Adequaat risicomanagement voor fysieke beveiliging: het gebruik van modellen en metaforen gebaseerd op kennis uit het veiligheidsdomein

Sas, Marlies; Reniers, G.L.L.M.E.; van Nunen, K.L.L.; Hardyns, Wim ; Ponnet, Koen

Publication date
2020

Document Version
Final published version

Published in
Tijdschrift voor Toegepaste Arbowetenschap

Citation (APA)
Sas, M., Reniers, G. L. L. M. E., van Nunen, K. L. L., Hardyns, W., & Ponnet, K. (2020). Adequaat risicomanagement voor fysieke beveiliging: het gebruik van modellen en metaforen gebaseerd op kennis uit het veiligheidsdomein. *Tijdschrift voor Toegepaste Arbowetenschap*, *33*(3), 93 - 103.

Full paper

Adequaat risicomanagement voor fysieke beveiliging: het gebruik van modellen en metaforen gebaseerd op kennis uit het veiligheidsdomein

Marlies Sas[1,2,], Genserik Reniersi[1,3], Karolien van Nunen[3,4], Wim Hardyns[1,2,5], Koen Ponnet[6]*

Key words: veiligheid, beveiliging, beveiligingsmodellen, beveiligingsmetaforen, beveiligingsmanagement

Samenvatting

Een toename in het gebruik van informatie en de bijhorende communicatietechnieken, de complexe moderne infrastructuur en de toegenomen verbondenheid tussen verschillende systemen en organisaties hebben voor een grote kwetsbaarheid op het vlak van *physical security*, of 'fysieke beveiliging', gezorgd. Terwijl er in de afgelopen eeuw talrijke conceptuele modellen, metaforen en beginselen ontwikkeld werden om risico's op het vlak van veiligheid (*safety*) te beheersen, kan beveiliging (*security*) beschouwd worden als een relatief nieuw wetenschapsdomein. Omwille van de grote gelijkenissen en verwevenheid tussen beide domeinen, kan er veel geleerd worden van de reeds ontwikkelde modellen en beginselen op het vlak van veiligheid. Zowel veiligheid als beveiliging vertrekken van het hetzelfde uitgangspunt, namelijk dat verliezen zoveel mogelijk moeten vermeden of verminderd worden. In dit artikel wordt uitgelegd hoe fysieke beveiliging in relatie tot veiligheid staat en welke modellen en metaforen uit het safety domein aangewend kunnen worden om fysieke beveiligingsrisico's binnen bedrijven te beheersen.

Abstract

An increase in the use of information and communication techniques, the complex modern infrastructure and a closer connection between different systems and organizations have created a greater vulnerability with respect to physical security. While numerous conceptual models, metaphors and principles have been developed to manage safety risks, security can be considered as a relatively young field of science. However, because of the similarities and interwovenness between safety and security, much can be learned from the models and principles that have been developed within safety science. Both safety and security have the same objective, that is, to avoid or reduce any losses. This article explains how physical security relates to safety and which models and principles from safety science can be employed to manage company's physical security risks.

1. Inleiding

In tegenstelling tot veiligheid (*safety*) is beveiliging (*security*) nog een relatief nieuw wetenschapsdomein. In de laatste decennia zorgde de toename van beveiligingsincidenten zoals terrorisme, spionage, georganiseerde criminaliteit en cyberaanvallen er echter voor dat de aandacht voor beveiliging een sterke stijging kende in de praktijk. Terwijl bedrijven voordien voornamelijk focuste op relatief kleine criminaliteitsvormen, zoals vandalisme en diefstal, tracht men zich nu te beschermen tegen alle intentionele en kwaadwillige dreigingen van buitenaf. Er kan een onderscheid gemaakt worden tussen dreigingen in de fysieke wereld en dreigingen in een digitale omgeving. We focussen in dit artikel op de eerste soort dreigingen en verwijzen hiernaar met het begrip 'fysieke beveiliging'.

