

VRKI 2.0 Deel B: definities van beveiligingsmaatregelen

Verbeterde risicoklasseindeling

Versie 2024

Publicatiedatum 1 december 2023

Overgangstermijn

VRKI 2.0 versie 2024 mag vanaf 1-1-2024 worden gebruikt, daarnaast mag tot 01-04-2024 ook gebruik worden gemaakt van VRKI 2.0 versie 2023.

Gedurende de overgangstermijn mogen:

- Projecten die reeds in de uitvoeringfase zitten doorgang vinden;
- Nieuwe plannen/offertes alleen gemaakt worden op basis van de VRKI 2.0 versie 2024;
- Plannen/offertes die reeds zijn opgestart worden afgerond op basis van de voorgaande VRKI 2.0, (versie 2023), indien verwacht wordt dat de startdatum van uitvoeringsfase ligt voor het verlopen van de overgangperiode;
- Delen van de VRKI 2.0 versie 2023 **niet** worden gecombineerd met versie 2024.

De VRKI 2.0 is eigendom van het Verbond van Verzekeraars en wordt beheerd en uitgegeven door het Centrum voor Criminaliteitspreventie en Veiligheid te 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 opnamen, of enige andere manier, zonder voorafgaande schriftelijke toestemming van het CCV en/of het Verbond van Verzekeraars.

Voor zover 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, Stb. 351, zoals gewijzigd bij het besluit van 23 augustus 1985, Stb. 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 or the owner.

Ondanks alle aan de samenstelling van deze uitgave bestede zorg, kunnen het Verbond van Verzekeraars en 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.

Inhoud

1. Inleiding	5
1.1 Definities en voorwaarden	6
1.2 Afkortingen	10
2. O – Organisatorische maatregelen	11
2.1 Niveau en omvang van de Organisatorische maatregelen	11
2.1.1 Niveau O1 – Standaard organisatorische maatregelen en voorlichting over preventie	11
2.1.2 Sleutelbeheer en -gebruik	11
2.1.3 Sluitronde	12
2.1.4 Merken en registreren van waardevolle zaken	12
2.1.5 Buren en omwonenden	12
2.1.6 Zichtbare afwezigheid voorkomen	12
2.1.7 Beveiligingsverlichting	12
2.1.8 Gebruik van compartimenten	12
2.1.9 Huisregels en discipline	13
2.1.10 Opklimmogelijkheden	13
2.1.11 Tuinaanleg	14
2.1.12 Toegangscontrole	14
2.1.13 Gegevensbeveiliging	14
2.1.14 Wijzigingen en omstandigheden	14
2.1.15 In - en Uitschakelregistratie bij de PAC	14
2.1.16 Up en Downloaden	15
2.1.17 In- en uitschakelen met app	15
2.1.18 Logboek	15
2.2 Niveau O2	15
3. BK - Bouwkundige maatregelen	16
3.1 Ramen en deuren (gevelelementen) en hang- en sluitwerk	16
3.1.1 Glas	17
3.2 Rolluiken en -hekken voor/achter bereikbare gevelelementen	17
3.3 Muren	18
3.4 Dak	19
3.5 Kruipruimte	20
3.6 Ramkraakbeveiliging	20
4. CO - Compartimentering	22
4.1 Bouwkundig compartiment	22
4.2 Kluizen	22
4.3 Inbraaksignaleringsysteem bij bouwkundige compartimenten & kluizen	23
5. ME - Meeneembeperkende maatregelen	24
5.1 ME1 niveau	24
5.2 ME2 niveau prestatie-eis 3 minuten diefstalvertraging	24
5.2.1 Verplaatsen	24
5.2.2 Koppelen	25
5.2.3 Verankeren	25
5.3 ME3 niveau prestatie-eis 5 minuten diefstalvertraging	25
5.3.1 Kisten of kasten	25
5.3.2 Vitrines	26

5.3.3	Hekwerken	26
5.4	ME4 niveau prestatie-eis 10 minuten diefstalvertraging	26
5.4.1	Mistgeneratoren	27
6.	EL - Elektronische maatregelen	28
6.1	Omvang elektronische maatregelen	28
6.1.1	Subsysteem	28
6.2	Ontwerp, aanleg & onderhoud	28
6.3	Eisen aan alarmapparatuur	28
6.3.1	Security grades	29
6.3.2	Environmental classes	30
6.3.3	Inbraaksigaleringsystemen bedraad of draadloos	30
6.3.4	In- en uitschakelen	31
6.4	Niveaus van elektronische maatregelen	31
6.4.1	Minimale eisen inbraaksigaleringsysteem	31
6.4.2	Minimale eisen omvang projectie	32
6.4.3	Eisen schildetectie	36
6.5	transmissiesysteem	36
7.	AT – Alarmtransmissie	37
7.1	Toelichting op Normering	37
7.2	Vereiste alarmtransmissiewegen	38
7.2.1	Alarmtransmissieniveau AT1 (alleen toepasbaar bij risicoklasse 1)	38
7.2.2	Alarmtransmissieniveau AT2	39
7.2.3	Alarmtransmissieniveau AT3	40
7.2.4	Alarmtransmissieniveau AT4	40
7.3	Kenmerken	40
7.4	Algemene eisen Alarmtransmissiesystemen	40
7.4.1	Alarm over IP	41
7.4.2	Secundaire transmissieverbinding	41
7.4.3	Prestatieniveau transmissiesysteem	41
7.4.4	Alarmtransmissie via mobiel netwerk	41
7.4.5	VOIP	41
7.4.6	Verificatie van prestaties	41
7.4.7	Beschikbaarheid	42
7.5	Beschrijving van alarmtransmissiesysteem	42
7.5.1	Woningen met een enkelpadig alarmtransmissiesysteem	42
7.5.2	Woningen met een dubbelpadig alarmtransmissiesysteem	43
7.5.3	Bedrijven met enkelpadig alarmtransmissiesysteem	43
7.5.4	Bedrijven met dubbelpadig alarmtransmissiesysteem	44
8.	RE - Reactie	45
8.1	Alarmverificatie methoden	45
8.1.1	Persoonlijke alarmverificatie	45
8.1.2	Technische alarmverificatie	45
8.2	Niveaus van alarmopvolging	46
8.2.1	Niveau RE1	46
8.2.2	Niveau RE2	46
8.2.3	Niveau RE3	46
8.2.4	Niveau RE4	46
9.	Verwijzingen (verbonden aan de VRKI 2.0)	47

1. Inleiding

De verbeterde risicoklassenindeling, versie 2.0 (verder te noemen de VRKI 2.0), is een instrument waarmee een globale risico-inschatting van diefstal en inbraak voor woningen en bedrijven wordt gemaakt. Deze inschatting bepaalt in welke risicoklasse een woning of bedrijf valt en de hoogte van deze klasse bepaalt de beveiligingsmaatregelen.

De keuze van beveiligingsmaatregelen is niet alleen gebaseerd op de beveiligingsgedachte, maar ook mede gebaseerd op de risico-acceptatie van verzekeraars. De VRKI 2.0 is niet wettelijk verplicht en het is ook geen erkennings- of certificatieregeling.

De VRKI 2.0 is geschreven voor verschillende belanghebbende partijen:

- De eindgebruiker die zijn woning/bedrijf wil beveiligen;
- De verzekeraar die er belang bij heeft om een object of voorraad in dekking te nemen tegen bepaalde voorwaarden;
- De installateur die de wensen van de eindgebruiker en/of verzekeraar gaat uitvoeren.

De VRKI 2.0 is bedoeld voor standaard objecten, voor de meest voorkomende woningen en bedrijven. De VRKI 2.0 is niet bedoeld voor (zeer) grote of bijzondere objecten met een hoge waarde concentratie of hoog risico, zoals bijvoorbeeld sommige juweliers, musea, een groot warenhuis, etc. Voor het vaststellen van het optimale beveiligingsconcept voor dergelijke situaties is maatwerk noodzakelijk.

De VRKI 2.0 bestaat uit twee delen. In deel A vindt u het instrument voor het bepalen van de risicoklassen en de keuze van een combinatie van beveiligingsmaatregelen.

In dit document, de VRKI 2.0 deel B, is invulling gegeven aan de verschillende niveaus van beveiligingsmaatregelen die zijn opgenomen in de tabellen voor woningen en bedrijven in deel A.

Volgens de VRKI 2.0 is het mogelijk en soms praktisch noodzakelijk om door middel van 'gelijkwaardigheid' een beveiligingsoplossing met behulp van andere materialen of componenten te realiseren.

1.1 Definities en voorwaarden

Beveiligingsplan

Primair zijn de eisen van toepassing die de brancheverenigingen in hun kwaliteitsregeling en certificatieschema hebben opgenomen. Mochten deze eisen niet of naar mening van de installateur/adviseur onvoldoende bruikbaar zijn kan gebruik gemaakt worden van onderstaande indeling en elementen voor het beveiligingsplan. Er is geen onderscheid voor woningen of bedrijven, maar wél voor lage en hogere risico's.

Bij risicoklasse 1 en 2 bevat het beveiligingsplan:

- De NAW-gegevens van de ontwerper/installateur en opdrachtgever;
- Projectnummer en datum van het beveiligingsplan;
- Een verwijzing naar het intakedocument (kenmerk en datum);
- Omschrijving van het object (of deel van een object bouwwerk of terrein);
- De functies (doelstelling), zwaartepunt van de beveiliging;
- De *geconstateerde risicoklasse* conform deel A van de VRKI op basis van te specificeren:
 - Waarde attractieve zaken van de inboedel (woningen);
 - of
 - Waarde en attractiviteit van goederen en inventaris (bedrijven).
- De *uitgevoerde risicoklasse* of (gedeeltelijke) uitvoering op een lager niveau;
- Een omschrijving/aanduiding van de te treffen beveiligingsmaatregelen;
- De elektronische maatregelen worden bij voorkeur aangegeven middels een plattegrond of installatietekening;
- Het af te geven kwaliteitsdocument (beveiligingscertificaat of opleveringsbewijs);
- De toegepaste referentiedocumenten;
- Ondertekening door het beveiligingsbedrijf en opdrachtgever.

Bij risicoklasse 3 en 4 bevat het beveiligingsplan:

- De NAW-gegevens van de ontwerper/installateur en opdrachtgever;
- Projectnummer en datum van het beveiligingsplan;
- Een verwijzing naar het intakedocument (kenmerk en datum);
- Omschrijving van het object (of deel van een object bouwwerk of terrein);
- De functies (doelstelling), zwaartepunt van de beveiliging;
- Een risicoanalyse (gericht op de materiële - en immateriële - attractieve zaken);
- De *geconstateerde risicoklasse* conform deel A van de VRKI op basis van te specificeren:
 - Waarde attractieve zaken van de inboedel (woningen);
 - of
 - Waarde en attractiviteit van goederen en inventaris (bedrijven).
- De *uitgevoerde risicoklasse* of (gedeeltelijke) uitvoering op een lager niveau;
- Een *gespecificeerde omschrijving* van de te treffen beveiligingsmaatregelen;
- Een plattegrond of installatietekening waarop de elektronische maatregelen worden aangegeven. Naast de verplichte eisen uit de VRKI moet ook rekening gehouden worden met de onderlinge samenhang op basis van de "schillentheorie";
- Het af te geven kwaliteitsdocument (beveiligingscertificaat of opleveringsbewijs);
- De toegepaste referentiedocumenten;
- Ondertekening door het beveiligingsbedrijf en opdrachtgever.

Beweegbare gevelelementen

Alle beweegbare gevelopeningen en dak elementen die door een gebruiker geopend kunnen worden. Zoals bijvoorbeeld: ramen, deuren, (dak)luiken.

Gelijkwaardige oplossingen

Met gelijkwaardige oplossingen wordt bedoeld het toepassen van componenten en materialen die leiden tot een oplossing die gelijkwaardig is aan het niveau van de componenten en materialen die in de desbetreffende risicoklassen zijn voorgeschreven. De gelijkwaardige oplossingen moeten voldoen aan de beoogde prestatie eis. Bij producten, constructies of installaties waarvoor genormaliseerde beproevingen of voorschriften bestaan, vindt de beoordeling plaats aan de hand van testresultaten of de desbetreffende voorschriften. Als dat niet mogelijk is, moet de beoordeling plaatsvinden op grond van vakkennis en ervaring. Gelijkwaardige oplossingen worden vastgelegd in het intakedocument en worden voor akkoord ondertekend door de belanghebbende partij(en), zoals opdrachtgever en beveiligingsbedrijf. De opdrachtgever moet de verzekeraar hierover informeren.

Goed vakmanschap

Het begrip 'goed vakmanschap' is een subjectief begrip. Het toepassen van 'goed vakmanschap' betekent dat goed en deugdelijk werk wordt geleverd dat voldoet aan de essentie van de in de VRKI 2.0 beschreven beveiligingsmaatregelen met de daarbij behorende prestaties. Waar mogelijk wordt bij het kiezen van componenten of beveiligingsoplossingen aansluiting gezocht bij gangbare normen of keurmerken, die anders kunnen zijn dan die in de VRKI 2.0 worden genoemd. Het toepassen van 'gelijkwaardigheid' en uitvoeren van 'maatwerk' vindt altijd plaats op basis van 'goed vakmanschap', waarbij het geleverde werk een effectieve en efficiënte beveiligingsoplossing moeten bieden. Goed vakmanschap betekent dat de effectiviteit van de maatregel leidend is en niet de wens van de klant om de beveiligingsmaatregelen zo goedkoop mogelijk te houden (met als gevolg dat tekort wordt gedaan aan de prestatie-eisen).

Intakedocument

Het intakedocument is een startdocument ter inventarisatie van de wensen van de klant en ten behoeve van installateur, adviseur, alarmopvolger en de verzekeraar, dat specifiek het risico van inbraak en diefstal vastlegt met de daarbij behorende maatregelen om dit risico beheersbaar te krijgen. Het intakedocument vormt het uitgangspunt voor elk beveiligingsplan. Afwijkingen ten opzichte van de geconstateerde risicoklasse dienen te worden vastgelegd in het intakedocument. Bij een geconstateerde risicoklasse 4 en/of indien er wordt afgeweken van de geadviseerde combinatie van maatregelen conform de geconstateerde risicoklasse, wordt het document altijd ter ondertekening aan de verzekeraar aangeboden. De opdrachtgever dient aantoonbaar kennis te nemen van het intakedocument*. De inhoud van het intakedocument is verplicht, de opmaak is vrij (zoals het toevoegen van een bedrijfslogo en het gebruik van andere lettertypen). Er moet altijd een intakedocument worden opgesteld.

Toelichting *

Het aantoonbaar kennis nemen van het intakedocument kan door ondertekening van het intakedocument, maar opdrachtgever is dat niet verplicht. In sommige gevallen roept het vragen om ondertekening van het intakedocument weerstand op, omdat opdrachtgever ten onrechte denkt dat hij tekent voor een opdracht. Het is echter in het belang van de ontwerper/adviseur dat de opdrachtgever juist geïnformeerd wordt over de soort, omvang en waarde van attractieve zaken en/of goederen. Daarom verdient het in alle gevallen aanbeveling om opdrachtgever te verzoeken te tekenen voor correcte opgave van attractiviteit en/of goederen. Bij het weigeren van ondertekening is het verstandig het intakedocument per mail aan opdrachtgever te verstrekken met verzoek voor ontvangstbevestiging.

Maatwerk

Maatwerk is de specifieke op het object toegesneden combinatie van beveiligingsmaatregelen. Waarbij de beoogde prestatie-eis van de vastgestelde risicoklasse wordt behaald. Maatwerk mag in alle risicoklassen worden uitgevoerd.

