onderwijsinstellingen de O, B, C/M en E maatregelen conform de richtlijn.	conform Definities beveiligingsmaatregelen document D03-385 maart 2014 : <input type="checkbox"/> O1 <input type="checkbox"/> O2 Organisatorische maatregelen : <input type="checkbox"/> BO <input type="checkbox"/> B1 <input type="checkbox"/> B2 <input type="checkbox"/> B3 Bouwkundige maatregelen : <input type="checkbox"/> C/M1 <input type="checkbox"/> C/M2 <input type="checkbox"/> C/M3 Meeneembeperkende maatregelen : <input type="checkbox"/> Ed <input type="checkbox"/> E1 <input type="checkbox"/> E2 <input type="checkbox"/> E3 Elektronische maatregelen : <input type="checkbox"/> SP1 <input type="checkbox"/> SP2 <input type="checkbox"/> DP1 <input type="checkbox"/> DP2 <input type="checkbox"/> DP3 <input type="checkbox"/> DP4 Alarmtransmissie : <input type="checkbox"/> R0 <input type="checkbox"/> R1 <input type="checkbox"/> R2 <input type="checkbox"/> R3 Reactie alarmopvolging : <input type="checkbox"/> video <input type="checkbox"/> audio <input type="checkbox"/> meerdere zones Alarmverificatie : <input type="checkbox"/> persoonlijke verificatie sleutelhouder <input type="checkbox"/> bewakingsdienst
Onderhoud	: <input type="checkbox"/> contract voor onderhoud maal per jaar <input type="checkbox"/> geen
Op te leveren met kwaliteitsdocument	: <input type="checkbox"/> Beveiligingscertificaat : <input type="checkbox"/> Opleveringsbewijs alarminstallatie : <input type="checkbox"/> Opleveringsbewijs bouwkundige beveiliging : <input type="checkbox"/> anders: : <input type="checkbox"/> geen
Maatwerk / afwijkingen:	: Toelichting: in een bijlage <input type="checkbox"/> ja <input type="checkbox"/> n.v.t : projectnummer vermelden

2: autorisatie			
Bewoner /eigenaar / beheerder	naam..... telefoonnummer.....	datum	handtekening
Verzekeraar bij klasse 4 verplichte handtekening	Verzekeraar:..... naam:..... telefoonnummer	datum	handtekening
Beveiligingsbedrijf	naam:..... telefoonnummer	datum	handtekening
Gehanteerde versienummers van referentiedocumenten			
<input type="checkbox"/> NBRL BORG Beveiligingsbedrijf <input type="checkbox"/> VEB 3 kwaliteitsregeling <input type="checkbox"/> Richtlijn inbraakbeveiliging onderwijsinstellingen, document 002754 <input type="checkbox"/> VRKI: Risicoklassenindeling voor woningen, document D03-375, <input type="checkbox"/> VRKI: Risicoklassenindeling voor bedrijven, document D03-376, <input type="checkbox"/> VRKI: Definities beveiligingsmaatregelen, document D03-385, <input type="checkbox"/> Installatievoorschriften alarmapparatuur, document. 002080, <input type="checkbox"/> Voorschriften beheer en onderhoud alarmapparatuur,document 002079, <input type="checkbox"/> Protocol stil overval alarm Projectteam Overvalcriminaliteit, doc. Pto, <input type="checkbox"/> Veiligheid verzekerd. Uitgave van Vereniging Gelden en Waardeberging <input type="checkbox"/> Installatievoorschriften rolluiken, rolhekken en schaarhekken, doc. 002757 <input type="checkbox"/> Inbraakwerende beglazing, document D03-394 <input type="checkbox"/> Installatievoorschriften Mistgeneratoren, document D01-026 <input type="checkbox"/> Beveiligingsrichtlijn bestaande bouw <input type="checkbox"/> Productenlijst bestaande bouw <input type="checkbox"/> NEN-EN 1726 Inbraakwerendheid eisen en classificatie <input type="checkbox"/> Leveringsvoorwaarden van de leverancier <input type="checkbox"/> Onderhoud- en servicecontract van de leverancier <input type="checkbox"/> <input type="checkbox"/>		Oktober 2010 November 2010 Versie maart 2014 Versie maart 2104 Versie maart 2014 Versie maart 2014 Juli 2000 v2 Juli 2000 v2 September 1997 v2 c 2005 Augustus 2001 v2 September 2003 v2 Oktober 2001v2 Versie februari 2013 Versie september 2013 Versie mei 2011 Versie:..... Versie:..... Versie:..... Versie:.....	