Om dit soort dreigingen te voorkomen of beperken, hebben steeds meer bedrijven aandacht voor een combinatie van technische (bv. camerabewaking en toegangscontrole), organisatorische (bv. procedures en communicatie) en menselijke maatregelen (bv. persoonlijke uitrusting en opleidingen). De behoefte aan onderzoek omtrent fysieke beveiliging en meer specifiek naar de manieren waarop men zich kan beschermen is daarom groter dan ooit. Dit heeft ervoor gezorgd dat wetenschappelijk onderzoek naar beveiligingsmanagement langzaamaan groeide, maar in vergelijking met het grote aantal studies binnen het veiligheidsdomein nog in de kinderschoenen staat.

Zowel veiligheid als beveiliging vertrekken van hetzelfde

1 Antwerp Research Group on Safety and Security (ARGoSS), Universiteit Antwerpen, Belgie
2 Onderzoeksgroep Rechtshandhaving, Universiteit Antwerpen, Belgie
3 Sectie Safety and Security Science, Technische Universiteit Delft, Nederland
4 Leerstoel Vandeputte, Universiteit Antwerpen, Belgie
5 Institute for International Research on Criminal Policy (IRCP), Vakgroep Vakgroep Criminologie, Strafrecht en Sociaal Recht, Universiteit Gent, Belgie
6 Onderzoeksgroep IMEC-MICT, Vakgroep Communicatiewetenschappen, Universiteit Gent, Belgie

[*] *Correspondentieadres: Venusstraat 23, 2000 Antwerpen (marlies.sas@uantwerpen.be)*

Tabel 1 Verschillen en gelijkenissen tussen veiligheid (safety) en beveiliging (security), overgenomen van Sas et al. (2019).

	Veiligheid ***Safety***	**Beveiliging** ***Security***
Verschillen	✓ De oorzaak van het incident is niet-opzettelijk ✓ Afwezigheid van agressor/intelligente tegenstander ✓ Transparantie is essentieel voor hoog veiligheids-niveau ✓ Voornamelijk interne risico's	✓ De oorzaak van het incident is opzettelijk ✓ Aanwezigheid van agressor/intelligente tegen-stander ✓ Transparantie levert niet altijd voordelen op ✓ Voornamelijk externe dreigingen
Gelijkenissen	✓ Nemen van preventiemaatregelen is essentieel om tot aanvaardbaar niveau van veiligheid en beveiliging te komen ✓ Veiligheidsmaatregelen kunnen positief effect hebben op het vlak van beveiliging (en omgekeerd) ✓ Integrale cultuuraanpak: focus op technische, organisatorische en menselijke aspecten	

uitgangspunt, namelijk dat verliezen moeten voorkomen of beperkt worden. Het belangrijkste verschil situeert zich in de manier waarop deze verliezen ontstaan (zie Tabel 1). Bij een veiligheidsincident is het nooit de bedoeling om schade aan te richten, waardoor het incident steeds op een niet-intentionele wijze wordt veroorzaakt, door bijvoorbeeld een procesfout of het falen van een machine. Bij een beveiligingsincident is er steeds sprake van een 'intelligente tegenstander' of agressor die op een kwaadwillige en intentionele manier schade veroorzaakt. In dit geval wordt het verlies met opzet veroorzaakt, door bijvoorbeeld een gefrustreerde ex-werknemer die wraak wil nemen. Dit belangrijkste verschil heeft een impact op de gewenste mate van transparantie voor beide domeinen. Terwijl het op het vlak van veiligheid transparantie essentieel is om onder andere optimaal te leren van onveilige situaties, kan dit op het vlak van beveiliging ervoor zorgen dat personen met een kwaadwillige intentie een beveiligingsincident veroorzaken door van de transparantie van informatie gebruik te maken. Een terroristische aanslag kan bijvoorbeeld gepland worden op basis van de beschikbare informatie over de aanwezige toxische stoffen. Tot slot moet er een onderscheid gemaakt worden tussen de risico's op het vlak van veiligheid en de dreigingen op het vlak van beveiliging. Terwijl veiligheidsrisico's voornamelijk voortkomen uit het bedrijf zelf, zijn beveiligingsdreigingen vaak extern aan het bedrijf. Dit houdt in dat het niet altijd eenvoudig is om dreigingen in kaart te brengen, aangezien er heel wat externe en onbekende factoren meespelen (Sas et al., 2019).