Toelichting

Beveiligingsmaatregelen die onder “Maatwerk” worden uitgevoerd moeten natuurlijk wel aan enkele uitgangspunten voldoen:

- De beveiligingsmaatregelen moeten op een gelijkwaardige manier worden uitgevoerd. Bijvoorbeeld: als je in klasse 4 voor maatwerk kiest mogen de EL4-maatregelen onder maatwerk niet worden uitgevoerd als EL3 of EL1;
- 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.

Mechanische afscherming

Vaste afscherming, zoals: traliewerk, barrière stang, rolluiken, rolhekken, schaarhekken.

Partiële beveiliging

Dit is de beveiliging van het gedeelte van het object waar zich concentraties van attractieve goederen bevinden (magazijn/opslag) die door inschaling in een hogere risicoklasse vallen dan het overige deel van het object (kantoren en/of productieruimten). In dat geval kan er voor de verschillende bouwdeelen een op het risico afgestemde combinatie van beveiligingsmaatregelen worden vastgesteld. Voorwaarde is dat het gaat om een fysiek afgescheiden gebouwgedeelte. Bij een afgescheiden gebouwgedeelte moeten de scheidingswanden e.d. met de rest van het gebouwencomplex voldoen aan dezelfde bouwkundige (inbraakwerendheid) eisen als die voor de buitengevels (daken etc.) van het beveiligde gedeelte. De hoogste risicoklasse wordt vastgelegd in het intakedocument met de daarbij behorende geadviseerde beveiligingsmaatregelen. In het beveiligingsplan wordt de partiële beveiliging toegelicht.

Rapportagetijd

Rapportagetijd is de tijd tussen het moment waarop er een fout in het alarmtransmissiesysteem (ATS) optreedt en het moment waarop dit wordt gerapporteerd aan de PAC. 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 hoofdstuk 7).

Risicoanalyse maken (security)

Bij elk object is er sprake van allerlei soorten risico's. Criminele en niet-criminele risico's. Onder het maken van een risicoanalyse, zoals dat vermeld is bij de eisen voor een beveiligingsplan, wordt bedoeld het analyseren van criminele risico's in de ruimste zin van het woord. Hoewel de nadruk op diefstal en inbraak ligt moet er ook gekeken worden naar overvalrisico, verduistering door eigen personeel, hacking, brandstichting, vandalisme, ontvoering, etc. Daarnaast moet ook een analyse gemaakt worden van andere factoren die van invloed zijn op het risico. We noemen wat voorbeelden bij een woning. Bij een woning wordt in de risicoklasse bepaling VRKI alleen gekeken naar de aanwezigheid van attractieve zaken van de inboedel, terwijl er veel andere factoren zijn die meespelen bij het bepalen van het inbraakrisico. Als voorbeeld noemen we enkele zaken: bouwaard van de woning, ligging van de woning (bebouwde kom of platteland, In Amsterdam of Drenthe, op de begane grond of 12^e etage), bestaande preventieve voorzieningen (waaronder b.v. een portier in een appartementencomplex, buurtpreventie, deelname aan PKVW, toezicht door particuliere beveiligers, etc.). En natuurlijk de welvaartsklasse van de woning, uitstraling en zichtbaarheid attractieve zaken en gedrag bewoners. De lijst met factoren is heel lang en per situatie anders. Van u wordt een professioneel advies verwacht.

Schildetectie

Schildetectie heeft betrekking op inbraaksignalering bij de eerste aanval op of voor de periferie van een gebouw of deel van een gebouw.

Schillentheorie

Uitgangspunt van beveiligen bij bedrijven is “buit” compartimenteren en rondom voorzien van detectie. Zo wordt voldaan aan het principe: eerst signaleren en dan vertragen.

Voor woningen is dat vaak praktisch niet haalbaar (m.u.v. geld, sieraden, waardepapieren en sommige verzamelingen) Bij woningen speelt als belangrijkste eis: daders buiten houden. Dus inbraakpreventie.

Hoge risico's bedrijven: Afstemmen van de onderlinge samenhang van de verplichte maatregelen uit de VRKI die genoemd worden in de beveiligingsmatrix (op basis van O, BK, CO, ME, EL, SD, AT en RE-maatregelen) is verplicht; daarbij rekening houden met de schillentheorie is dringend gewenst. Elke schil draagt het karakter van eerst signaleren en dan vertragen.

Voorbeeld van een bedrijf met zeer hoge attractieve goederen en zeer hoge waarde. Denk aan een diamantair of vergelijkbaar risico.

- 1e schil: de attractieve goederen worden opgeborgen in een inbraakwerende kast;
- 2e schil: detectie rondom en op de inbraakwerende kast;
- 3e schil: de inbraakwerende kast wordt geplaatst in een compartiment CO;
- 4e schil: in het compartiment wordt een mistgenerator geplaatst;
- 5e schil: rondom het compartiment is ruimtelijk werkende detectie voorzien van anti-Masking;
- 6e schil: in het object is valstrikbeveiliging aangebracht;
- 7e schil: de gevels van het object voldoen aan BK2-niveau;
- 8e schil: buiten de gevels van het object vindt detectie plaats d.m.v. AIR of buitendetectie;
- 9e schil: buiten de gevels van het object vindt toezicht plaats d.m.v. CCTV;
- 10e schil: het buitenterrein is voorzien van een deugdelijk hekwerk;
- 11e schil: achter het hekwerk is schrikdraad detectie aangebracht;
- 12e schil: toezicht en alarmopvolging door een particuliere beveiligiger.

Subsysteem

Deel van het inbraaksignaleringssysteem dat zich in een gedefinieerd deel van het beveiligd gebied bevindt en dat onafhankelijk van andere delen van het inbraaksignaleringssysteem kan functioneren. Bij het gebruik van subsystemen behoren de betreffende geografische gebieden bouwkundig afsluitbaar te zijn. Hierdoor kan worden voorkomen dat door het betreden van het beveiligd gebied van een ingeschakeld subsysteem ongewenst alarm ontstaat.

Vaste gevelementen

Alle niet beweegbare gevel- en dak elementen.

Verbeterde risicoklasseindeling (VRKI)

De VRKI is een instrument waarmee een globale risico-inschatting van diefstal en inbraak voor woningen en bedrijven gemaakt wordt. Dit mag niet verward worden met het maken van een risicoanalyse. De VRKI is slechts een globale risico-inschatting. Er wordt met een beperkt aantal meetfactoren rekening gehouden.

Zwaartepunt van het risico

Het benoemen van het zwaartepunt van het risico maakt voor alle partijen direct inzichtelijk: waar ligt de concentratie van goederen met de hoogste attractieve waarde? Met andere woorden; welke buit is voor daders het meest interessant? Naast de waarde van goederen kan het ook gaan om zaken waardoor een bedrijf erg kwetsbaar wordt uit oogpunt van bedrijfscontinuïteit. De beveiliging dient zich dus hierop te concentreren.

1.2 Afkortingen

De VRKI 2.0 gebruikt de volgende afkortingen:

ADSL	A-symmetric Digital Subscriber Loop (standaard voor een digitale technologie die snellere datacommunicatie over een telefoonlijn toestaat)
AT(..)	Niveau alarmtransmissie traject
ATP	Alarmtransmissiepad
ATS	Alarmtransmissiesysteem
ATSN	Alarmtransmissieservicenetwerk
ATSP	Alarmtransmissieserviceprovider
CCS	Centrale Controle Stuur eenheid
DP(..)	Dual Path (dubbelpadig alarmtransmissiesysteem)
EN	Europese Norm
Grade	Security Grade (niveau waaraan de beveiliging moet worden voldaan)
IP	internetprotocol
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	Particuliere Alarmcentrale
POTS-poort	plain old telephone service (poort op router ten behoeve van analoge telefonie. Ook als PSTN aangeduid)
PSTN-poort	public switch telephone network (poort op router ten behoeve van analoge telefonie. Ook als POTS aangeduid)
Shared line	Gedeelde lijnverbinding met andere gebruikers
SP(..)	Single Path (enkelpadig alarmtransmissiesysteem)
SPT	Supervised Premises Transceiver (alarmoverdrager)
UPS	Uninterruptible Power Supply (niet onderbrekbare voeding/noodstroomvoorziening)
VoIP	Voice over IP (hierbij wordt het internet of een ander IP-netwerk gebruikt om spraak te transporteren)
VRKI 2.0	Verbeterde risicoklassenindeling 2.0

2. O – Organisatorische maatregelen

Onder de O-maatregelen vallen de organisatorische maatregelen die bijdragen aan de preventie van inbraak en/of diefstal. Zoals het juiste gebruik van technische preventieve voorzieningen en het regelen van het onderhoud daarvan. Organisatorische maatregelen moeten zijn afgestemd op het bewuste risico-object en de overeengekomen andere beveiligingsmaatregelen met als doel het de inbreker zo moeilijk mogelijk te maken. Zonder de overeengekomen Organisatorische maatregelen kunnen de andere beveiligingsmaatregelen niet of niet goed functioneren.

In de tabellen met een combinatie van beveiligingsmaatregelen voor woningen en bedrijven in VRKI 2.0 deel A worden de niveaus van organisatorische maatregelen aangeduid met de letter O en een cijfer. Dit cijfer heeft betrekking op de zwaarte van het niveau van de O-maatregelen.

Er zijn twee niveaus aan O-maatregelen:

- O1: standaard organisatorische maatregelen;
- O2: Als O1 met daarbij een omschrijving van de specifieke organisatorische maatregelen die zijn toegespitst op het risico-object.

Onderstaand volgen enkele belangrijke voorbeelden van organisatorische maatregelen, zowel op het gebied van verantwoordelijkheid, als in en rondom een huis of pand.

2.1 Niveau en omvang van de Organisatorische maatregelen

2.1.1 Niveau O1 – Standaard organisatorische maatregelen en voorlichting over preventie

Inbraakpreventie is niet alleen een kwestie van het nemen 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 er de nodige organisatorische maatregelen worden getroffen. Het heeft dus vooral te maken met (preventief) gedrag. 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 aan organisatorische maatregelen zal van geval tot geval verschillen; het is sterk afhankelijk van de situatie. Die verschillen kunnen veroorzaakt worden door bouwaard van het te beveiligen object, ligging, al of niet aanwezig zijn van aantrekkelijke attractieve goederen, woon- en werkpatronen, soort beveiliging, eisen verzekeraar, etc. Er zijn voldoende publicaties voorhanden die aandacht besteden aan de volgende standaard onderwerpen. De op het risico-object afgestemde organisatorische maatregelen behoren bij oplevering van een alarminstallatie of het beveiligingssysteem op schrift te worden gesteld en aan de gebruiker te worden overhandigd.

2.1.2 Sleutelbeheer en -gebruik

Een slot moet goed worden gebruikt, 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 worden gemaakt 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. Het uitdraaien van de nachtschoot voorkomt dat door middel van flipperen (terugduwen van de dagschoot met behulp van bijvoorbeeld een betaalpasje) de deur kan worden geopend. De sleutel uit het slot halen voorkomt dat de deur van het slot wordt gedraaid middels gaatjes boren of een via een handgat in het raam. Bij bedrijven verdient het aanbeveling om te registreren wie een sleutel in gebruik heeft en om daarnaast gebruik te maken van een

gecertificeerde sleutel. Het voorkomt snel (illegaal) kopiëren van de sleutel. Er dient, met name bij bedrijven, een meldingsplicht te zijn bij verlies van een sleutel.

2.1.3 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. Zorg voor een vaste afsluitronde; 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. Tevens dient de sluitronde ervoor om vast te stellen dat detectoren “vrij zicht” hebben. 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.

2.1.4 Merken en registreren van waardevolle zaken

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

2.1.5 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 bijvoorbeeld worden georganiseerd in de vorm van buurtpreventie projecten zoals een buurtapp. 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 kan de bewaking worden georganiseerd in samenwerking met particuliere beveiligingsorganisatie, gemeente en politie.

2.1.6 Zichtbare afwezigheid voorkomen

In vakantieperiodes kunnen gesloten gordijnen, overvolle brievenbussen en niet gemaaide gazons afwezigheid verraden. Buren, kennissen of familieleden kunnen helpen om een huis bewoond te laten lijken. Het laten branden van enkele lichtpunten in het huis accentueert het bewoonde uiterlijk. Door middel van instelbare schakelklokken of domotica kan met enkele lichtpunten in het huis een normaal bewoningspatroon worden gesimuleerd. Bij bedrijfspanden werkt nachtverlichting preventief en dit maakt het tevens mogelijk voor alarmopvolgers zich te oriënteren.

2.1.7 Beveiligingsverlichting

Een inbreker wordt niet graag gezien. Vandaar dat eventueel automatische beveiligingsverlichting langs de buitenkant van het gebouw preventief werkt indien de omgeving (sociale) controle toelaat. 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.

2.1.8 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. Menselijk gedrag speelt hierbij een grote rol, want ook overdag moet het compartiment gesloten zijn. De deur van de koelkast is ook dicht als u thuis bent.

2.1.9 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 brandwerend te worden opgeborgen?

Voor grotere bedrijfspanden en overheidsgebouwen is de “kleurenmethode” hiervoor ideaal. Het is de bedoeling dat er door eigen mensen van het bedrijf (liefst de afdelingschef mét zijn medewerkers) twee plattegronden van het te beveiligen pand worden ingekleurd.

Plattegrond 1

- Groen: alle ruimtes waar bezoekers vrij mogen rondlopen;
- Geel: alle ruimtes waar bezoekers onder begeleiding van medewerkers mogen komen;
- Rood: alle ruimtes die alleen toegankelijk zijn voor geautoriseerd personeel. Denk hierbij aan de kluis- of computer ruimte.

Plattegrond 2

- Groen: alle ruimtes waar geen attractieve goederen aanwezig zijn en/of die niet kwetsbaar zijn voor de organisatie;
- Geel: alle ruimtes met enige attractiviteit en/of die van belang zijn voor de organisatie;
- Rood: alle ruimtes met concentratie van zeer hoge attractiviteit of kwetsbaarheid voor de organisatie.

Op deze wijze wordt eenvoudig antwoord gegeven op alle vragen. Hierdoor krijg je overzicht waar de compartimenten moeten komen én je ziet in één opslag waar de toegangscontrole moet plaatsvinden. Echter het allerbelangrijkste is: alle maatregelen worden gedragen door het personeel en de afdelingschef. Want mensen hebben van nature de neiging zichzelf belangrijk te vinden. Eigen werknemers zullen zwaardere maatregelen voorstellen dan de VRKI 2.0.

2.1.10 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 een van het gebouw verwijderde plek te worden geplaatst. 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 naar verbreking van de schil; het dak wordt zelden gecontroleerd. Inbrekers weten dit en maken hiervan handig gebruik.

2.1.11 Tuinaanleg

Het is van belang dat de inbreker niet ongezien te werk kan gaan door hoge begroeiingen. Het verdient aanbeveling om de hoogte van de struiken voor het gebouw te beperken tot circa 1 meter. Het is goed om hiermee rekening te houden bij de tuinaanleg en ook om bij het tuinonderhoud de 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 vormt wel een extra barrière. Ook voor vandalen en ook bij de eventuele afvoer van de buit. Bovendien vormt een gesloten hekwerk een juridische afscherming. Iemand die zich achter een gesloten hekwerk bevindt, is in overtreding volgens artikel 461 Sr.

2.1.12 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 kan dit met elektronische toegangscontrole. Anderzijds kan dit met persoonlijke toegangscontrole zoals 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.

2.1.13 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 beveiligd moeten worden tegen brand en diefstal. En niet te vergeten: tegen 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. Daar waar mogelijk zou ook gebruik kunnen worden gemaakt van een gecertificeerde cloudoplossing.

2.1.14 Wijzigingen en omstandigheden

De klant moet bij oplevering van de beveiligingsmaatregelen op de hoogte worden gesteld dat een verandering van het risico ook kan leiden tot een wijziging van de beveiligingsmaatregelen. Het verdient aanbeveling om dit steeds goed in het oog te houden zodra 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. Zodra er wijzigingen worden doorgevoerd die van invloed zijn op de beveiliging, dienen deze zo spoedig mogelijk te worden doorgegeven aan het beveiligingsbedrijf. 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.