Indien van toepassing:

Bijlage bij projectnummer:

BIJLAGE 2 Het belang van certificatie (INFORMATIEF)

Wat is een certificaat? Er zijn vele definities. Vanuit het toepassingsgebied van de VRKI sluit de volgende definitie het beste aan.

Een certificaat is “een verklaring die is opgemaakt om tot bewijs te dienen”.

Consumenten en overheden of andere partijen zoals verzekeraars zijn zich in toenemende mate bewust van de gevaren voor veiligheid en gezondheid. Maar de kwaliteit van een geleverd product of dienst is een vanzelfsprekendheid die helaas niet altijd aanwezig is. Het betekent dat een behoefte aanwezig is dat oorsprong, inhoud, productieprocessen en/of product dienst aantoonbaar moet voldoen aan de gestelde eisen. Een certificatie-instelling kan op basis van deskundigheid en onafhankelijkheid invulling geven aan de aantoonbaarheid hiervan.

Er zijn meerdere vormen van certificaten, met verschillende benamingen (certificatieschema, (erkenning)regeling, beoordelingsrichtlijn.

Een certificatie-instelling kan verklaren dat het (kwaliteit)managementsysteem van een bedrijf voldoet aan gestelde eisen. Hierdoor komt een bepaalde mate van vertrouwen tot stand dat het te leveren product of dienst aan de gestelde eisen zal voldoen.

Aan andere vorm is meer gericht op de kwaliteit van het product of dienst. Hierbij zijn o.a. aan de orde:

- product of dienst wordt periodiek gecontroleerd,
- het kwaliteitssysteem wordt veelal eveneens gecontroleerd, hierbij zijn vaak eisen over de vakbekwaamheid van het personeel opgenomen,
- er is sprake van een keurmerk, aangebracht op het product zelf, of op het document verbonden aan de levering. Dit document wordt vaak certificaat genoemd, en wordt door de leverancier opgesteld.

Bij de uitwerking hoe certificatie uitgevoerd wordt, worden vele keuzes gemaakt. Hierbij ontstaat dan ook variatie in de waarde van het certificaat.

Er zijn hierbij twee belangrijke elementen aan de orde:

1. certificatie wordt ingericht op basis van (accreditatie)normen. Deze normen geven niet alleen richting aan de deskundigheid en onafhankelijkheid van de certificatie-instelling, maar ook aan een heldere en transparante inrichting van de te stellen eisen, en de wijze waarop deze beoordeeld wordt. Hiermee wordt het mogelijk dat de Raad voor Accreditatie beoordeeld of de certificatie-instelling zich aan de kwaliteitseisen houdt. De Raad voor Accreditatie is dan de “de certificeerder van de certificeerder”.
2. Het certificatieschema wordt beheerd door een onafhankelijke beheerder. Hierbij is dan tevens een structuur aanwezig waarbij de belanghebbende partijen inbreng hebben, met draagvlak.

Het CCV, als beheerder van de VRKI, heeft zich ingericht als schemabeheerder voor BORG 2005, en het beleid is uitvoering onder accreditatie.