Hoewel veiligheid en beveiliging enkele verschillen vertonen, zijn er ook heel wat gelijkenissen tussen beide domeinen. Zo zijn preventiemaatregelen essentieel om zowel een adequaat niveau van veiligheid als van beveiliging te bekomen. Dit houdt bijgevolg in dat genomen maatregelen op het vlak van veiligheid ook een positief effect kunnen hebben op het vlak van beveiliging en omgekeerd. Zo kunnen *awareness* trainingen om het veiligheidsbewustzijn te vergroten er ook voor zorgen dat het beveiligingsbewustzijn onder werknemers wordt gestimuleerd. Tot slot is het belangrijk dat er bij het creeren van een veilige of beveiligde omgeving steeds gefocust wordt op een integrale cultuuraanpak die bestaat uit technische, organisatorische en menselijke aspecten (van Nunen et al., 2018).

Om een adequaat veiligheids- of beveiligingsniveau binnen de organisatie te bereiken, is er nood aan efficient risicomanagement. Om een helder beeld te krijgen van de manier waarop risico's kunnen worden beheerst, is het belangrijk om te verduidelijken wat net met de term 'risico' wordt bedoeld. Volgens ISO 31000 (International Standardization Organization, 2009) kan risico gedefinieerd worden als *'the effect of uncertainty on objectives'*. Met deze zeer brede definitie wordt bedoeld dat een risico niet kan bestaan zonder specifieke doelstellingen of onzekerheden binnen de organisatie. Voor niet-intentionele (veiligheids)risico's worden steeds drie aspecten blootgelegd: gevaren, blootstellingen en niet-intentionele verliezen. Om intentionele (beveiligings)risico's te identificeren worden eveneens drie aspecten in kaart gebracht, naar analogie met de veiligheidsrisico's: dreigingen (*threats*), kwetsbaarheden en intentionele verliezen (zie Figuur 1).

Figuur 1 Aspecten van niet-intentionele (veiligheids)risico's en intentionele (beveiligings)risico's.

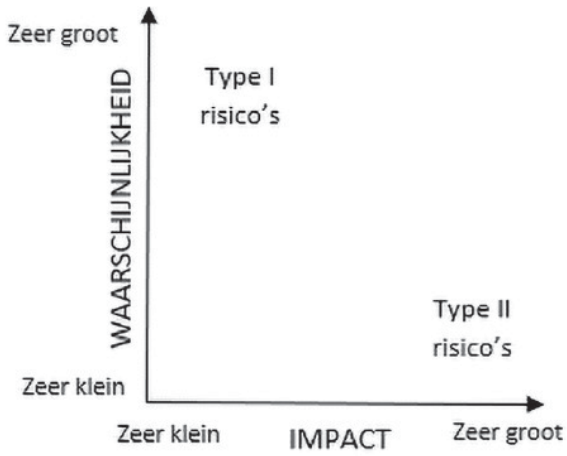
Met dreigingen wordt verwezen naar onwenselijke situaties, processen, scenario's of clusters van scenario's, die kunnen leiden tot schade of verlies. Om een dreiging correct in te schatten is er informatie nodig over het type dreiging (bv. diefstal, terrorisme, vandalisme), de intentie van de potentiele dader (bv. geldgebrek, een kick, een overtuiging), de methodes (bv. verbaal geweld, cybercrime, wapens), de trends (bv. technieken die worden overgenomen van eerdere incidenten, experimenten met nieuwe technieken) en de triggers of events die een aanval kunnen initieren (Baybutt, 2017; Moteff, 2005). De kwetsbaarheden zijn de elementen die schade kunnen ondervinden van een dreiging (Talbot & Jakeman, 2008). Het gaat om de meest kwetsbare aspecten binnen een bedrijf, zoals onder andere operationele processen (bv. aankoop, productie, transport), infrastructuur (bv. ICT-infrastructuur, machines), mensen (bv. werknemers, bezoekers, contractoren) of goederen (bv. financiele middelen, chemische stoffen). De potentiele verliezen ontstaan wanneer een aanval met succes wordt uitgevoerd. Dit kunnen onder andere negatieve effecten inhouden op het vlak van financien (bv. faillissement, vermindering van financiele middelen), reputatie (bv. minder klanten, moeilijker aanwerven van nieuwe werknemers), infrastructuur (bv. kapotte machines, verwoeste gebouwen) of mensenlevens (bv. gewonden, doden) (Kortekaas, 2005).