2.1.15 In - en Uitschakelregistratie bij de PAC

Bij gebruik van een inbraaksignaleringsstelsel met aansluiting op een PAC dienen de (gedeeltelijke) in - en uitschakelingen met status en tijdstip te worden verstuurd. Hiermee wordt bereikt dat de centralist bij een inbraakalarmmelding zicht heeft op de actieve status van het stelsel. Bedieningsfouten waarbij een inbraakmelding wordt veroorzaakt zijn hierdoor herkenbaar.

2.1.16 Up en Downloaden

Onder uploaden 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 upload procedure kunnen uitsluitend gegevens, komende uit het systeem, worden uitgelezen. Het is met deze procedure niet mogelijk parameters te wijzigen of te verwijderen.

Downloaden 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 download communicatieverbinding mag slechts tot stand komen na een bewuste handeling die in het beveiligde object moet plaatsvinden. De bewuste handeling dient door het systeem automatisch te worden gemeld en geregistreerd bij de 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 downloaden (indien van toepassing) in het dossier van de klant bij het beveiligingsbedrijf aanwezig te zijn.

2.1.17 In- en uitschakelen met app

Bij gebruik van een app om een inbraaksignaleringsysteem in- en uit te schakelen is de beheerder van het inbraaksignaleringsysteem volledig verantwoordelijk voor de risico's die daaraan kleven. Zorg dat autorisatie voor toegang in de app goed geregeld is. Voor in- en uitschakelen zie ook paragraaf 6.3.4.

2.1.18 Logboek

Bij oplevering van de alarminstallatie ontvangt de gebruiker een logboek. Het logboek kan ook digitaal worden verstrekt. Het logboek bevat:

- Een instructie voor de gebruiker welk preventief onderhoud de gebruiker zelf periodiek dient uit te voeren;
- Een notieblad 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 storing opheffing met vermelding van datum en naam van de monteur die deze werkzaamheden heeft uitgevoerd.

2.2 Niveau O2

Als O1 met aanvulling: omschrijving van **de specifieke** organisatorische maatregelen die zijn toegespitst op het risico-object. 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. BK - Bouwkundige maatregelen

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

Waar wordt verwezen naar normen wordt gebruik gemaakt van de vigerende versie.

Uitgangspunt woningen

- De beveiligingsfilosofie voor woningen is gericht op het buiten houden van inbrekers. Voor woningen geldt daarom dat de combinaties van beveiligingsmaatregelen met ten minste niveau BK2 in alle gevallen de voorkeur hebben.

Uitgangspunt bedrijven

- De beveiligingsfilosofie voor bedrijven is gericht op signaleren en compartimenteren. Niveau BK3 en BK4 maatregelen voor bedrijven in klasse 3 en 4 zijn primair bedoeld voor de gevels waarachter zich direct attractieve goederen H of ZH bevinden, die niet beveiligd zijn met CO en/of ME maatregelen. Vanaf risicoklasse 3 kan tevens ramkraakbeveiliging van toepassing zijn.

In de tabellen met combinaties van beveiligingsmaatregelen voor woningen en bedrijven in VRKI 2.0 deel A worden de niveaus van bouwkundige maatregelen aangeduid met de letter BK en een cijfer. Dit cijfer heeft betrekking op de zwaarte van het niveau van de BK-maatregelen.

Er zijn vier niveaus aan BK-maatregelen:

- BK1: Bouwkundige maatregelen met functionerend hang- en sluitwerk en goede kwaliteit van de gevelementen
- BK2: Bouwkundige maatregelen met prestatie-eis van 3 minuten inbraakwerendheid
- BK3: Bouwkundige maatregelen met prestatie-eis van 5 minuten inbraakwerendheid
- BK4: Bouwkundige maatregelen met prestatie-eis van 10 minuten inbraakwerendheid

3.1 Ramen en deuren (gevelementen) en hang- en sluitwerk

De bereikbaarheid van dak- en gevelementen wordt bepaald aan de hand van NEN 5087. Ondanks dat deze norm in basis is bedoeld voor woningen, moet deze norm binnen de VRKI voor alle te beveiligen objecten (ook voor bedrijven, winkels, scholen ect.) worden toegepast. Hierop is maar een uitzondering: voor woningen mag bij BK2 voor het bepalen van de bereikbaarheid van dak- en gevelementen ook gebruik worden gemaakt van de PKVW-handleiding 2020 bestaande bouw (Bijlage bereikbaarheid).

- BK2: Om te voldoen aan BK2 moeten bereikbare ramen en deuren voldoen aan de prestatie-eisen in NEN 5089, inclusief de BRL 3104 (*eisen hang- en sluitwerk*) óf de prestatie-eisen in NEN 5096 weerstandsklasse 2 (*eisen geattesteerde gevelementen*) of aan gelijkwaardige oplossingen. BK2 mag bij woningen ook gerealiseerd worden door PKVW.
- Bij BK2, BK3 en BK4 is cilinderkerntrek beveiliging verplicht.
- BK3: Om te voldoen aan BK3 moeten bereikbare ramen en deuren voldoen aan de prestatie-eisen in NEN 5096 weerstandsklasse 3 of aan gelijkwaardige oplossingen.
- BK4: Om te voldoen aan BK4 moeten alle gevelementen voldoen aan weerstandsklasse 4 conform NEN-EN 1627.

Om te komen tot gelijkwaardige oplossingen die voldoen aan de prestatie-eisen in NEN 5096, kan gebruik worden gemaakt van conformiteitsverklaringen van erkende keuringsinstituten, op basis van toetsing en goedkeuring. Onder gelijkwaardige oplossingen voor BK2 wordt in ieder geval verstaan dat het gevelement en hang- en sluitwerk voldoen aan de NEN 5089 in combinatie met BRL 3104 + AE 3104. Eisen voor elektronisch bediend hang- en sluitwerk zijn opgenomen in SKG AE 3104. Denk hierbij aan elektromagnetische sloten en sluitplaten en mechatronische cilinders. Bij overheaddeuren dient rekening gehouden te worden met opdrukbeveiliging conform NEN-EN 1627-1630. Het afschakelen van overheaddeuren leidt niet altijd tot de juiste opdrukbeveiliging. In die gevallen is aanvullende mechanische opdrukbeveiliging noodzakelijk.

TABEL 3.1 – PRESTATIE-EISEN BOUWKUNDIGE INBRAAKWERENDHEID

	BK1	BK2	BK3	BK4
Prestatie-eis	Functionerend hang- en sluitwerk en goede kwaliteit gevelementen	3 minuten inbraakwerendheid	5 minuten inbraakwerendheid	10 minuten inbraakwerendheid
Van toepassing zijnde normen	geen norm	Bestaande bouw: NEN 5089 en BRL 3104 + AE 3104	NEN 5096 (weerstandsklasse 3)	NEN-EN 1627 (weerstandsklasse 4)
		Renovatie of nieuwbouw: NEN 5096 (weerstandsklasse 2)		

3.1.1 Glas

De prestatie-eisen voor glas zijn conform de glastabellen uit de NEN 5096 en NEN-EN 1627.

TABEL 3.2 – PRESTATIE-EISEN GLAS

	BK1	BK2	BK3	BK4
Prestatie-eis	Geen eisen	Enkel glas, isolatieglas of gelaagd glas	P5 A volgens NEN-EN 356	P6 B volgens NEN-EN 356
Van toepassing zijnde normen	Geen norm	Renovatie of nieuwbouw: NEN 5096 (weerstandsklasse 2),	NEN-EN 1627 (weerstandsklasse 3)	NEN-EN 1627 (weerstandsklasse 4)
		Bestaande bouw: Beveiligingsrichtlijn Politiekeurmerk Veilig Wonen of NEN 5089 en brl 3104 + AE 3104		

3.2 Rolluiken en -hekken voor/achter bereikbare gevelementen

Rolluiken en -hekken kunnen zowel vóór als achter een gevelement worden geplaatst. Dit is bepalend voor het BK-niveau van het beveiligde gevelement. Voor BK1 geldt geen prestatie-eis voor het rolluik of het rolhek. Voor BK2 geldt de prestatie-eis van 3 minuten inbraakwerendheid. Voor BK3 geldt de prestatie-eis van 5 minuten inbraakwerendheid. En voor BK4 geldt de prestatie-eis van 10 minuten inbraakwerendheid.

Als een rolluik of rolhek vóór het gevelement, aan de buitenzijde van het gebouw, geplaatst wordt, is een vrije aanval mogelijk op het rolluik of rolhek. Daarbij is aandacht vereist voor het voorkomen dat het rolluik

of rolhek wordt opgedrukt. Rolluiken en rolhekken die op deze manier geplaatst zijn, moeten zijn getest en goedgekeurd volgens de NEN 5096 en NEN-EN 1627, NEN-EN 1628, NEN-EN 1629 en NEN-EN 1630. Het rolluik of rolhek moet van openstand detectie worden voorzien die niet te manipuleren is. Een uitzondering hierop is mogelijk als een rolluik of rolhek maximaal 20 centimeter achter het gevelement, zowel vaste ramen als deuren, wordt geplaatst. Er is dan geen vrije aanval mogelijk op het rolluik of rolhek. Bij rolluiken en -hekken die op deze manier zijn geplaatst, mag in de weerstandsklasse BK3 ook worden gekozen voor rolluiken of rolhekken die zijn goedgekeurd en opgenomen in de NCP/Romazo Rolluiken matrix. Deze uitzondering is niet van toepassing bij volglazen deuren, schuifdeuren en naar buiten draaiende deuren. Detectie dient plaats te vinden voordat het rolluik kan worden aangevallen.

Besturing van het rolluik of -hek dient in beveiligd gebied geplaatst te worden of door middel van een afstandsbediening of in gesloten positie spanningsloos.

TABEL 3.3 - PRESTATIE-EISEN ROLLUIKEN EN ROLHEKKEN

	BK1	BK2	BK3	BK4
Prestatie-eis	Functionerend rolluik of rolhek	3 minuten inbraakwerend	5 minuten inbraakwerend	10 minuten inbraakwerend
Van toepassing zijnde normen, voor de gevel of meer dan 20 cm achter de gevel	geen eis	NEN 5096	<ul style="list-style-type: none"> ■ NEN 5096 of ■ NEN-EN 1627 	NEN-EN 1627 NEN-EN 1628 NEN-EN 1629 NEN-EN 1630
Van toepassing zijnde normen binnen 20 cm achter het gevelement m.u.v.: <ul style="list-style-type: none"> ■ Volglas deuren ■ Schuifdeuren ■ Naar buiten draaiende deuren 	geen eis	<ul style="list-style-type: none"> ■ NEN 5096 of ■ gekwalificeerd volgens de NCP/Romazo matrix O2, G2 	<ul style="list-style-type: none"> ■ NEN 5096; of ■ NEN-EN 1627, NEN-EN 1628, NEN-EN 1629 en NEN-EN 1630; of ■ gekwalificeerd volgens NCP/Romazo matrix O3, G3 	<ul style="list-style-type: none"> ■ NEN-EN 1627, NEN-EN 1628, NEN-EN 1629 en NEN-EN 1630* of ■ doorzichtige rolluiken gekwalificeerd volgens WK3
* Voor bestaande situaties is G3 volgens de Romazo matrix voldoende voor BK4, zolang de gevel niet wordt aangepast.				

3.3 Muren

Het bouwkundig niveau wordt niet alleen bepaald door de deuren en ramen, maar ook door de gevel van het gebouw.

Woningen

Gevels en daken (buitenschil) moeten voldoen aan dezelfde BK-eisen als de gevelementen. Bij woningen is er sprake van inbraakpreventie; daders buiten houden.

Bedrijven

Muren van bedrijven moeten voldoen aan het gekozen BK-niveau als direct achter deze muur de attractieve goederen (H en ZH) aanwezig zijn en er geen sprake is van compartimentering of meeneembepurende maatregelen volgens het gekozen niveau. Dit geldt voor alle aanvalszijden van de ruimte(n), ook als dit binnenmuren, vloeren en plafonds zijn.

Bij bedrijven is sprake van diefstalpreventie. Daders zijn in de meeste gevallen niet of nauwelijks buiten te houden. Het gaat om compartimenteren of meeneembeperving in combinatie met detectie op de aanvalszijden.

TABEL 3.4 - TYPEN MUREN

	BK1	BK2	BK3	BK4
Betonmuur	wel toegestaan	wel toegestaan	eis: min. 70 mm dikte met wapening	eis: min. 80 mm dikte met wapening
Stenen muur	wel toegestaan	wel toegestaan	eis: tweemaal halfsteens (min. 100 mm) muur van gebakken steen of kalkzandsteen	eis: steens muur van gebakken steen of kalkzandsteen, min. 200 mm
Overige muren, bijvoorbeeld: <ul style="list-style-type: none"> ■ metalstud, ■ spaanplaat ■ gips ■ gasbeton ■ hout 	Handhaven bestaande situatie	Woningen (Risicoklasse 1 t/m 4) en bedrijven (Risicoklasse 1 en 2): handhaven bestaande situatie. Bedrijven in risicoklasse 3 en 4 met H of ZH goederen waar CO of ME maatregelen ontbreken: niet toegestaan versterking nodig om tot de benodigde weerstandsklasse te komen	niet toegestaan, versterking nodig om te komen tot benodigde weerstandsklasse	niet toegestaan, versterking nodig om te komen tot benodigde weerstandsklasse

3.4 Dak

Voor het beoordelen van de inbraakwerendheid van de schil van het gebouw moet ook het dak worden beoordeeld. Het bouwtype, de attractiviteit en de maatvoering van de goederen in het gebouw zijn bepalend voor de vroegtijdige signalering en de beoogde vertraging. Voor de binnen de beveiligingsniveaus toegestane dakconstructies, zie tabel 3.5. De bereikbaarheid van daken wordt bepaald aan de hand van de NEN 5087. Voor daken die niet bereikbaar zijn volgens NEN 5087 zijn alle type daken toegestaan bij alle beveiligingsniveaus.

TABEL 3.5 - TYPEN DAKEN

	BK1	BK2	BK3	BK4
Dunne metalen dakplaten	Toegestaan	Toegestaan	Niet toegestaan zonder aanvullende beveiligingsmaatregelen, tenzij onbereikbaar	Niet toegestaan zonder aanvullende beveiligingsmaatregelen, tenzij onbereikbaar
Sandwichpanelen	Toegestaan	Toegestaan	Niet toegestaan zonder aanvullende beveiligingsmaatregelen, tenzij onbereikbaar	Niet toegestaan zonder aanvullende beveiligingsmaatregelen, tenzij onbereikbaar
Houten daken al dan niet met isolatie	Toegestaan	Toegestaan	Niet toegestaan zonder aanvullende beveiligingsmaatregelen, tenzij onbereikbaar	Niet toegestaan zonder aanvullende beveiligingsmaatregelen, tenzij onbereikbaar
Pannen daken voorzien van houten dakbeschot al dan niet met isolatie	Toegestaan	Toegestaan	Toegestaan	Niet toegestaan zonder aanvullende beveiligingsmaatregelen, tenzij onbereikbaar
Betonconstructie	Toegestaan	Toegestaan	Toegestaan	Toegestaan

3.5 Kruipruimte

Voor vloeren zonder kruipruimte gelden geen prestatie-eisen voor de verschillende BK-niveaus. Voor vloeren met een kruipruimte die vanaf buiten of via een naburig pand te bereiken is, geldt dat de kruipruimte vanaf BK2 (bedrijven) en vanaf BK3 en BK4 (woningen en bedrijven) beveiligd moet worden. De prestatie eis van het luik is gelijk aan de weerstandsklasse van de gevel. Voor kwetsbare vloeren, waaronder houten vloeren en vloeren met gaten, geldt maatwerk.