Bij certificering van beveiligingsmaatregelen, gebaseerd op de VRKI, wordt een onderscheid gemaakt tussen:

- Het beveiligingscertificaat.
Het certificaat zegt niet alleen iets over de kwaliteit van de toegepaste componenten en de manier waarop ze zijn verwerkt, maar vooral ook iets over de samenhang en het beveiligend vermogen ervan, op het niveau van de risicoklasse voortvloeiend uit het gebruik van de VRKI.
- Het opleveringsbewijs.
Het opleveringsbewijs wordt uitgegeven als er sprake is van een gedeeltelijke uitvoering van de beveiligingsmaatregelen, of als er sprake is van realisatie op een lagere risicoklasse.

Zowel het beveiligingscertificaat als het opleveringsbewijs dienen ondubbelzinnig aan te geven op welk niveau de maatregelen (B+C/M+E+AL+O+R) zijn gerealiseerd.

Verschillen tussen BORG certificering en de VEB regeling zijn o.a.:

	BORG 2005	VEB 3.0
Beheer	het CCV	VEB
Uitvoering	Meerdere certificatie-instellingen	VEB i.s.m. inspectie-instelling
Accreditatie	Nog niet mogelijk	Niet mogelijk
Structuur belanghebbende partijen	Commissie van Belanghebbenden Criminaliteitspreventie van het CCV	Niet
Bedoeld voor	Beveiligingsbedrijven	VEB leden
Kwaliteitsaspect	Gericht op aantonen van kwaliteit	Gericht op kwaliteitsbevordering
Eisen aan certificaten en opleveringsbewijzen	Volgens artikel 3.6, 3.7, 4.2.9, 4.4 en 5.5 van het BORG-certificatieschema	Volgens artikel 7 f van de VEB-regeling 3.0
Sancties	Op accreditatieniveau	Beperkt
Steekproefinspecties	Gedefinieerd	Gedefinieerd, vrijstelling bij BORG erkenning

BIJLAGE 3 Verwijzingen die direct of indirect verbonden zijn aan de VRKI (INFORMATIEF)