Wanneer alle mogelijke dreigingen, kwetsbaarheden en potentiele verliezen gekend zijn (wat in de realiteit uiteraard niet mogelijk is), kunnen optimale beslissingen worden genomen om de beveiligingsrisico's te beperken of te elimineren. Dit is echter niet altijd zo eenvoudig als het op het eerste gezicht lijkt. Er zou, naar analogie met het veiligheidsdomein, een onderscheid moeten gemaakt worden tussen twee types van beveiligingsrisico's:

1) type I risico's met mogelijke beperkte gevolgen,
2) type II risico's met een mogelijk catastrofaal gevolg.

Type I risico's vinden regelmatig plaats, waardoor ze een grote waarschijnlijkheid hebben. Ze kunnen ernstig van aard zijn, maar hebben vaak een (relatief) kleine impact aangezien de gevolgen zich beperken tot schade voor het bedrijf en/of de dichte gemeenschap. Deze risico's komen overeen met de gekende delicten zoals diefstal, doodslag en moord. Type II risico's zijn eerder zeldzaam in het dagelijkse leven, maar wel realistisch. Ze hebben vaak een grote tot zeer grote impact en hun gevolgen reiken zelfs (internationaal) tot op maatschappelijk vlak. Een terreuraanslag is een typisch voorbeeld van een type II beveiligingsrisico. De verschillende types vragen elks om een eigen risicobeoordeling en - managementaanpak. Het is daarom noodzakelijk dat ze apart worden ge"dentificeerd, geanalyseerd, geevalueerd en geprioriteerd. Figuur 2 geeft een overzicht weer van type I en type II risico's aan de hand van hun waarschijnlijkheid en impact.

De bestaande risicobeoordelingstechnieken voor niet-intentionele (veiligheids)risico's (bv. Hazop, *What-if*



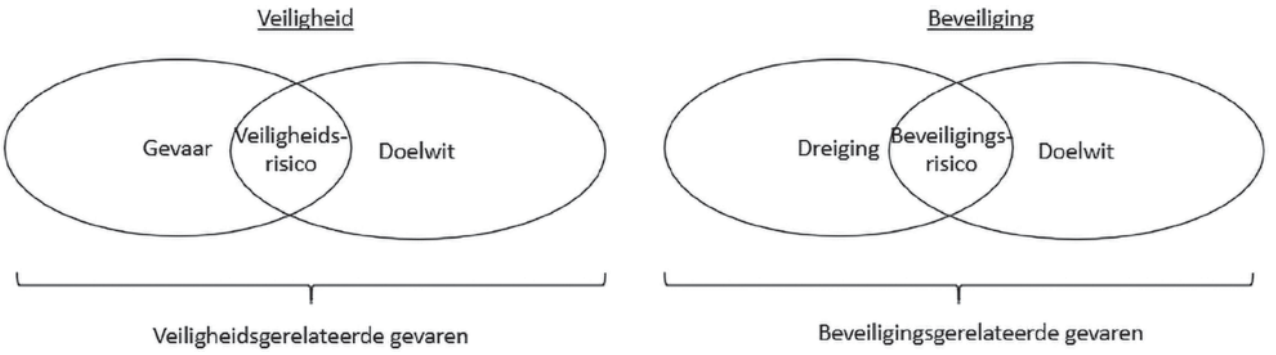
Figuur 2 Type I en type II risico's voorgesteld op grafiek volgens waarschijnlijkheid en impact.