3.6 Ramkraakbeveiliging

In een aantal situaties is het alleen toepassen van bouwkundige beveiligingsmaatregelen, genoemd in de VRKI 2.0, niet voldoende. Er bestaat namelijk ook het risico van een ramkraak. Bij een ramkraak is er altijd sprake van een voertuig waarmee de buitenschil (gevel/muur/raam) van het beveiligde object met geweld wordt geforceerd. Een eenduidig antwoord is niet te geven op de vraag wanneer ramkraak beveiliging noodzakelijk, dan wel gewenst is. In elk geval is er sprake van ramkraakgevoeligheid bij een object:

- Als een volume aan attractiviteit H of ZH aanwezig is, en;
- de buitenschil (muur) van het object onvoldoende sterk is om een rijdend voertuig dat met kracht tegen de muur rijdt te weerstaan, en;
- er sprake is van een bepaalde (vrije) “aanrijdbaarheid” van een (motor)voertuig.

Ramkraakbeveiliging is noodzakelijk, indien:

- Het risico in risicoklasse 3 of 4 valt, en;
- Een risico-gevelement 'aanrijdbaar' is (let op: afsluiting van een gebied met bijvoorbeeld pollers of dergelijke voorkomt niet dat de gevel aanrijdbaar is. Er is dan grote afhankelijkheid van andere partijen), en;
- De ramkraak toegang geeft tot de attractieve goederen en inventaris. Indien de goederen en inventaris zijn beveiligd door middel van compartimentering en/of goede meeneembeperkende maatregelen, is ramkraakbeveiliging alleen nodig als een ramkraak de gerealiseerde beveiliging (voor een belangrijk deel) teniet doet.

Bij de dimensionering van de ramkraakbeveiliging moet worden uitgegaan van de impact op de beveiligingsmiddelen, gebaseerd op de te verwachten aard en de snelheid van het gebruikte voertuig. De te verwachten aard en snelheid van het voertuig dienen op basis van goed vakmanschap te worden afgestemd op de VRKI 2.0 risicoklasse en plaatselijke omstandigheden.

Voorbeelden van ramkraakbeveiliging

- Straatmeubilair, zoals banken, bloembakken of bespeelbaar straatmeubilair;
- Voldoende stevige palen van metaal (al dan niet volgestort met beton) of hout, waarbij goede aandacht nodig is voor de verankering in de grond (voldoende diep);
- Metalen beugels (autovangrail is relatief goedkoop en wordt veel gebruikt);
- Indien mogelijk een beveiliging achter het gevelement;
- Ramkraak bestendig rolluik of rolhek;
- Andere mogelijkheden zijn bijvoorbeeld: waterpartijen, een grindbak, greppel of verhoogde entree.

Het is zinvol om tijdig rekening te houden met ontwikkelingen die in de toekomst te verwachten zijn. Denk aan:

- Verhoogde voertuigmassa waardoor de oplossingen die op dit moment worden aangeboden door de markt wellicht te licht van uitvoering kunnen zijn.
- Het voertuig onbemand kunnen bedienen, zoals met een App op een smartphone. Hierbij is het risico van letsel bij de bestuurder afwezig, waardoor inzet van voertuigen voor een ramkraak breder wordt.
- Na een ramkraak met een elektrisch voertuig is het risico van brand groter. Een brandend elektrisch voertuig is nog nauwelijks te blussen.

4. CO - Compartimentering

De CO-maatregelen staan voor compartimentering. Het doel van een compartiment is het zodanig bouwkundig afschermen van een concentratie attractieve goederen, dat er een effectieve bescherming tegen diefstal van deze attractieve goederen wordt verkregen.

In de tabellen met beveiligingsmaatregelen voor woningen en bedrijven in VRKI 2.0 deel A worden de niveaus van compartimentering aangeduid met de letter CO en een cijfer. Dit cijfer heeft betrekking op de zwaarte van het niveau van de CO-maatregelen.

Er zijn vier niveaus aan CO-maatregelen:

- CO1: Compartimentering waarvan geen prestatie-eis voor inbraakwerendheid is bepaald;
- CO2: Compartimentering met prestatie-eis van 3 minuten inbraakwerendheid;
- CO3: Compartimentering met prestatie-eis van 5 minuten inbraakwerendheid;
- CO4: Compartimentering met prestatie-eis van 10 minuten inbraakwerendheid.

Compartimentering kan worden toegepast door middel van:

- een bouwkundig compartiment;
- een inbraakwerende kluis conform EN 14450 of EN 1143-1.

4.1 Bouwkundig compartiment

Een bouwkundig compartiment is een ruimte in een gebouw die is voorzien van een bouwkundige schil. Hierbij geldt dat voor een bouwkundig compartiment alle aanvalszijden moeten voldoen aan de prestatie-eisen zoals gesteld in hoofdstuk 3 BK – Bouwkundige maatregelen.

Aanvullend hierop geldt dat ruiten in een compartiment CO2 minimaal moeten voldoen aan de eisen voor glasvullingen weergegeven bij BK3.

4.2 Kluizen

Een kluis is geschikt voor het opbergen van attractieve en waardevolle goederen (zoals contant geld, sieraden, horloges, etc.). Een kluis die is getest door een geaccrediteerd Europees testinstituut conform EN 14450 of EN 1143-1 heeft een dekkingsadvies voor contant geld en kostbaarheden volgens de informatiekaart kluizen van de Vereniging Geld- en Waardeberging (VGW).

Het dekkingsadvies behorend bij de S1- of S2-norm of de Grade 0 t/m Grade VII of hoger, bepaalt de maximale waarde die in de kluis opgeborgen mag worden. Voor kluizen die zich bevinden binnen elektronisch beveiligd gebied met ruimtelijk werkende detectoren, mag de maximale waarde worden verdubbeld. Bij een kluis geplaatst in een CO3 of CO4 compartiment, mag de maximale waarde worden verdrievoudigd.

Brandwerende kluizen en kasten zijn in principe niet bedoeld en geschikt voor het inbraakwerend opbergen van diefstalattractieve zaken. Indien een brandwerende kast ook door een Europees geaccrediteerd testinstituut getest is conform EN-14450 en EN-1143-1, is deze kast ook geschikt om in te zetten als inbraakwerende kluis.

Vrijstaande kluizen die lichter zijn dan 1.000 kg vereisen een sterke verankering:

- Vrijstaande kluizen die onderdeel uit maken van de beveiligingsmaatregelen volgens de VRKI 2.0 en die lichter zijn dan 1.000 kg, moeten altijd worden verankerd.
- Kluizen die voldoen aan EN 14450 S1/S2 of EN 1143-1 Grade 0 moeten bij voorkeur worden verankerd door een Erkend Verankeraar Kluizen. Vereist is dat de kluis ten minste wordt verankerd volgens de instructie van de leverancier en met gebruik van de meegeleverde bevestigingsmaterialen. Soms is een betere of andere verankeringsmethode gewenst. Op basis van goed vakmanschap mag dan een andere of aanvullende bevestigingsmethode worden toegepast.
- Kluizen die voldoen aan NEN-EN 1143-1 grade 1 of hoger die na 1-1-2025 zijn geplaatst, moeten worden verankerd door een Erkend Verankeraar Kluizen. Na de verankering moet een Verankeringscertificaat A1 of A2 worden afgegeven. Als verankering volgens A1 of A2 niet mogelijk is en de kluis in redelijkheid ook niet op een andere plaats kan worden geïnstalleerd waar gecertificeerde verankering wel mogelijk is, mag de Erkend Kluis Verankeraar de verankering naar beste kunnen uitvoeren. Hierna moet een Verklaring van Verankering volgens B worden afgegeven.
- Bestaande kluizen die lichter zijn dan 1.000 kg moeten zijn verankerd. Indien voor de verankering geen Verankeringscertificaat of Verklaring van Verankering is afgegeven, moet het bouwkundig beveiligingsbedrijf de kwaliteit van de bestaande verankering vaststellen. Er moet altijd gebruik zijn gemaakt van minimaal 2 verankeringsgaten. Indien de kluis maar één verankeringsgat heeft, moeten in principe zowel de bevestigingszijde als de andere zijde van de kluis aanvullend zijn verlijmd. Indien het beveiligingsbedrijf twijfelt aan de deugdelijkheid van de verankering, moet de kluis opnieuw worden verankerd. Bij kluizen die voldoen aan EN 1143-1 grade 1 of hoger en die na 1-1-2025 opnieuw worden verankerd, moet dit door een Erkend Verankeraar Kluizen plaatsvinden en moet hiervoor een Verankeringscertificaat of Verklaring van Verankering worden afgegeven.

Meer informatie over de gecertificeerde kluisverankering is te vinden op Verankeringskaart van VGW:
https://geldenwaardeberging.nl/wp-content/uploads/2021/03/VGW-Verankeringskaart_1.1.pdf.

4.3 Inbraaksignaleringsysteem bij bouwkundige compartimenten & kluizen

Een bouwkundig compartiment of kluis is bestemd voor het opbergen van goederen of zaken die voor inbrekers zeer attractief zijn. De beveiligingstheorie is er daarom op gericht om een inbraak in het gebouw te detecteren, nog voor het bouwkundig compartiment of kluis wordt bereikt of aangevallen. Het betekent dat een bouwkundig compartiment en/of kluis altijd moet worden gecombineerd met een inbraaksignaleringsysteem in het gebied buiten het bouwkundig compartiment of kluis. Hierbij moet de beveiliging zich uitstrekken tot alle aanvalszijden van het bouwkundig compartiment of de kluis.

Als door het volume van een bouwkundig compartiment de kans bestaat op insluiting, is de ruimtelijke detectie ook in het bouwkundig compartiment verplicht. Als een bouwkundig compartiment direct achter de schil is gesitueerd of deel uitmaakt van de buitenschil, is schildetectie verplicht. Openstand detectie op de toegangsdeur(en), geldt voor elk bouwkundig compartiment.

Voor deuren van kluizen is openstand detectie geen eis. Zie hoofdstuk 6, inbraaksignalering.

Indien de kluis tegen een buitenmuur is geplaatst moet deze zijn voorzien van seismische detectie.

5. ME - Meeneembeperkende maatregelen

Onder de ME-maatregelen vallen de meeneembeperkende maatregelen die de zichtbare drempel voor de inbreker zo hoog mogelijk legt.

In de tabellen met combinaties van beveiligingsmaatregelen voor woningen en bedrijven in VRKI 2.0 deel A worden de niveaus van meeneembeperkende maatregelen aangeduid met de letter ME en een cijfer. Dit cijfer heeft betrekking op de zwaarte van het niveau van de ME-maatregelen.

Er zijn vier niveaus aan ME-maatregelen:

- ME1: Meeneembeperkende maatregel waarvan geen prestatie-eis voor diefstalvertraging is bepaald;
- ME2: Meeneembeperkende maatregel met prestatie-eis van 3 minuten diefstalvertraging;
- ME3: Meeneembeperkende maatregel met prestatie-eis van 5 minuten diefstalvertraging;
- ME4: Meeneembeperkende maatregel met prestatie-eis van 10 minuten diefstalvertraging.

Voor de meeneembeperkende maatregelen wordt een beroep gedaan op het inlevingsvermogen van iedere adviseur, ondernemer en/of particulier. De mogelijkheden van vormgeving, uiterlijk, materiaaltoepassing en gebruikersgemak zijn oneindig. Er zijn slechts enkele standaardoplossingen. Een installateur kan dit op basis van goed vakmanschap per situatie beoordelen.

Opmerking hierbij is dat waar voor het ten uitvoer brengen van een maatregel producten nodig zijn, deze bij voorkeur zijn getest en goedgekeurd op basis van de SKG-KE470.

5.1 ME1 niveau

Aan niveau ME1 is geen prestatie-eis of voorbeeld gekoppeld, dit gaat naar eigen inzicht van particulier of ondernemer met winkel/showroom of magazijn/opslag. Een adviseur kan op basis van goed vakmanschap per situatie beoordelen of ME1 in zijn beveiligingsplan toegevoegde waarde heeft.

5.2 ME2 niveau prestatie-eis 3 minuten diefstalvertraging

5.2.1 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 dient uitsluitend voor enkele kleine gevallen, omdat de praktijk ook uitwijst dat de inbreker vaak zeer brutaal is en/of met meer personen 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 onmogelijk. Wél is het zaak om de heftruck na sluitingstijd onbruikbaar te maken. Niet zelden komt het voor dat de inbreker het eigen expeditie voertuig, welke soms al geladen staat met attractieve goederen, gebruikt voor de afvoer. Meeneembeperkende 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.

5.2.2 Koppelen

Eigen gebruik

Ook producten voor eigen gebruik kunnen attractief zijn en snel worden meegenomen. Soms kunnen deze worden gekoppeld en op deze manier minder interessant gemaakt worden voor diefstal. Zie hiervoor de aanbevelingen Meeneembeperkende Producten op basis van SKG-KE 470.

Winkel of showroom

Door duurdere fietsen, scooters en/of bromfietsen onderling te koppelen met beugel sloten (eigen verkoop) en/of geplastificeerde staalkabels wordt snelkraak voorkomen. Een goed zichtbare drempel werkt op deze manier met name overdag zeer preventief.

Magazijn of opslag

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

5.2.3 Verankeren

Eigen gebruik

Goederen kunnen worden verankerd en tegen snelkraak worden beschermd door het vastzetten met bijvoorbeeld een chemisch anker of keilbout. Zo zijn er ook speciale bevestigingen te koop 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 gewenst effect beoogd. 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.

5.3 ME3 niveau prestatie-eis 5 minuten diefstalvertraging

5.3.1 Kisten of kasten

Eigen gebruik

Een aannemersbedrijf kan na werktijd zijn elektrisch gereedschap verzamelen in een inbraakwerende kist of kast, om inbraak en snelkraak te voorkomen. Let wel op dat deze zelf goed wordt verankerd en dat de kist de prestatie-eis van 5 minuten haalt. Evenals het hang- en sluitwerk dat op niveau BK3 moet zijn. 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 zijn, zoals navigatie - en sonarsystemen, kunnen in een goed afsluitbare houten of stalen kast worden geborgen die deel uitmaakt van de stellingwanden. De kast moet de prestatie-eis van 5 minuten halen, evenals het hang- en sluitwerk dat op niveau BK3 moet zijn. Een getest inbraakwerend rolluik met prestatie-eis 5 minuten volgens de NCP/Romazo matrix volstaat ook. Door deze kast overdag 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 geschikte afsluitbare houten (met staal verstevigd en verlijmd multiplex 38 mm) of stalen

kasten. Het hang- en sluitwerk hiervan moet voldoen aan niveau BK3, evenals de bevestiging van bijvoorbeeld de overvalsluiting voor een hangslot. Standaard zwaardere archiefkasten of kluisen kunnen veelal dienst doen als opslag van inbraakgevoelige goederen.

5.3.2 Vitrines

Eigen gebruik

Een vitrine is in deze situatie eigenlijk geen optie of het betreft een verzameling 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 polycarbonaat en/of gelaagde beglazing (norm NEN-EN 356), in een geschikt kader, met goed sluitwerk, kan een beveiligde vitrine worden gerealiseerd. Veelal is het een eigen fabrikaat of zal de inventiviteit van een vitrinebouwer hierbij doorslaggevend zijn.

Magazijn of opslag

Niet van toepassing.

5.3.3 Hekwerken

Eigen gebruik

Een bedrijf kan attractieve goederen eenvoudig tegen snelkraak beschermen door hiervoor na sluitingstijd consequent een raster of hekwerk te plaatsen en af te sluiten. Zo moet muziekapparatuur bijvoorbeeld niet worden onderschat qua attractiviteit en vervangingskosten, bijvoorbeeld in een café.