Wettelijk kader:	
Wpbr 15 december 2011	Wet Particuliere beveiligingsorganisaties en recherchebureaus
Rpbr 27 juli 2011	Regeling Particuliere beveiligingsorganisaties en recherchebureaus
Wbp 9 februari 2012	Wet bescherming persoonsgegevens
Certificatie en Accreditatie:	
ISO IEC 17020-A	Algemene criteria voor het functioneren van verschillende soorten instellingen die keuringen uitvoeren
NEN-EN-ISO/IEC 17020:2012 en	Conformiteitsbeoordeling - Algemene criteria voor het functioneren van verschillende soorten instellingen die keuringen uitvoeren
NEN-EN-ISO/IEC 17025:2005	Algemene eisen voor de competentie van beproevings- en kalibratielaboratoria
NEN-EN 45011:1998	Algemene eisen voor instellingen die productcertificatie-systemen uitvoeren
NEN-EN-ISO/IEC 17021:2006	Conformiteitsbeoordeling - Eisen voor instellingen die audits en certificatie van managementsystemen uitvoeren
NEN-EN-ISO/IEC 17021:2011 en	Conformiteitsbeoordeling - Eisen voor instellingen die audits en certificatie van managementsystemen uitvoeren
NEN-EN-ISO 9001:2008+C1:2009 nl	Kwaliteitsmanagementsystemen - Eisen
Waardeberging:	
NEN-EN 14450:2005	Waardeberging - Eisen, classificatie en beproevingsmethoden voor weerstand tegen inbraak - Inbraakwerende kasten
NEN-EN 1143-1:2005+A1:2009	Waardeberging - Eisen, classificatie en beproevingsmethoden van de weerstand tegen inbraak - Deel 1: Safes, geldautomaatkluisen, kluisdeuren en kluisen
NEN-EN 1143-1:2012 en	Waardeberging - Eisen, classificatie en beproevingsmethoden van de weerstand tegen inbraak - Deel 1: Safes, geldautomaatkluisen, kluisdeuren en kluisen
NEN-EN 1047-1:2005	Waardeberging - Eisen en beproevingsmethoden voor de brandwerendheid - Deel 1: Brandwerende kasten en disketteverpakkingen
Elektronische maatregelen:	
NPR 8136: 2012	Is op 1-5-2012 gepubliceerd door NEN. In deze NPR 8136 wordt verwezen naar de normenreeksen NEN-EN 50131 en NEN-EN 50136
NEN-EN 50131-1:2006/A1:2009 en	Alarmsystemen - Inbraak- en overvalsysteem - Deel 1: Systeemeisen
NEN-EN 50131-2-2:2008 en	Alarmsystemen - Inbraakalarmsystemen - Deel 2-2: Inbraakdetectoren - Passieve infrarood detectoren
NEN-EN 50131-2-3:2008 en	Alarmsystemen - Inbraakalarmsystemen - Deel 2-3: Eisen voor microgolfdetectoren
NEN-EN 50131-2-4:2008 en	Alarmsystemen - Inbraakalarmsystemen - Deel 2-5: Eisen voor gecombineerde passieve infrarood- en ultrasone detectoren
NEN-EN 50131-2-5:2008 en	Alarmsystemen - Inbraakalarmsystemen - Deel 2-5: Eisen voor gecombineerde passieve infrarood- en ultrasone detectoren
NEN-EN 50131-2-6:2008 en	Alarmsystemen - Inbraakalarmsystemen - Deel 2-6: Openingsmelders (magneetcontacten)
NPR-CLC/TS 50131-2-7-1:2009 en	Alarmsystemen - Inbraakalarmsystemen - Deel 2-7-1: Inbraakdetectoren - Glasbreukdetectoren (akoestisch)
NPR-CLC/TS 50131-2-7-2:2009 en	Alarmsystemen - Inbraakalarmsystemen - Deel 2-7-2: Inbraakdetectoren - Glasbreukdetectoren (passief)
NPR-CLC/TS 50131-2-7-3:2009 en	Alarmsystemen - Inbraakalarmsystemen - Deel 2-7-3: Inbraakdetectoren - Glasbreukdetectoren (actief)