analyse, foutenboomanalyse, bow-tie analyse) werden zo ontwikkeld dat ze zoveel mogelijk gevaren identificeren, zoveel mogelijk blootstellingen in kaart brengen en zoveel mogelijk realistische verliesscenario's formuleren (CCPS – Center of Chemical Process Safety, 2000). Ook voor intentionele (beveiligings)risico's zullen risicobeoordelingen trachten zoveel mogelijk dreigingen, kwetsbaarheden en realistische verliesscenario's te identificeren. Gezien de grote gelijkenissen en verwevenheid tussen beide domeinen kan er veel geleerd worden van de talrijke studies die werden uitgevoerd op het vlak van veiligheid. In dit artikel zullen enkele van de veiligheidsmodellen en -beginselen die tijdens de afgelopen eeuw ontwikkeld werden door veiligheidswetenschappers en ongevallenanalisten uit diverse disciplines en industriele sectoren, vertaald worden naar het fysieke beveiligingsdomein. Er zal voornamelijk gefocust worden op de preventieve aanpak of de manieren waarop men zich kan beschermen tegen beveiligingsdreigingen en in mindere mate op de reactieve aanpak van deze dreigingen.

2. Beveiligingsmodellen gebaseerd op het safety domein

2.1. Model van fysieke beveiligingsrisico's

Zoals reeds werd weergegeven worden veiligheidsrisico's gekenmerkt door gevaren, blootstellingen en niet-intentionele verliezen en beveiligingsrisico's door dreigingen, kwetsbaarheden en intentionele verliezen. In het veiligheidsdomein wordt de term 'gevaar' gebruikt om de intrinsieke eigenschappen te duiden van een voorwerp, proces, situatie, - die fatale gevolgen kunnen hebben voor productie, omgeving, gezondheid en veiligheid van de mens. In het beveiligingsdomein wordt de term 'dreiging' gebruikt om onwenselijke situaties, processen of scenario's, die kunnen leiden tot schade of verlies op het vlak van financien, mensen, reputatie, - te duiden. Een risico ontstaat wanneer een gevaar of dreiging inwerkt op een of meerdere doelwitten. Zowel op het vlak van veiligheid als beveiliging kunnen doelwitten voorkomen in verschillende vormen, zoals:



Figuur 3 Model van fysieke veiligheids- en beveiligingsrisico's.

- Persoon/een groep personen (bv. werknemers, bezoekers, contractoren)
- Omgeving (bv. nabijgelegen bedrijven en woningen)
- Bedrijfsproces (bv. transport, aankoop, verkoop)
- Kritieke infrastructuur (bv. opslagtanks, procesvaten, gevaarlijke stoffen, productiemateriaal)
- Informatie (bv. formules, prijzen, stoffen, paswoorden)
- Reputatie van een persoon, bedrijf, enzovoort

Wanneer een doelwit niet wordt blootgesteld aan een ge"dentificeerd gevaar of een dreiging, is er geen risico. Bijvoorbeeld: Het dagelijkse leven in Irak of Syrie zit momenteel vol dreigingen. Zolang potentiele doelwitten in Canada niet worden blootgesteld aan deze dreigingen, bestaan er geen potentiele verliezen voor Canada en hoeft men dus geen rekening te houden met beveiligingsrisico's die voortkomen uit deze ge"dentificeerde dreigingen. Een risico bevindt zich in de overlap tussen een gevaar of dreiging en het doelwit, zoals wordt voorgesteld in Figuur 3.