Winkel of showroom

Een inpandig rolluik, rol- of schaarhek 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 overdag helpen te 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 schappen gedeelte 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 iedereen zomaar een kijkje in de keuken kan nemen. Als aandachtspunt geldt dat rekening moet worden gehouden met vluchtwegen.

5.4 ME4 niveau prestatie-eis 10 minuten diefstalvertraging

Meeneembeperkende maatregelen binnen niveau ME4 moeten voldoen aan 10 minuten diefstalvertraging. Voor mistgeneratoren geldt dat binnen 10 seconden het zicht beperkt is tot ten hoogste 30 cm, waarbij de mist minimaal 20 minuten blijft hangen. Voor de regels omtrent mistgeneratoren wordt verwezen naar het vigerende document D01-026 Installatievoorschriften mistgeneratoren.

5.4.1 Mistgeneratoren

Eigen gebruik

Een kostbare particuliere inboedel of een 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.

Winkel of showroom

Een winkel, met bijvoorbeeld parfumerie, telefonie en/of ander zeer attractief kleingood, kan met mistgeneratoren worden beveiligd. Helaas is er vaak geen sprake van een duidelijke zichtbare en fysieke drempel, zoals een rolluik en/of hekwerk. Echter, de effectiviteit van een beveiliging met mistgeneratoren is 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.

6. EL - Elektronische maatregelen

In de tabellen met beveiligingsmaatregelen in deel A van de VRKI 2.0 worden de elektronische maatregelen voor woningen en bedrijven aangeduid met de letters EL en een cijfer. Het cijfer heeft hierbij betrekking op de omvang en het niveau van deze maatregelen.

6.1 Omvang elektronische maatregelen

In het op te stellen beveiligingsplan moet 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 de attractieve goederen zich bevinden.

6.1.1 Substelsysteem

In een inbraaksignaleringsstelsysteem kunnen componenten van verschillende grades (zie 6.3.1) worden toegepast indien het inbraaksignaleringsstelsysteem is verdeeld in duidelijk te onderscheiden subsystemen. In dat geval kunnen de subsystemen een verschillende grade hebben. De grade van een subsysteem is die van de component met de laagste grade binnen het subsysteem. Componenten die deel uitmaken van meer dan één subsysteem moeten een grade hebben die gelijk is aan die van het subsysteem met de hoogste grade, bijvoorbeeld centrale controle- en stureeenheid (CCS) en alarmtransmissiesysteem (ATS).

De CCS moet zich binnen het beveiligd gebied bevinden. Wanneer een inbraaksignaleringsstelsysteem is verdeeld in subsystemen met verschillende grades moet de CCS zich bevinden in het beveiligd gebied van het subsysteem met de hoogste grade.

Bij inbraaksignaleringsstelsystemen grade 3 moet bij inschakeling van een subsysteem altijd tevens het subsysteem worden ingeschakeld dat het gebied beveiligt waarin de CCS zich bevindt.

6.2 Ontwerp, aanleg & onderhoud

De alarminstallatie moet ontworpen worden conform de eisen van dit document. De aanleg en het onderhoud vinden plaats volgens de voorschriften:

- Installatievoorschriften voor alarmapparatuur (document 002080, vigerende versie)
- Voorschriften beheer en onderhoud alarmapparatuur (document 002079, vigerende versie)

Er moet gebruik worden gemaakt van een op het risico afgestemde detectie. De status van de alarminstallatie mag buiten het beveiligd gebied niet door onbevoegden afleesbaar zijn.

6.3 Eisen aan alarmapparatuur

De toegepaste componenten moeten voldoen aan de eisen gesteld in de Europese normen: NEN-EN 50131-1 vigerende versie, inclusief addendum & NEN-EN 50136-1 vigerende versie, inclusief addendum. De componenten worden in deze normen gekoppeld aan zogenoemde security grades. Bij deze security grades wordt uitgegaan van het niveau van de aanvaller.

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

Daarnaast moeten de gebruikte componenten geschikt zijn voor de heersende omgevingsomstandigheden.

6.3.1 Security grades

De security grades maken een risico-inschatting van het niveau van de aanvaller.

Opmerking

Let bij het gebruik van de security grades op, dat het begrip grades tweeledig is. Enerzijds wordt hiermee een risico-inschatting gemaakt van het niveau van de aanvaller, zoals hieronder beschreven. Daarnaast worden er ook de componenten mee bedoeld, zoals gedefinieerd in tabel 6.1.

Grade 1 (laag risico): Verwacht wordt dat aanvallers weinig kennis hebben van detectiesystemen, en het gebruik van hulpmiddelen is gelimiteerd tot een beperkte set standaard gereedschappen.

Grade 2 (laag tot gemiddeld risico): Verwacht wordt dat aanvallers gelimiteerde kennis hebben van detectiesystemen en gebruik zullen maken van vrij verkrijgbare gereedschappen en draagbare apparatuur.

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

Grade 4 (hoog risico): Wanneer beveiliging voorrang heeft op alle andere factoren. Verwacht wordt dat aanvallers de middelen of het vermogen hebben alles tot in detail voor te bereiden en de beschikking hebben over een volledige set gereedschappen/ apparatuur inclusief mogelijkheden om vitale componenten van een detectiesysteem te vervangen.

Tabel 6.1 laat zien hoe de security grades zich verhouden ten opzichte van de verschillende niveaus van elektronische maatregelen.

TABEL 6.1 – SECURITY GRADES				
	niveau EL1	niveau EL2	niveau EL3*	niveau EL4
Grade	Grade 2	Grade 2	<ul style="list-style-type: none"> ■ Woningen: Grade 2 ■ Bedrijven: Grade 2 of 3 	Grade 3

* Bij niveau EL 3 is security Grade 2 of 3 van toepassing. De ruimtelijk werkende detectoren zijn grade 3 (type anti-masking). Voor woningen is dit geen eis.

6.3.2 Environmental classes

Voor toepassing van apparatuur is ook de omgeving waarin deze moet worden geplaatst van belang. Hiervoor dienen de environmental classes te worden toegepast.

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)

6.3.3 Inbraaksignaleringsystemen bedraad of draadloos

Inbraaksignaleringsystemen zijn over het algemeen volledig bedrade systemen, maar mogen in sommige gevallen ook draadloos worden toegepast. Tabel 6.2 geeft dit per EL-niveau weer.

TABEL 6.2 – BEDRAAD OF DRAADLOOS				
	niveau EL1	niveau EL2	niveau EL3	niveau EL4
Inbraaksignaleringsysteem bedraad	Woningen: Toegestaan	Woningen: Toegestaan	Woningen: Toegestaan	Woningen: Toegestaan
	Bedrijven: Toegestaan	Bedrijven: Toegestaan	Bedrijven: Toegestaan	Bedrijven: Toegestaan
Inbraaksignaleringsysteem draadloos	Woningen: Toegestaan	Woningen: Toegestaan	Woningen: Toegestaan	Woningen: Niet Toegestaan
	Bedrijven: Toegestaan	Bedrijven: Toegestaan	Bedrijven: Niet Toegestaan	Bedrijven: Niet Toegestaan

Extra eisen bij toepassing van draadloze alarmapparatuur:

- Bij aansluiting op een PAC is doormelding van de beheers- en communicatiemeldingen verplicht. De PAC moet op deze meldingen van een geactiveerd systeem reageren als bij een sabotagemelding. Er moet een schriftelijke overeenkomst met gebruiker en/of installateur zijn. Hierin is vastgelegd dat deze meldingen zo spoedig mogelijk aan klant en/of installateur worden doorgegeven om ervoor te zorgen dat zij adequate maatregelen treffen.
- De levensduur van een batterij moet worden bepaald aan de hand van de te verwachten activeringen. Batterijen moeten van een door de fabrikant voorgeschreven type zijn. Een batterij “laag” signaal moet vooraf door het systeem lokaal worden aangegeven. Indien de batterij niet tijdig wordt vervangen moet dit als laatste worden doorgemeld naar de PAC.

6.3.4 In- en uitschakelen

Het in- en uitschakelen van het inbraaksignaleringsstelsel mag op verschillende manieren. Hieronder staan de verschillende mogelijkheden weergegeven.

TABEL 6.3 – MOGELIJKHEDEN IN- EN UITSCHAKELEN				
	EL1	EL2	EL3	EL4
Een codebedienpaneel met een pincode	✓	✓	✓	✓
Een kaartlezer voor gebruik van een tag, pas, smartphone met NFC functie	✓	✓		
Een afstandsbediening	✓			
Een afstandsbediening verstrekt door de fabrikant van de CCS	✓	✓		
Een app op een smartphone	✓	✓		
Een kaartlezer voor gebruik van een tag, pas, smartphone met NFC functie i.c.m. codebedienpaneel met een pincode	✓	✓	✓	✓

6.4 Niveaus van elektronische maatregelen

Er zijn vier niveaus van elektronische maatregelen. Hierna volgen de omschrijvingen van de eisen waaraan de elektronische maatregelen moeten voldoen per EL-niveau.

6.4.1 Minimale eisen inbraaksignaleringsstelsel

Niveau EL2 wordt gebruikt als basis voor de elektronische inbraaksignaleringsstelsels voor woningen en utiliteitsgebouwen. Hierbij geldt voor alle niveaus, op EL1 na, dat de alarminstallatie te allen tijde op een erkende PAC moet worden aangesloten.

EL1 is dus een uitzondering op deze regel. In bepaalde gevallen kunnen er voor gebruikers en verzekeraars namelijk redenen zijn om genoegen te nemen met een inbraaksignaleringsstelsel zonder aansluiting op een PAC. Hierbij geldt wel dat aansluiting op een PAC in een later stadium altijd mogelijk moet blijven.

TABEL 6.4 – MINIMALE EISEN INBRAAKSIGNALERINGSSYSTEEM				
Eis	Niveau EL 1	Niveau EL 2	Niveau EL 3	Niveau EL4
Gebruik gecertificeerde componenten	Verplichting ontwerper en installateur	Verplichting ontwerper en installateur	Verplichting ontwerper en installateur	Verplichting ontwerper en installateur
Doormelding naar:	Bij bedrijven (mobiele) telefoon	PAC	PAC	PAC
Optische*/akoestische alarmgevers	Akoestisch alarm en optische alarmering verplicht	Akoestisch alarm en optische alarmering verplicht	Akoestisch alarm en optische alarmering verplicht	Akoestisch alarm en optische alarmering verplicht
Ruimtelijk werkende detectoren type anti-masking**	N.v.t.	N.v.t.	Woningen: Geen Bedrijven: Eis	Woningen: Eis Bedrijven: Eis
Onderhoudsstelsel	Ten minste één onderhoudsbeurt per jaar	Ten minste één onderhoudsbeurt per jaar	Ten minste één onderhoudsbeurt per jaar	Ten minste één onderhoudsbeurt per jaar

* Optische alarmgevers hoeven niet gecertificeerd te zijn. Als het te beveiligen object zodanig is gesitueerd dat het voor derden onmogelijk is om de optische indicatie waar te nemen, kan het toepassen daarvan achterwege blijven.

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

Daarnaast moeten akoestische alarmgevers binnen het gebouw zodanig zijn geplaatst dat binnen het beveiligde gebied het geluid duidelijk waarneembaar is. Met duidelijk wordt bedoeld een minimale geluidssterkte van 60 dB(A), gemeten ter plaatse waar de attractieve goederen zich normaliter bevinden. Dit is ook van toepassing op een sabotagealarm als het inbraaksignaleringsysteem is ingeschakeld.

Bij sabotage van een luid-alarmgever moet minimaal één tweede alarmgever blijven functioneren (tenzij alarmgevers gelijktijdig worden gesaboteerd). Het voorgaande is ook van toepassing bij deel-inschakeling van het inbraaksignaleringsysteem.

In de praktijk betekent dit dat er binnen minimaal 2 luid-alarmgevers moeten zijn geïnstalleerd die ieder op een apart gezekerde sirene-uitgang van de CCS 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 risicoklasse 1. Hier kan worden volstaan met één luid-alarmgever. In de overige risicoklassen kan de installateur, in situaties waarbij één kleine ruimte beveiligd wordt, op basis van goed vakmanschap afwijken en volstaan met één luid-alarmgever binnen.

6.4.2 Minimale eisen omvang projectie

Voor de omvang van de projectie is een minimaal eisenpakket vastgesteld. De omvang van de projectie moet worden vastgelegd in een beveiligingsplan. Zie ook definitie beveiligingsplan Hoofdstuk 1.

In het op te stellen beveiligingsplan wordt bepaald welke typen detectoren in welke ruimten en op welke plaatsen moeten worden aangebracht. Dit zijn in principe alle ruimten die voor een inbreker bereikbaar zijn. De bereikbaarheid van dak- en gevelementen wordt bepaald aan de hand van NEN 5087. Ondanks dat deze norm in basis is bedoeld voor woningen, moet deze norm binnen de VRKI, voor alle te beveiligen objecten (ook voor bedrijven, winkels, scholen ect.) worden toegepast.

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 voor vroegtijdige detectie.

Uit het voorgaande volgt dat het gedetecteerde 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.

De ruimtes die van het bewaakte gebied worden uitgezonderd van detectie moeten in het intakedocument en het beveiligingsplan worden toegelicht en vastgelegd. Deze uitzondering geldt uitsluitend voor ruimtes met goederen attractiviteit laag en bij woningen voor ruimten waar zich geen attractieve zaken van de inboedel bevinden.

6.4.2.1 Niveau EL1 Omvang projectie minimale eisen

Ruimte detectie:

- In alle bereikbare ruimten met vaste en/of beweegbare gevelopeningen; en
- Op plaatsen waar zich attractieve goederen bevinden; en
- Op strategische plaatsen in het pand voor vroegtijdige detectie; en
- Voordat de CCS* en de daartoe behorende delen (input/output) kunnen worden bereikt; en
- Voordat de alarmoverdrager en de bij het alarmtransmissiepad behorende delen kunnen worden bereikt; en
- Ter plaatse van de bediendelen; en
- In ruimten met een waardeberging (Alle zijden van de waardeberging moeten worden gedetecteerd); en
- In ruimten waar meeneem beperkende maatregelen zijn toegepast; en
- In een compartiment als de kans op insluiting bestaat.

** Bij bedrijven - (en woningen met uitzondering van risicoklasse 1) - moet de CCS en de alarmoverdrager, altijd worden geplaatst in een met sleutel afsluitbare kast (meterkast o.i.d.) waarbij de desbetreffende deur dient te worden voorzien van NIET VERTRAAGDE openstanddetectie.*

Openstand detectie:

- Op de entreedeuren** van het pand; en
- Op rolluiken, rolhekken en schaarhekken met een beveiligingsfunctie.

** Met entreedeuren 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 in- en uitlooptijd aan.

6.4.2.2 Niveau EL2 Omvang projectie minimale eisen

Ruimte detectie:

- In alle bereikbare ruimten met vaste en/of beweegbare gevelopeningen; en
- Op plaatsen waar zich attractieve goederen bevinden; en
- Op strategische plaatsen in het pand voor vroegtijdige detectie; en
- Voordat de CCS* en de daartoe behorende delen (input/output) kunnen worden bereikt; en
- Voordat de alarmoverdrager en de bij het alarmtransmissiepad behorende delen kunnen worden bereikt; en
- Ter plaatse van de bediendelen; en
- In ruimten met een waardeberging (Alle zijden van de waardeberging moeten worden gedetecteerd); en
- In ruimten waar meeneem beperkende maatregelen zijn toegepast; en
- In een compartiment als de kans op insluiting bestaat.