NEN-EN 50131-2-2: 2008 en	Alarmsystemen - Inbraakalarmssystemen - Deel 2-2: Inbraakdetectoren - Passieve infrarood detectoren
NPR-CLC/TS 50131-2-8: 2012 en	Alarmsystemen - Inbraak- en overvalsystemen - Deel 2-8: Inbraakdetectoren - Schokdetectoren
NEN-EN 50131-3: 2009 en	Alarmsystemen - Inbraak- en overvalsystemen - Deel 3: Bedienings- en aanduidingsapparatuur
NEN-EN 50131-4: 2009 en	Alarmsystemen - Inbraakalarmssystemen - Deel 4: Waarschuwingsapparatuur
NEN-EN 50131-5-3: 2005 en	Alarmsystemen - Inbraakalarmssystemen - Deel 5-3: Eisen voor interconnectiesystemen met gebruik van RF-technieken
NEN-EN 50131-6: 2008 en	Alarmsystemen - Inbraakalarmssystemen - Deel 6: Voedingseenheden
NPR-CLC/TS 50131-7: 2010 en	Alarmsystemen - Inbraak- en overvalsystemen - Deel 7: Richtlijnen voor de toepassing
NEN-EN 50131-8: 2009 en	Alarmsystemen - Inbraakalarmssystemen - Deel 8: Mistgeneratoren voor inbraakbeveiliging
NEN-EN 50131-9: 2010 en	Ontw.Alarmsystemen - Inbraak- en overvalsystemen - Deel 9: Alarm verificatie - Methoden en principes (nog uitwerken in hoofdstuk 7.7)
NEN-EN 50131-10: 2011 Ontw. en	Alarmsystemen - Inbraak- en overvalsystemen - Deel 10: Toepassing specifieke eisen voor alarmoverdragers
NEN-EN 50134-5: 2004 en	Alarmsystemen - Sociale alarmsystemen - Deel 5: Verbindingen en communicaties
NPR-CLC/TS 50134-7: 2004 en	Alarmsystemen - Sociale alarmsystemen - Deel 7: Richtlijnen voor de toepassing
NEN-EN 50136-1: 2012 en	Alarmsystemen - Alarmtransmissiesystemen en -apparatuur - Deel 1: Algemene eisen voor alarmtransmissiesystemen
NEN-EN 50136-2-1: 1998/C1:1998/A1:2001 en	Alarmsystemen - Alarmtransmissiesystemen en -apparatuur - Deel 2-1: Algemene eisen voor alarmtransmissieapparatuur
NEN-EN 50136-2-2: 1998 en	Alarmsystemen - Alarmtransmissiesystemen en -apparatuur - Deel 2-2: Eisen voor apparatuur gebruikt in systemen die gebruik maken van vaste alarmverbindingen
NEN-EN 50136-2-3: 1998 en	Alarmsystemen - Alarmtransmissiesystemen en -apparatuur - Deel 2-3: Eisen voor apparatuur gebruikt in systemen met overdrachtseenheden die digitale signalen doorgeven via het openbare telefoonnetwerk
NEN-EN 50136-2-4: 1998 en	Alarmsystemen - Alarmtransmissiesystemen en -apparatuur - Deel 2-4: Eisen voor apparatuur gebruikt in systemen met overdrachtseenheden die gesproken berichten doorgeven via het openbare telefoonnetwerk
NEN-EN 50518-3: 2011 en	Monitoring en alarmontvangstcentrales - Deel 3: Procedures en eisen voor de werking
Voorschriften (Nationaal):	
Document D01-026	Installatievoorschriften mistgeneratoren
Document D03-375	Verbeterderde Risicoklassenindeling voor woningen
Document D03-376	Verbeterderde Risicoklassenindeling voor bedrijven
Document D03-385	Verbeterderde Risicoklassenindeling Definities beveiligingsmaatregelen
Document 002754	Richtlijn inbraakbeveiliging onderwijsinstellingen
Document D03-394	Inbraakwerende beglazing
Document 002079	Voorschriften beheer en onderhoud alarmapparatuur
Document 002080	Installatievoorschriften voor alarmapparatuur
Document 002757	Installatievoorschriften rolluiken
NCP AMR augustus 2007 versie 1.0	Algemene Montagerichtlijnen Elektrische Bediende Beveiligingsrolluiken
NEN 1010:2007+ C1:2008/A1:2011 +C1:2011 nl	Veiligheidsbepalingen voor laagspanningsinstallaties
Brandbeveiliging	
NEN-EN 14604: 2005/C1:2008 en	Rookmelders