Om te voorkomen dat het gevaar of de dreiging oncontroleerbaar wordt en het doelwit bereikt, zijn er beschermende of preventieve barrieres nodig op het vlak van veiligheid of zogenaamde 'tegenmaatregelen' op het vlak van beveiliging (zie Figuur 4). Dit houdt in dat een risico in zijn fysieke vorm gekarakteriseerd wordt door vier constitutieve elementen:

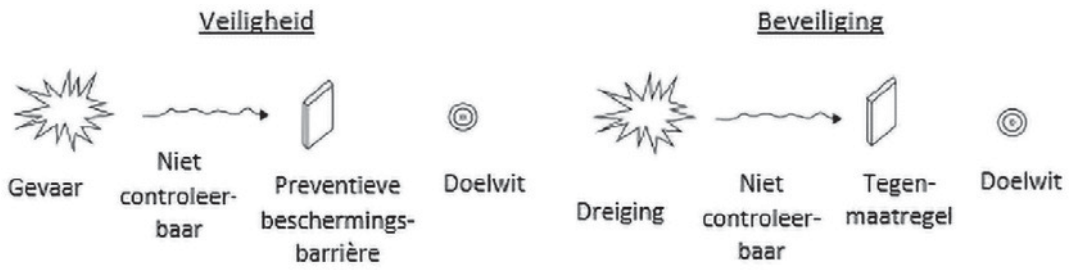
1) een gevaar/dreiging,
2) een of meerdere doelwitten die bedreigd worden door het gevaar/de dreiging,
3) het blootstellingsniveau/kwetsbaarheid van het doelwit voor het gevaar/de dreiging,
4) de maatregelen die worden genomen om het gevaar/de dreiging te beheersen of te beperken.

2.2. Rings of protection model

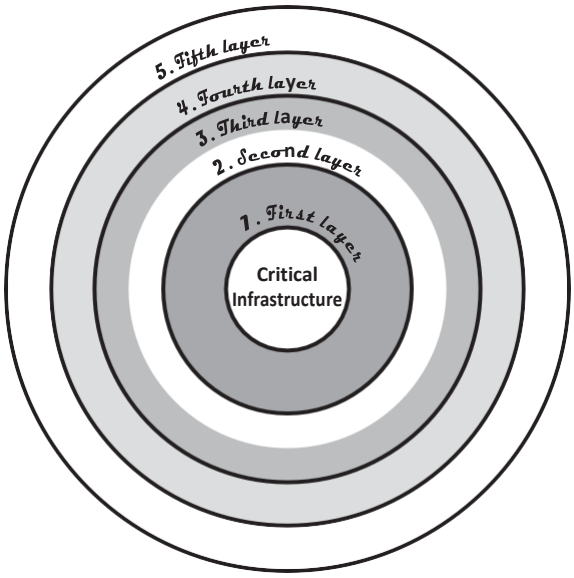
Wat betreft veiligheid (safety) binnen chemische procesbedrijven, wordt in de fundamentele basis van risicomanagement gebruik gemaakt van het instellen van onafhankelijke veiligheidsbarrieres, de zogenaamde *Layers of Protection*. Ook wat betreft beveiliging (security) wordt op analoge manier gebruik gemaakt van onafhankelijke beveiligingsbarrieres, de zogenaamde *Rings of Protection* (CCPS, 2003). In dit model met concentrische beschermingslagen fungeert de ruimtelijke relatie tussen de locatie van het doelwit en de locatie van de tegenmaatregelen als uitgangspunt. Figuur 5 verduidelijkt deze *Rings of Protection* aan de hand van vijf lagen van bescherming en een niet-limitatieve lijst van mogelijke beveiligingsbarrières.

2.3. Zwitserse kaasmodel

Het Zwitserse kaasmodel van de Britse psycholoog Reason (1997) werd oorspronkelijk ontwikkeld om te visualiseren hoe zware ongevallen kunnen plaatsvinden op basis van de aanwezigheid van 'pathogenen' of gaten in het risicomanagementsysteem. Het gebruik van de metafoor kent een lange geschiedenis binnen het veiligheidsdomein, maar is ook zeer toepasbaar op het vlak van beveiliging aangezien vertrokken wordt vanuit het *'defenses in depth'* principe, een uitgangspunt dat centraal staat in talrijke beveiligingsmodellen (Kamoun & Nicho, 2014). Het *defenses in depth* principe wordt in het Zwitserse kaasmodel voorgesteld door de plakjes kaas, welke verwijzen naar de barrieres die worden ingebouwd om fouten te vermijden. Terwijl er op het vlak van veiligheid barrieres worden ingevoerd om het aantal ongevallen te reduceren, zorgen barrieres op het vlak van beveiliging ervoor dat kwaadwillige incidenten worden beperkt (zie Figuur 6).