** Bij bedrijven - (en woningen met uitzondering van risicoklasse 1) - moet de CCS en de alarmoverdrager, altijd worden geplaatst in een met sleutel afsluitbare kast (meterkast o.i.d.) waarbij de desbetreffende deur dient te worden voorzien van NIET VERTRAAGDE openstand detectie.*

Openstand detectie:

- Op de entreedeuren** van het pand; en
- Op de nooduitgangen*** van het pand; en
- Op rolluiken, rolhekken en schaarhekken met een beveiligingsfunctie.; en
- Op de deur(en) van compartimenten; en
- Op de deur(en) waar achter de CCS is opgesteld (niet vertraagde openstand detectie); en
- Op de deur(en) waar achter de alarmoverdrager en de daartoe behorende delen zijn opgesteld.

** Met entreedeuren 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 in- en uitlooptijd aan.

**** Met nooduitgangen worden de nooduitgangen bedoeld die door middel van een vluchtwegaanduiding als zodanig herkenbaar zijn. Voor overige deuren wordt geadviseerd om deze aan de buitenzijde te voorzien van blind bouwbeslag om bedieningsfouten te voorkomen.*

Seismische detectie:

- Als een kluis tegen een buitenmuur of scheidingswand naar derden staat opgesteld.

6.4.2.3 Niveau EL3 Omvang projectie minimale eisen

Ruimte detectie:

- In alle bereikbare ruimten met vaste en/of beweegbare gevelopeningen; en
- Op plaatsen waar zich attractieve goederen bevinden; en
- Op strategische plaatsen in het pand voor vroegtijdige detectie; en
- Voordat de CCS* en de daartoe behorende delen (input/output) kunnen worden bereikt; en
- Voordat de alarmoverdrager en de bij het alarmtransmissiepad behorende delen kunnen worden bereikt; en
- Ter plaatse van de bediendelen; en
- In ruimten met een waardeberging (Alle zijden van de waardeberging moeten worden gedetecteerd); en
- In ruimten waar meeneem beperkende maatregelen zijn toegepast; en
- In een compartiment als de kans op insluiting bestaat.

** Bij bedrijven - (en woningen met uitzondering van risicoklasse 1) - moet de CCS en de alarmoverdrager, altijd worden geplaatst in een met sleutel afsluitbare kast (meterkast o.i.d.) waarbij de desbetreffende deur dient te worden voorzien van NIET VERTRAAGDE openstand detectie.*

Openstand detectie:

- Op de entreedeuuren** van het pand; en
- Op de nooduitgangen*** van het pand; en
- Op de bereikbare ramen en deuren in de buitenschil van het pand, mits niet mechanisch beschermd; en
- Op rolluiken, rolhekken en schaarhekken, met een beveiligingsfunctie.; en
- Op de deur(en) van compartimenten; en
- Op de deur waar achter de CCS is opgesteld (niet vertraagde openstand detectie); en
- Op de deur(en) waar achter de alarmoverdrager en de daartoe behorende delen zijn opgesteld.

*** Met entreedeuuren 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 in- en uitlooptijd aan.*

**** Met nooduitgangen worden de nooduitgangen bedoeld die door middel van een vluchtwegaanduiding als zodanig herkenbaar zijn. Voor overige deuren wordt geadviseerd om deze aan de buitenzijde te voorzien van blind bouwbeslag om bedieningsfouten te voorkomen.*

Seismische detectie:

- Als een kluis tegen een buitenmuur of scheidingswand naar derden staat opgesteld.

Schildetectie:

SD2 is verplicht:

- Bij bedrijven indien compartimentering en/of meeneembeperkende maatregelen niet zijn uitgevoerd; en/of
- Als een compartiment direct achter de schil is gesitueerd of deel uitmaakt van de buitenschil.

SD4 kan worden toegepast als SD2 (gedeeltelijk) niet mogelijk is.

6.4.2.4 Niveau EL4 Omvang projectie minimale eisen

Ruimte detectie:

- In alle bereikbare ruimten met vaste en/of beweegbare gevelopeningen; en
- Op plaatsen waar zich attractieve goederen bevinden; en
- Op strategische plaatsen in het pand voor vroegtijdige detectie; en
- Voordat de CCS* en de daartoe behorende delen (input/output) kunnen worden bereikt; en
- Voordat de alarmoverdrager en de bij het alarmtransmissiepad behorende delen kunnen worden bereikt; en
- Ter plaatse van de bediendelen; en
- In ruimten met een waardeberging (Alle zijden van de waardeberging moeten worden gedetecteerd); en
- In ruimten waar meeneem beperkende maatregelen zijn toegepast; en
- In een compartiment als de kans op insluiting bestaat.

** Bij bedrijven - (en woningen met uitzondering van risicoklasse 1) - moet de CCS en de alarmoverdrager, altijd worden geplaatst in een met sleutel afsluitbare kast (meterkast o.i.d.) waarbij de desbetreffende deur dient te worden voorzien van NIET VERTRAAGDE openstand detectie.*

Openstand detectie:

- Op de entreedeuken** van het pand; en
- Op de nooduitgangen*** van het pand; en
- Op de bereikbare ramen en deuren in de buitenschil van het pand, mits niet mechanisch beschermd; en
- Op rolluiken, rolhekken en schaarhekken, met een beveiligingsfunctie.; en
- Op de deur(en) van compartimenten; en
- Op de deur waar achter de CCS is opgesteld (niet vertraagde openstand detectie); en
- Op de deur(en) waar achter de alarmoverdrager en de daartoe behorende delen zijn opgesteld.

*** Met entreedeuken 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 in- en uitlooptijd aan.*

**** Met nooduitgangen worden de nooduitgangen bedoeld die door middel van een vluchtwegaanduiding als zodanig herkenbaar zijn. Voor overige deuren wordt geadviseerd om deze aan de buitenzijde te voorzien van blind bouwbeslag om bedieningsfouten te voorkomen.*

Seismische detectie:

- Als een kluis tegen een buitenmuur of scheidingswand naar derden staat opgesteld.

Schildetectie:

SD3 is verplicht:

- Bij bedrijven indien compartimentering en/of meeneembepaalde maatregelen niet zijn uitgevoerd; en/of
- Als een compartiment direct achter de schil is gesitueerd of deel uitmaakt van de buitenschil.

SD4 kan worden toegepast als SD3 (gedeeltelijk) niet mogelijk is.

6.4.3 Eisen schildetectie¹

Als een compartiment direct achter de schil is gesitueerd of deel uitmaakt van de buitenschil, is schildetectie verplicht.

Voor het functioneren van schildetectie is het van belang dat:

- De verschillende componenten van schildetectie aansluiten op het inbraaksignaleringssysteem (compatibiliteit);
- De verschillende componenten passen bij de omgevingsinvloeden die van toepassing zijn conform de NEN-EN 50131-1 en IP klasse;

Er zijn vier niveaus van schildetectie te onderscheiden:

- SD1 voor woningen: De schildetectie bestaat uit openstand detectie op, voor inbrekers bereikbare, beweegbare gevelelementen. Deze keuzeoptie is met name bedoeld om binnen de woning vrij te kunnen bewegen als de ruimtelijk werkende detectoren niet actief zijn. De keuze voor schildetectie niveau SD1 is optioneel.
- SD1 voor bedrijven: De schildetectie bestaat uit openstand detectie op nooduitgangen in combinatie met een optische en/of akoestische signalering en alarmering om ongewenst gebruik van nooduitgangen in de dag situatie te signaleren. Het alarmeren mag op iedere gewenste wijze plaatsvinden.
- SD2 bestaat uit detectie, met als doel inbraaksignalering bij de eerste aanval op vaste en beweegbare gevelelementen van of voor, de periferie van ruimten waar de attractieve goederen zich bevinden. SD2 kan op meerdere wijze worden gerealiseerd: bijvoorbeeld glasbreukdetectie en trillingsdetectie op de gevelelementen van de ruimten. Voor de bereikbaarheid van gevelelementen welke zich aan de buitengevel bevinden moet de NEN-5087 worden gebruikt.
- SD3 zie SD2 met als aanvulling dat (bereikbare) wanden, vloeren en daken zijn voorzien van geschikte detectie.
- SD4 bestaat uit buitendetectie rond een object. SD4 is een alternatief voor SD2 of SD3 wanneer SD2 of SD3, mits onderbouwd, niet volledig te realiseren is. SD4 kan dan een vervanging zijn voor dat deel wat niet middels SD2 of SD3 te realiseren is.

Schildetectie niveau SD4 kan op de volgende wijze worden gerealiseerd: detectiesysteem op terrein(grenzen) in combinatie met een camerasysteem met video analytics. De camerabeelden moeten worden doorgemeld naar de PAC.

Met Live View kan de meldkamer van de politie rechtstreeks meekijken met de camerabeelden van een winkelier of ondernemer. Zo is die direct op de hoogte als er een inbraak of overval (of ander gewelddadig delict) wordt gepleegd.

6.5 transmissiesysteem

Zodra de alarminstallatie in alarm komt, dat wil zeggen dat één of meerdere detectoren in het bewaakte gebied de alarmstatus bereiken, moet alarmering plaatsvinden. Het alarmsignaal moet via de alarmoverdrager worden gezonden naar een PAC. De verbinding daarnaar is het alarmtransmissienetwerk. De eisen daaraan zijn opgenomen in hoofdstuk 7: "Alarmtransmissie".

¹ Schildetectie: Zie ook Handreiking beveiligingsmaatregelen voor buitenterreinen mobiliteitsbedrijven en Handreiking beveiligingsmaatregelen voor buitenterreinen transport en logistiek. (Verbond van Verzekeraars)

7. AT – Alarmtransmissie

Het alarmtransmissiesysteem moet gebruikmaken van een veilig en betrouwbaar netwerk. Transmissie start op het moment dat een alarm wordt gesignaleerd en loopt door tot het moment dat het signaal wordt ontvangen in de meldkamer. Onderstaande figuur 7.1 geeft schematisch weer hoe dit met elkaar in verhouding staat en waar de verantwoordelijkheden liggen.



Figuur 7.1

De VRKI 2.0 gaat uit van vier alarmtransmissie (AT) niveaus. Hierbij is een aansluiting gemaakt met de indeling in ATS-categorieën en Security Grades die worden gehanteerd in de Nationale en Europese normen, tabel 7.1. Niveau AT1 is niet in de tabel opgenomen.

TABEL 7.1 - ALARMTRANSMISSIENIVEAUS			
	Niveau AT2	Niveau AT3	Niveau AT4
ATS-categorie	SP2/DP1	DP3	DP4
Security Grade	Grade 2	Grade 3	Grade 3
Ontvangst PAC	T2	T4	T5

7.1 Toelichting op Normering

De functionele eisen aan inbraaksignaleringsystemen zijn afgeleid van de Europese en ook in Nederland gehanteerde normen:

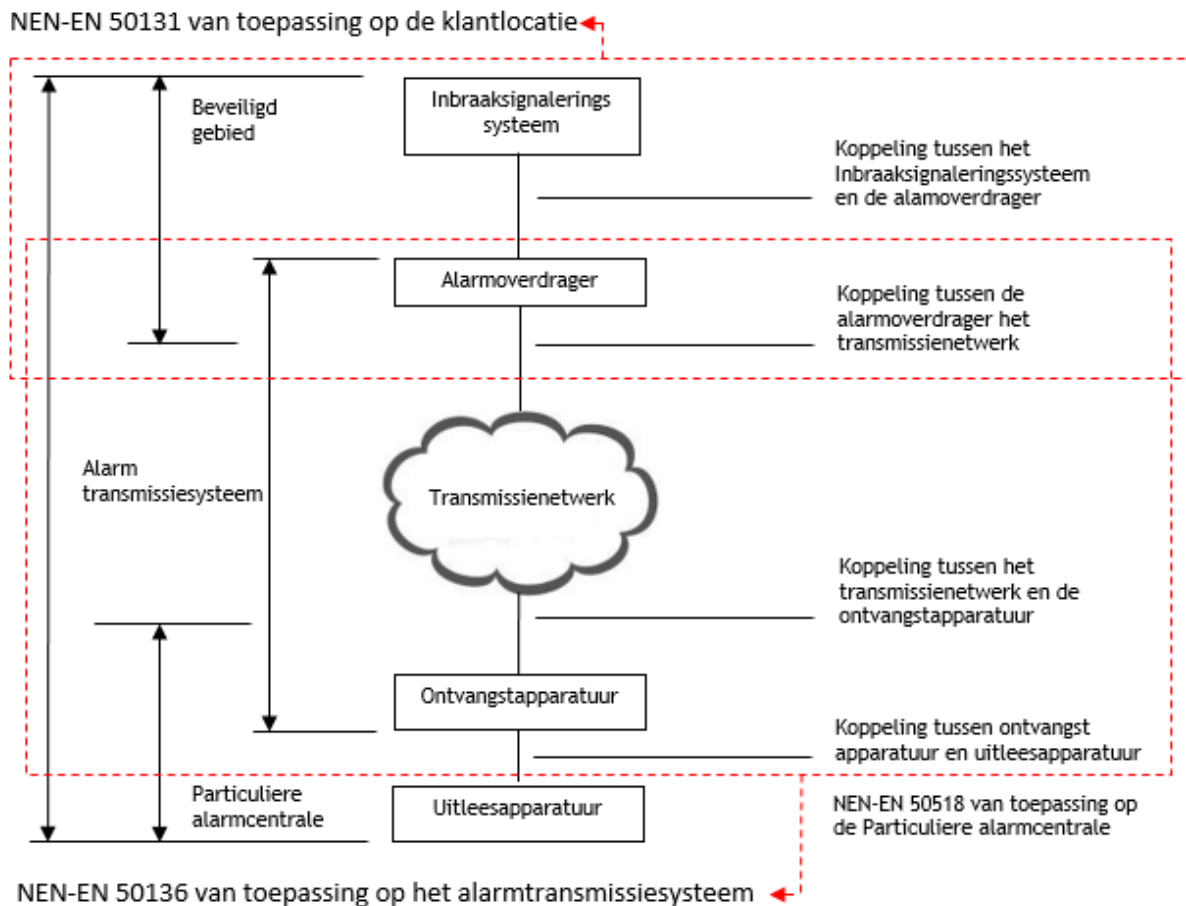
- NEN-EN 50131-1 Alarmsystemen, inbraak- en overvalsystemen, deel 1: systeemeisen;
- NEN-EN 50136-1 Alarmsystemen, alarmtransmissiesystemen en -apparatuur, deel 1: algemene eisen voor alarmtransmissiesystemen.

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 moeten voldoen.

In de NEN-EN 50136-1 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.

Figuur 7.2 geeft schematisch de relatie tussen de NEN-EN 50131 en NEN-EN 50136 weer.



Figuur 7.2: relatie tussen NEN-EN 50131 en NEN-EN 50136

7.2 Vereiste alarmtransmissiewegen

De VRKI 2.0 gaat uit van vier verschillende alarmtransmissieniveaus: AT1, AT2, AT3 en AT4. Aan deze vier niveaus worden verschillende eisen gesteld.

7.2.1 Alarmtransmissieniveau AT1 (alleen toepasbaar bij risicoklasse 1)

Bij een alarmsituatie moet binnen het gebouw een akoestisch alarm worden gegenereerd. Daarnaast moet er optische alarmering aanwezig zijn, die goed zichtbaar is vanaf de openbare weg. Akoestische alarmgevers binnen moeten zodanig zijn geplaatst dat binnen het beveiligde gebied en in slaapvertrekken het geluid duidelijk waarneembaar is. Met duidelijk wordt bedoeld een minimale geluidssterkte van 60 dB(A). Dit is ook van toepassing op een sabotagealarm.

Met betrekking tot de alarmering kan worden gekozen uit:

Woningen:

- Een luidalarminstallatie én een optische alarmering zonder doormelding;
- Een luidalarminstallatie én een optische alarmering aangevuld met een doormelding naar een (mobiele) telefoon (spraak, sms, of push-bericht). Voor een adequate alarmopvolging is het belangrijk dat deze (mobiele) telefoon bereikbaar is. Er is geen garantie of controle dat de melding tijdig de alarmopvolger bereikt. Ook kan de melding in een voicemail terecht komen.