NEN 2535:2009/C1:2010-06 nl	Brandveiligheid van gebouwen - Brandmeldinstallaties - Systeem- en kwaliteitseisen en projectierichtlijnen
NEN 2555:2008 nl	Brandveiligheid van gebouwen - Rookmelders voor woonfuncties
NEN 2575:2004/C1:2006 nl	Brandveiligheid van gebouwen - Ontruimingsinstallaties - Systeem- en kwaliteitseisen en projecteringsrichtlijnen
Toegangsbeheer en cameratoezicht:	
NEN-EN 50133-1: 1996/C1:1998/A1:2002 en	Alarmsystemen - Toegangsbewakingssystemen voor beveiligingstoepassingen - Deel 1: Systeemeisen
Cameratoezicht in de openbare ruimte	Handreiking cameratoezicht
Bouwkundige beveiliging:	
CCV	PKVW Beveiligingsrichtlijn versie februari 2013 en Productenlijst bestaande bouw versie september 2013
NEN-EN 356: 1999 en	Glas in gebouwen - Beveiligingsbeglazing - Beproeving en classificatie van de weerstand tegen manuele aanval
NEN 5087: 2013 nl	Inbraakveiligheid van woningen - Bereikbaarheid van dak- en gevelelementen: deuren, ramen en kozijnen
NEN 5089: 2009 nl	Inbraakwerend hang- & sluitwerk - Eisen en beproevingsmethoden
NEN 5096:2012	Inbraakwerendheid - Dak- of gevelelementen met deuren, ramen, luiken en vaste vullingen - Eisen, classificatie en beproevingsmethoden
NEN-EN 1627: 2011 en	Deuren, ramen, vliesgevels, traliehekken en luiken - Inbraakwerendheid - Eisen en classificatie
NEN-EN 1628: 2011 en	Deuren, ramen, vliesgevels, traliehekken en luiken - Inbraakwerendheid - Beproevingmethode voor de bepaling van de weerstand tegen statische belasting
NEN-EN 1629: 2011 en	Deuren, ramen, vliesgevels, traliehekken en luiken - Inbraakwerendheid - Beproevingmethode voor de bepaling van de weerstand tegen dynamische belasting
NEN-EN 1630: 2011 en	Deuren, ramen, vliesgevels, traliehekken en luiken - Inbraakwerendheid - Beproevingmethoden voor de bepaling van de weerstand tegen manuele inbraakpogingen
NEN-EN 14351-1: 2006+A1:2010 en	Ramen en deuren - Productnorm, prestatie-eisen - Deel 1: Ramen en deuren zonder brand- en rookwerende eigenschappen
SKG-KE 470	SKG - Kwaliteitseisen 470 voor het SKG productcertificaat voor meeneembeperkende producten
BRL 3104 (12-07-2012)	Nationale beoordelingsrichtlijn voor het KOMO® productcertificaat voor hang- en sluitwerk voor dak- en gevelelementen Deze BRL 3104 verwijst naar onderstaande normen
NEN-EN 12320: 2010 en	Hang- en sluitwerk - Hangsloten en beslag voor hangsloten - Eisen en beproevingsmethoden
NEN-EN 1303: 2005/C1:2008 en	Hang- en sluitwerk - Cilinders voor sloten - Eisen en beproevingsmethoden
NEN-EN 1906: 2012 en	Hang- en sluitwerk - Deurklinken en -knoppen - Eisen en beproevingsmethoden
NEN-EN 1935: 2002/C1:2007 en	Hang- en sluitwerk - Klepscharnieren met enkelvoudige as - Eisen en beproevingsmethoden
NEN-EN 12209: 2004/C1:2006 en	Hang- en sluitwerk - Sloten en grendels - Mechanisch bediende sloten, grendels en sluitplaten - Eisen en beproevingsmethoden
NEN-EN 12051: 1999 en	Hang- en sluitwerk - Schoten voor deuren en ramen - Eisen en beproevingsmethoden

NEN-EN 1627: 2011 en	Ramen, deuren, luiken - Inbraakwerendheid - Eisen en classificatie
NEN-EN 1630: 2011 en	Ramen, deuren, luiken - Inbraakwerendheid - Manuele beproeving
NEN-EN 1670: 2007/C1:2008 en	Hang- en sluitwerk - Bestandheid tegen corrosie - Eisen en beproevingsmethoden
NEN-EN-ISO 9227: 2006 en	Corrosiebeproeving in kunstmatige omgevingen - Zoutsproeibeproeving
NEN-EN 179: 2008 en	Hang- en sluitwerk - sluitingen voor nooduitgangen met een deurkruk of een drukplaat , voor gebruik van vluchtroutes - eisen en beproevingsmethoden (Noodopeners)
NEN-EN 1125: 2008 en	Hang- en sluitwerk - panieksluitingen voor vluchtdeuren met een horizontale bedieningsstang - eisen en beproevingsmethoden (Paniekopeners)
SKG-AE 3104: 2010	Prestatie-eisen, producteisen en andere eisen aan beveiligingsproducten voor ramen en deuren - additionele eisen voor BRL 3104