Bedrijven:

- Een luidalarminstallatie én een optische alarmering aangevuld met een doormelding naar een (mobiele) telefoon (spraak, sms, of push-bericht). Voor een adequate alarmopvolging is het belangrijk dat deze (mobiele) telefoon bereikbaar is. Er is geen garantie of controle dat de melding tijdig de alarmopvolger bereikt. Ook kan de melding in een voicemail terechtkomen.

Opmerking

Als het te beveiligen object zodanig is gesitueerd dat het voor derden onmogelijk is om de optische indicatie waar te nemen, kan het toepassen daarvan achterwege blijven.

7.2.2 Alarmtransmissieniveau AT2

Bij een alarmsituatie moet binnen het gebouw een akoestisch alarm worden gegenereerd. Daarnaast moet er optische alarmering aanwezig zijn, die goed zichtbaar is vanaf de openbare weg.

Akoestische alarmgevers moeten binnen het gebouw zodanig zijn geplaatst dat binnen het beveiligde gebied het geluid duidelijk waarneembaar is. Met duidelijk wordt bedoeld een minimale geluidssterkte van 60 dB(A), gemeten ter plaatse waar de attractieve goederen zich normaliter bevinden. Dit is ook van toepassing op een sabotagealarm als het inbraaksignaleringsysteem is ingeschakeld. Bij sabotage van een luid-alarmgever moet minimaal één tweede alarmgever blijven functioneren (tenzij alarmgevers gelijktijdig worden gesaboteerd). Het voorgaande is ook van toepassing bij deel-inschakeling van het inbraaksignaleringsysteem.

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 risicoklasse 1. Hier kan worden volstaan met één luid-alarmgever. In de overige risicoklassen kan de installateur in situaties waarbij één kleine ruimte beveiligd wordt op basis van goed vakmanschap afwijken en volstaan met één luid-alarmgever.

Met betrekking tot de alarmering moet voor het versturen van de alarmmelding de ATS-categorie SP2 of DP1 worden toegepast. De alarmoverdracht moet geschieden naar een PAC. Minimaal één keer per 25 uur moet ook een controlemelding vanuit de CCS plaatsvinden.

Aanvullend vereist bij gebruik IP met enkelvoudige verbinding (SP)

Toepassing van extra netwerkcomponenten tussen de alarmoverdrager en IS-RA punt is toegestaan indien deze componenten zijn geplaatst in een beveiligde ruimte en – voor zover stroom verbruikend - zijn voorzien van een noodstroomvoorziening. Indien een gescheiden noodstroomvoorziening (UPS) wordt gebruikt voor deze componenten, mag worden afgeweken van de installatievoorschriften artikel 5.2.4 (Wegvallen netspanning) en 5.2.5 (Melding). Deze noodstroomvoorziening (UPS) dient dan wel te worden aangesloten op dezelfde 230V eindgroep waarop de CCS is aangesloten. Een uitval van deze 230V eindgroep en een herstel van 230 V zal dan via het CCS, via het alarmtransmissiesysteem of de alarmoverdrager worden doorgemeld naar een PAC. 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. Het doormelden van een netspanningsuitval van de CCS naar de PAC, dient binnen 2 minuten te geschieden.

Opmerking

Korte autonomietijd betekent dat er organisatorische maatregelen nodig zijn in geval van stroomuitval.

Actiepatroon PAC

De uitval van de CCS, de primaire verbinding, de secundaire verbinding en uitval van beide paden behoren te worden geconstateerd door de PAC. De PAC moet deze uitvalmeldingen opvolgen conform daarover schriftelijk vastgelegde afspraken.

7.2.3 Alarmtransmissieniveau AT3

De eisen aan de akoestische en optische alarmgevers en de eisen voor het actiepatroon door de PAC bij uitval van de CCS komen overeen met AT2.

Met betrekking tot de alarmering moet voor het versturen van de alarmmelding een systeem worden toegepast volgens ATS-categorie DP3. De alarmoverdracht moet geschieden naar een PAC.

Elke 3 minuten moet over de primaire verbinding een controlemelding tussen de alarmkiezer en de ontvanger plaatsvinden. Minimaal één keer per 25 uur vindt de controlemelding over de secundaire verbinding plaats.

7.2.4 Alarmtransmissieniveau AT4

De eisen aan de akoestische en optische alarmgevers en de eisen voor het actiepatroon door de PAC bij uitval van de CCS komen overeen met AT2.

Met betrekking tot de alarmering moet voor het versturen van de alarmmelding een systeem worden toegepast volgens ATS-categorie DP4. De alarmoverdracht moet geschieden naar een PAC. Elke 90 seconde moet over de primaire verbinding een controlemelding tussen de alarmkiezer en de ontvanger plaatsvinden. Minimaal één keer per 5 uur moet een controlemelding over de secundaire verbinding plaatsvinden.

7.3 Kenmerken

Volgens NEN-EN 50136-1 zijn de prestatiecriteria voor een alarmtransmissiesysteem (ATS) geclassificeerd in 10 categorieën. Categorie SP1 t/m SP6 specificeren een ATS met een enkelvoudig alarmtransmissie pad (ATP). Categorie DP1 t/m DP4 specificeren een ATS met een dubbel alarmtransmissie pad. De VRKI 2.0 hanteert de ATS-categorieën conform tabel 7.2.

TABEL 7.2: ATS-CATEGORIEËN

	Niveau AT2		Niveau AT3	Niveau AT4
ATS-categorie	SP2	DP1	DP3	DP4
Rapportagetijd – primair ATP	25 uur	25 uur	3 min	90 sec
Rapportagetijd – alternatief ATP	Optioneel	50 uur	25 uur	5 uur
Rapportagetijd – alternatief ATP bij uitval primair ATP	Optioneel	25 uur	3 min	90 sec

7.4 Algemene eisen Alarmtransmissiesystemen

Voor de transmissiesystemen moeten maatregelen worden getroffen ter voorkoming van het nabootsen van het transmissiesysteem in het te beveiligen gebouw. Bij SP2 en DP1 (AT2) is dit optioneel.

Bij DP3 (AT3) en DP4 (AT4) moet dit geschieden door: encryptie van een identiteit of een adres van alle uitgezonden signalen over het alarmtransmissie pad. Substitutiebeveiliging conform NEN-EN 50131-1:2006/At:2009 par. 8.6 tabel 11 (S2) en NEN-EN 50136-1:2012 par. 8.6.2 tabel 8 en tabel D.5 Substitutiebeveiliging.

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 Informatiebeveiliging.

7.4.1 Alarm over IP

Aan de ATS-categorieën zijn zogenoemde rapportagetijden gekoppeld, zie tabel 7.2.

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, moet voldoen aan de rapportagetijden in tabel 7.2.

7.4.2 Secundaire transmissieverbinding

Gedurende de periode 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.

7.4.3 Prestatieniveau transmissiesysteem

Het prestatieniveau van het totale alarmtransmissiesysteem wordt bepaald door de 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 (AT3) is ingesteld en de toegepaste alarmoverdrager staat op SP2 of DP1 (AT2), dan zal het prestatieniveau van de het totale alarmtransmissiesysteem uitkomen op SP2 of DP1 (AT2).

7.4.4 Alarmtransmissie via mobiel netwerk

Ondanks het feit dat een technische oplossing op basis van een enkelvoudig transmissiepad via mobiele netwerken mogelijk is, wordt deze wijze van alarmtransmissie afgeraden. Bij de keuze van de geadviseerde oplossingen is rekening gehouden met de sabotagegevoeligheid van mobiele netwerken.

7.4.5 VOIP

Het aansluiten van een analoge/PSTN-kiezer op de VOIP- of POTS-PTSN poort van een internetmodem, biedt een onvoldoende betrouwbare alarmtransmissie en is daarom niet toegestaan.

Telefonie via Internet Protocol is vaak voorzien van een aansluiting voor analoge telefonie en randapparatuur. Deze aansluiting is echter niet geschikt voor analoge modems en analoge alarmkiesers. De conversie van analoge alarmmeldingen (zoals afkomstig uit traditionele analoge alarmkiesers) 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. Bij gebruik van AoIP moet een IP kiezer/modem of IP converter worden toegepast die op een Ethernetaansluiting van de router kan worden aangesloten.

7.4.6 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 verificatie van de prestaties van een ATS behoort te worden uitgevoerd door de alarmtransmissie service provider (ATSP). In Nederland is dit in veel gevallen de aanbieder van het alarmtransmissiesysteem.

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 alarm doormelding 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.

Voor SP2 en DP1 (AT2) is het toegestaan verificatie van de prestaties achterwege te laten. Volstaan kan worden met het bewaken van de testmeldingen uit het inbraaksignaleringsstelsel door de PAC.

Voor AT3 en AT4 geldt in afwijking van de NEN-EN 50136-1 hetzelfde.

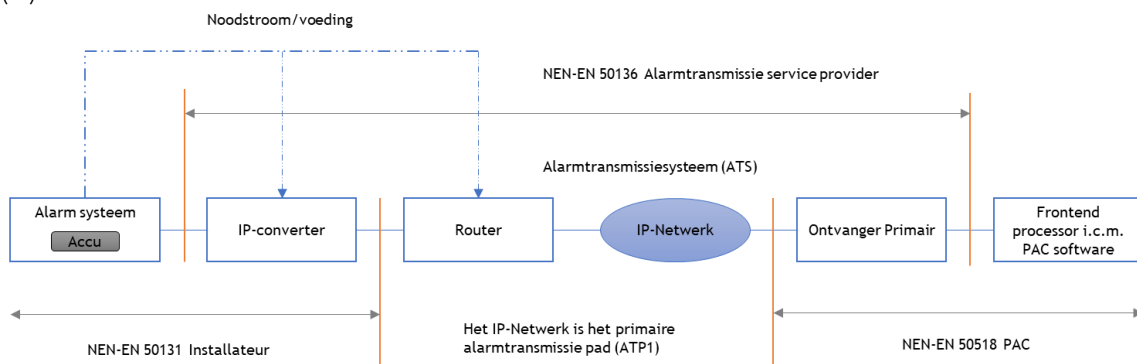
7.4.7 Beschikbaarheid

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 50136-1:2012, 7.5.3 Calculations. Registraties van de beschikbaarheid van elk ATS behoren op aanvraag aan de klant of installateur te worden verstrekt.

7.5 Beschrijving van alarmtransmissiesysteem

7.5.1 Woningen met een enkelpadig alarmtransmissiesysteem

Figuur 7.3 is een schematische weergave van een ATS-categorie SP2 met noodstroomvoorziening van de router vanuit het inbraaksignaleringsstelsel. De capaciteit van de accu in het alarmsysteem moet toereikend zijn voor een autonometijd van minimaal 12 uur. Voor woningen mag ook gebruik worden gemaakt van een enkelpadig alarmtransmissiesysteem zoals weergegeven in 7.5.3. In een dergelijk geval is het noodzakelijk dat het alarmsysteem en de UPS op dezelfde 230 volt eindgroep aangesloten worden. Zie ook bij "7.2.2. Alarmtransmissieniveau AT2 Aanvullend vereist bij gebruik IP met enkelvoudige verbinding (SP)".



Figuur 7.3

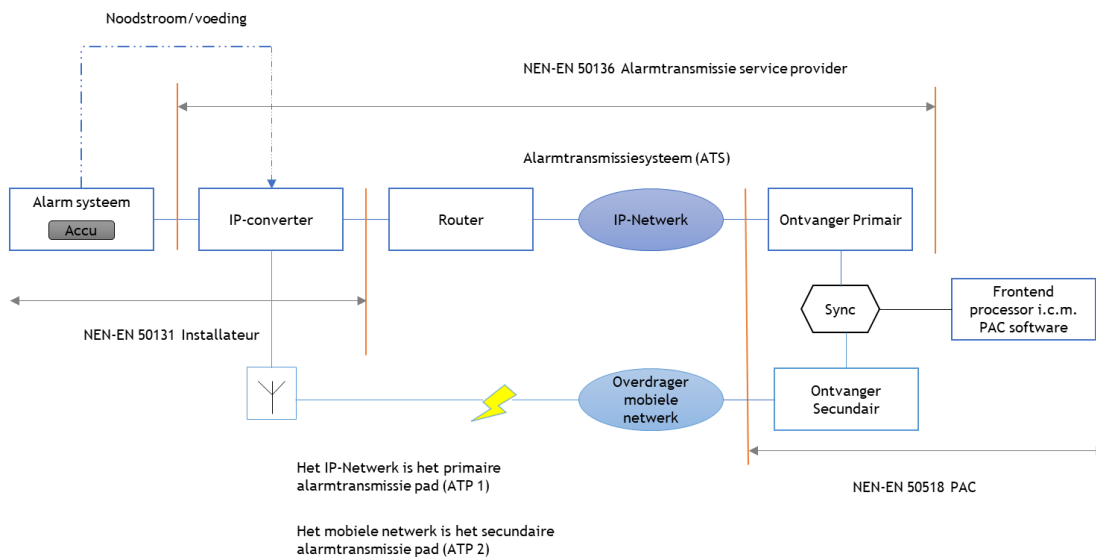
De noodstroom geldt voor alle componenten tussen het inbraaksignaleringsstelsel en het IS-RA punt die gebruikt worden voor de alarmtransmissie. Plaatsing in beveiligd gebied en een effectieve beveiliging tegen sabotage gelden ook voor alle apparatuur die voor het functioneren van de doormelding naar een PAC van belang is, alsmede voor de hierbij behorende noodstroomvoorziening(en). De voeding voor de apparatuur van het ATS moet selectief worden beveiligd ten opzichte van overige gebruikers die op een inbraaksignaleringsstelsel zijn aangesloten. Voorkomen moet worden dat bij een kortsluiting, in bijvoorbeeld een ruimtelijke melder of flitslicht of bediendeel, de voeding van de apparatuur van het ATS wegvalt.

7.5.2 Woningen met een dubbelpadig alarmtransmissiesysteem

Figuur 7.4 is een schematische weergave van een ATS-categorie DP1 en DP3 met noodstroomvoorziening van de IP-converter en de overdrager naar het mobiele netwerk vanuit het inbraaksignaleringsysteem.

Effectieve beveiliging tegen sabotage en plaatsing in beveiligd gebied gelden ook voor de apparatuur die voor het functioneren van de doormelding naar de PAC van belang is. De voeding voor de apparatuur van het ATS moet selectief worden beveiligd ten opzichte van overige gebruikers die op een inbraaksignaleringsysteem zijn aangesloten. Voorkomen moet worden dat bij een kortsluiting, in bijvoorbeeld een ruimtelijke melder of flitslicht of bediendeel, de voeding van de apparatuur van het ATS wegvalt.

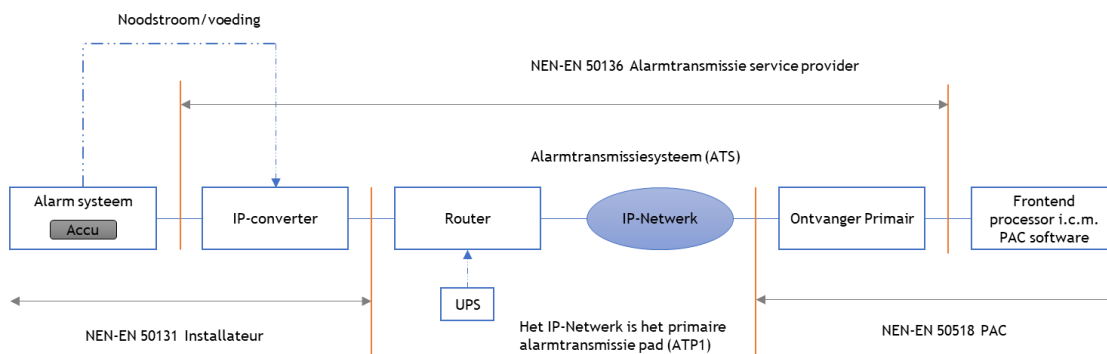
Een dubbel alarmtransmissiepad moet zijn opgebouwd uit primair een vaste fysieke verbinding en secundair een verbinding via een mobiel netwerk. Tweemaal een draadloze of mobiele verbinding is niet toegestaan als dubbel alarmtransmissiepad, ook niet als de alarmcommunicatie via twee verschillende netwerken plaatsvindt.



Figuur 7.4

7.5.3 Bedrijven met enkelpadig alarmtransmissiesysteem

Figuur 7.5 is een schematische weergave van een ATS-categorie SP2 met noodstroomvoorziening van de router, anders dan vanuit het inbraaksignaleringsysteem. Voor bedrijven mag ook gebruik worden gemaakt van een enkelpadig alarmtransmissiesysteem, zoals weergegeven in 7.5.1. Zie ook bij "7.2.2. Alarmtransmissieniveau AT2 Aanvullend vereist bij gebruik IP met enkelvoudige verbinding (SP)".

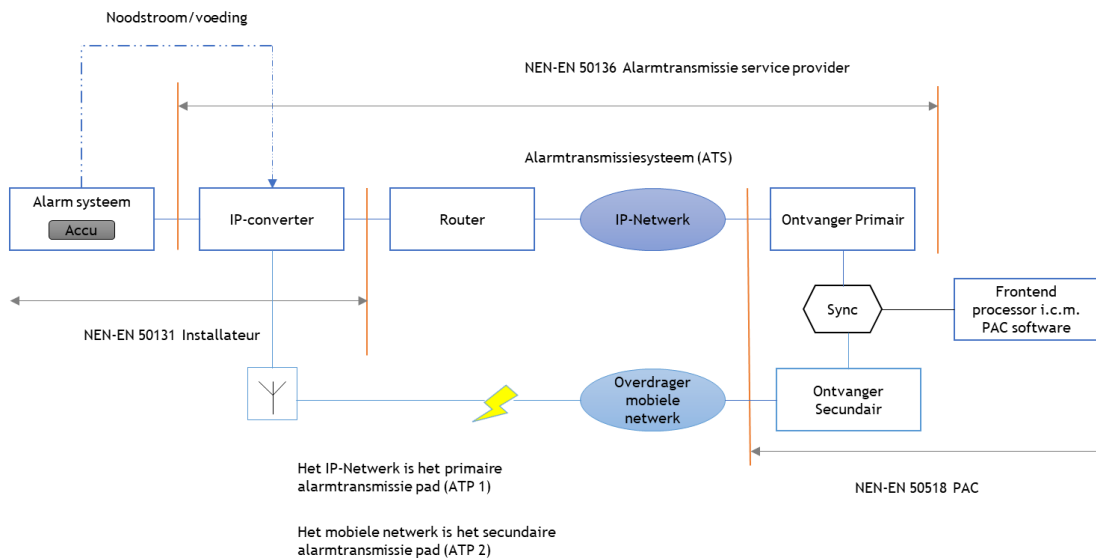


Figuur 7.5

Indien mogelijk wordt de router gevoed met 12 V gelijkspanning, bij voorkeur vanuit het inbraaksignaleringssysteem. Als dat niet mogelijk is, wordt een externe UPS toegepast. In een dergelijk geval is het noodzakelijk dat het alarmsysteem en de UPS op dezelfde 230 volt eindgroep aangesloten worden. De noodstroom geldt voor alle componenten tussen de IP-converter en het IS-RA punt die gebruikt worden voor de alarmtransmissie. Van belang zijn maatregelen om het risico te beperken dat op de noodstroomvoorziening andere apparatuur wordt aangesloten. Indien dit wel het geval is, voldoet de tijd dat de noodstroomvoorziening blijft werken niet meer aan de eis. De voeding voor de apparatuur van het ATS moet selectief worden beveiligd ten opzichte van overige gebruikers die op een inbraaksignaleringssysteem zijn aangesloten. Voorkomen moet worden dat bij een kortsluiting, in bijvoorbeeld een ruimtelijke melder of flitslicht of bediendeel, de voeding van de apparatuur van het ATS wegvalt.

7.5.4 Bedrijven met dubbelpadig alarmtransmissiesysteem

Figuur 7.6 is een schematische weergave van een systeem met ATS-categorie DP1, DP3 en DP4.



Figuur 7.6

Indien een back-up router gebruik maakt van een shared line, moeten aanvullende maatregelen worden getroffen om de back-up-alarmcommunicatie over deze shared line te borgen. Dit kan middels een voorkeurschakeling onder controle van het inbraaksignaleringssysteem of overdrager, of door toepassing van een beveiligde splitter. De beveiligde splitter wordt gevoed vanuit het inbraaksignaleringssysteem en rapporteert aan het inbraaksignaleringssysteem in de situatie dat er sprake is van het aanspreken van de beveiligingsfunctie met betrekking tot de verstoring op de shared line. De PAC moet deze uitvalmeldingen opvolgen conform daarover schriftelijk vastgelegde afspraken. De voeding voor de apparatuur van het ATS moet selectief worden beveiligd ten opzichte van overige gebruikers die op een inbraaksignaleringssysteem zijn aangesloten. Voorkomen moet worden dat bij een kortsluiting, in bijvoorbeeld een ruimtelijke melder of flitslicht of bediendeel, de voeding van de apparatuur van het ATS wegvalt.

Een dubbel alarmtransmissiepad moet zijn opgebouwd uit primair een vaste fysieke verbinding en secundair een verbinding via een mobiel netwerk. Tweemaal een draadloze of mobiele verbinding is niet toegestaan als dubbel alarmtransmissiepad, ook niet als de alarmcommunicatie via twee verschillende netwerken plaatsvindt.

8. RE - Reactie

RE-maatregelen zijn de maatregelen met betrekking tot de alarmopvolging. Alarmopvolging is noodzakelijk om het uiteindelijke doel van inbraakbeveiliging te bereiken.

8.1 Alarmverificatie methoden

Er zijn twee methoden van alarmverificatie mogelijk, namelijk persoonlijke alarmverificatie en technische alarmverificatie.

8.1.1 Persoonlijke alarmverificatie

Bij persoonlijke alarmverificatie vindt alarmopvolging plaats door bijvoorbeeld sleutelhouders of een particuliere beveiligingsorganisatie. Persoonlijke alarmverificatie genereert bij de politie een prioriteit 1 alarm. In geval van een geconstateerd delict, door bijvoorbeeld een voorbijganger, kan een 112-melding worden gemaakt.

8.1.2 Technische alarmverificatie

Bij technische alarmverificatie worden verschillende methoden van verificatie en beoordeling onderscheiden. Voor de toegestane mogelijkheden van technische alarmverificatie zie de Richtlijn Projectering Alarmverificatie – vigerende versie.

8.2 Niveaus van alarmopvolging

In de tabellen met beveiligingsmaatregelen in deel A van de VRKI 2.0 wordt de reactie aangeduid met de letters RE en een cijfer. Het cijfer heeft hierbij betrekking op het niveau van maatregelen. Er zijn vier niveaus van alarmopvolging te onderscheiden.

8.2.1 Niveau RE1

- Alleen van toepassing bij een alarminstallatie van niveau EL1 voor woningen en bedrijven.
- In deze situatie kan de alarmering door het inbraaksignaleringsstelsel gemeld worden naar een (mobiele) telefoon (spraak, tekstbericht) die bereikbaar is. Bij bedrijven is dit een eis.
- Er is geen garantie dat de melding tijdig de alarmopvolger bereikt. Melding kan bijvoorbeeld in voicemail terechtkomen.
- De alarmopvolging kan geschieden door persoonlijke verificatie door de eigenaar of sleutelhouder(s).
- Bij woningen mag de alarmering ook bestaan uit enkel luid- en optische alarmering. De opvolging kan geschieden door de bewoner, burens of passanten die reageren op de luid- en/of optische alarmgevers.

8.2.2 Niveau RE2

- Reactie alarmopvolging: alarmopvolging door sleutelhouder(s) die door de PAC worden gebeld. Bij de PAC moeten minimaal 3 sleutelhouders zijn opgegeven.
- Bij een alarmmelding waarbij alarmverificatie met technische middelen ontbreekt of leidt tot een negatieve verificatie, wordt alleen de sleutelhouder gebeld.
- Sleutelhouders moeten bereikbaar zijn en in staat zijn om te verifiëren of het geen vals alarm betreft.
- Uitgangspunt is alarmopvolging binnen maximaal 15 minuten.
- De sleutelhouder moet, bij mogelijk vermoeden dat het inbraakalarm door een criminele handeling ter plaatse is veroorzaakt, de PAC daarvan op de hoogte stellen en/of 112 te bellen.

8.2.3 Niveau RE3

- Reactie alarmopvolging: procedure als bij RE2 met de aanvulling dat voor de alarmopvolging een contract moet zijn gesloten met een door het Ministerie van Justitie en Veiligheid toegelaten particuliere beveiligingsorganisatie (geregistreerd middels ND nummer), die onder meer als sleutelhouder kan fungeren.
- Sleutelhouders moeten bij de PAC geregistreerd blijven voor terugkoppeling bij calamiteiten.
- Uitgangspunt is alarmopvolging binnen maximaal 15 minuten.
- Bij RE3 kan ook worden gekozen voor RE2 + technische alarmverificatie waarmee in plaats van alarmopvolging door een particuliere beveiligingsorganisatie alarmopvolging door een sleutelhouder samen met prioriteit 1 door de politie kan worden bereikt.

8.2.4 Niveau RE4

- Reactie alarmopvolging: procedure als bij RE3 (dus opvolging door een particuliere beveiligingsorganisatie).
- Minimaal één van de drie technische alarmverificatie-mogelijkheden moet operationeel zijn.
- Uitgangspunt is opvolgingstijd van maximaal 15 minuten door de particuliere beveiligingsorganisatie en een prioriteit 1 van de politie (15 minuten, na technisch alarmverificatie).
- Sleutelhouders moeten bij de PAC geregistreerd blijven voor terugkoppeling bij calamiteiten.

9. Verwijzingen (verbonden aan de VRKI 2.0)

Voor onderstaande documenten geldt dat de vigerende versie van toepassing is, inclusief wijzigingsbladen en correctiebladen. Daar waar de VRKI afwijkt van een norm of onderdeel hiervan, is de VRKI leidend.

Wettelijk kader:	
Wpbr	Wet Particuliere beveiligingsorganisaties en recherchebureaus, vigerende versie
Rpbr	Regeling Particuliere beveiligingsorganisaties en recherchebureaus, vigerende versie
Wbp	Wet bescherming persoonsgegevens, vigerende versie
Waardeberging:	
EN 14450	Waardeberging - Eisen, classificatie en beproevingsmethoden voor weerstand tegen inbraak - Inbraakwerende kasten
EN 1143-1	Waardeberging - Eisen, classificatie en beproevingsmethoden van de weerstand tegen inbraak - Deel 1: Safes, geldautomaatkluisen, kluisdeuren en kluisen
NEN-EN 15659	Waardeberging - Eisen en beproevingsmethoden voor de brandwerendheid - Lichte brandwerende opslageenheden
NEN-EN 1047-1	Waardeberging - Eisen en beproevingsmethoden voor de brandwerendheid - Deel 1: Brandwerende kasten en disketteverpakkingen
Vereniging Geld en Waardeberging (VGW)	Informatiekaart kluisen – normering en dekkingsadvies
Elektronische maatregelen:	
NEN-EN 50131	Alarmsystemen - Inbraak- en overvalsysteem
NEN-EN 50136	Alarmsystemen - Alarmtransmissiesystemen en -apparatuur -
NEN-EN 50518	Monitoring en alarmontvangstcentrales
Voorschriften (Nationaal):	
Document D01-026	Installatievoorschriften mistgeneratoren, het CCV
Document 002079	Voorschriften beheer en onderhoud alarmapparatuur
Document 002080	Installatievoorschriften voor alarmapparatuur

Toegangsbeheer en cameratoezicht:	
Cameratoezicht in de openbare ruimte	Handreiking cameratoezicht, het CCV
Buitenterreinen	Handreiking beveiligingsmaatregelen buitenterreinen transport-/logistieke bedrijven, Verbond van verzekeraars
	Handreiking beveiligingsmaatregelen voor buitenterreinen mobiliteitsbedrijven, Verbond van verzekeraars
Bouwkundige beveiliging:	
PKVW	PKVW Beveiligingsrichtlijn, Productenlijst, handleiding 2020 bestaande bouw (vigerende versie), het CCV

NCP/Romazo rolluiken matrix	http://www.romazorolluiken.nl/Rolluikenmatrix.html
NEN-EN 356	Glas in gebouwen - Beveiligingsbeglazing - Beproeving en classificatie van de weerstand tegen manuele aanval
NEN 5087	Inbraakveiligheid van woningen - Bereikbaarheid van dak- en gevelelementen: deuren, ramen en kozijnen
NEN 5089	Inbraakwerend hang- & sluitwerk - Eisen en beproevingsmethoden
NEN 5096	Inbraakwerendheid - Dak- of gevelelementen met deuren, ramen, luiken en vaste vullingen - Eisen, classificatie en beproevingsmethoden
NEN-EN 1627	Deuren, ramen, vliesgevels, traliehekken en luiken - Inbraakwerendheid - Eisen en classificatie
NEN-EN 1628	Deuren, ramen, vliesgevels, traliehekken en luiken - Inbraakwerendheid - Beproevingmethode voor de bepaling van de weerstand tegen statische belasting
NEN-EN 1629	Deuren, ramen, vliesgevels, traliehekken en luiken - Inbraakwerendheid - Beproevingmethode voor de bepaling van de weerstand tegen dynamische belasting
NEN-EN 1630	Deuren, ramen, vliesgevels, traliehekken en luiken - Inbraakwerendheid - Beproevingmethoden voor de bepaling van de weerstand tegen manuele inbraakpogingen
SKG-KE 470	SKG – Kwaliteitseisen 470 voor het SKG productcertificaat voor meeneembeperkende producten
BRL 3104	Nationale beoordelingsrichtlijn voor het KOMO® productcertificaat voor hang- en sluitwerk voor dak- en gevelelementen Deze BRL 3104 verwijst naar onderstaande norm
SKG-AE 3104	Prestatie-eisen, producteisen en andere eisen aan beveiligingsproducten voor ramen en deuren - additionele eisen voor BRL 3104



Centrum voor Criminaliteitspreventie en Veiligheid

Het Centrum voor Criminaliteitspreventie en Veiligheid is het centrum dat samenhangende instrumenten ontwikkelt en implementeert om de maatschappelijke veiligheid te vergroten. Het CCV stimuleert samenwerking tussen publieke en private organisaties om criminaliteit integraal terug te dringen en vormt een schakel tussen beleid en praktijk.

Van deze door het CCV ontwikkelde instrumenten, door andere partijen ontwikkelde instrumenten, of op marktniveau al aanwezige (technische) instrumenten kan de behoefte aanwezig zijn dat de kwaliteit van de gehaalde prestatie aantoonbaar gemaakt wordt.

Het CCV heeft hiervoor conformiteitschema's in beheer, waarvoor een structuur met inspraak van belanghebbende partijen ingericht is.

Het Centrum voor Criminaliteitspreventie en Veiligheid is gehuisvest te Utrecht:

Churchillaan 11

3527 GV Utrecht

Postbus 14069

3508 SC Utrecht

T (030) 751 6700

F (030) 751 6701



De stichting Centrum voor Criminaliteitspreventie en Veiligheid is een initiatief van het Ministerie van Veiligheid en Justitie, het Ministerie van Binnenlandse Zaken en Koninkrijksrelatie, het Verbond van Verzekeraars, werkgeversorganisatie VNO-NCW, de Vereniging van Nederlandse Gemeenten en de Raad van Korpschefs.