Figuur 4 Constitutieve elementen van een veiligheids- en beveiligingsrisico.



1. **Eerste beschermingslaag (binnenste ring)**
- Alert personeel
- Sloten op deuren en kasten
- Netwerk firewalls en wachtwoorden
- Noodcom municatie
- Beveiligde serverruimtes
- Bewakingscamera's

2. **Tweede beschermingslaag (binnenste middelste ring)**
- Sloten op deuren
- Receptionisten
- Badgecontroles
- Toegangscontrole

3. **Derde beschermingslaag (buitenste middelste ring)**
- Verlichting
- Hekken
- Intrusiedetectie
- Intrusiesensoren
- Bewakingsagenten aan buitenrand van site

4. **Vierde beschermingslaag (buitenste ring)**
- Badgecontroles
- Toegangscontrole
- Tourniquets
- Tralies
- Receptionisten

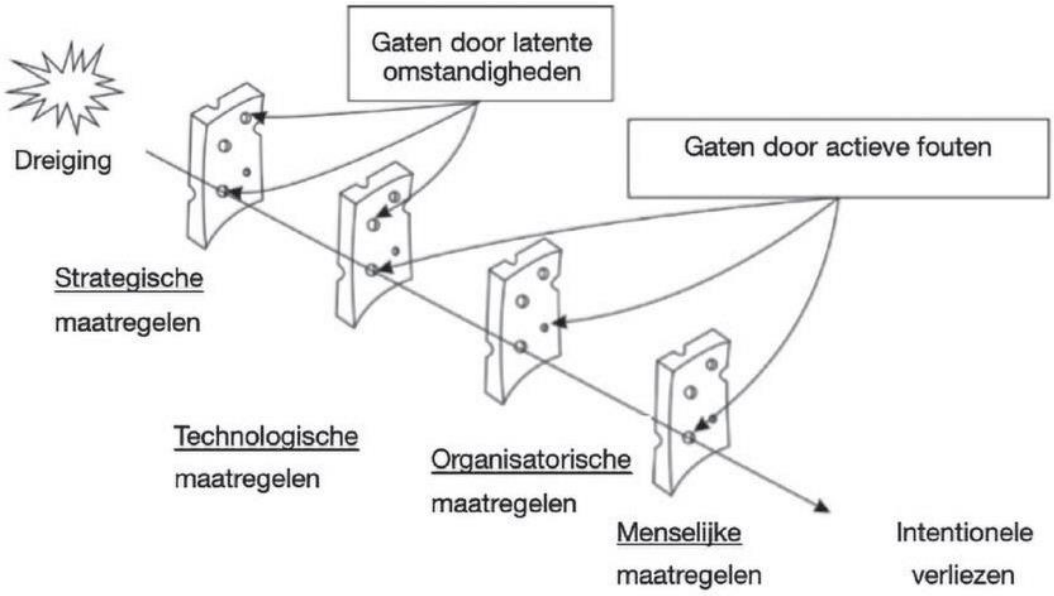
5. **Vijfde beschermingslaag (buitenring)**
- Politie
- Brandweer
- Andere handhavingsdiensten

Figuur 5 Rings of Protection model waarbij vijf onafhankelijke beschermingslagen het doelwit beschermen, overgenomen van Meyer en Reniers (2016).

Deze barrieres bevinden zich op vier niveaus: het strategische (bv. procedures of communicatie), het organisatorische (bv. organisatiestructuur of omgevingsfactoren), het technologische (bv. elektronische maatregelen) en het menselijke niveau (bv. het handelen van individuen of de persoonlijke uitrusting) (Reason, 1990).

In de barrieres kunnen gaten ontstaan door actieve fouten of latente gebreken. Actieve fouten treden op wanneer de bestaande veiligheids- of beveiligingsprocedures op zich efficient zijn, maar niet op een correcte manier worden uitgevoerd. De gevolgen van dit ongewenste gedrag zijn meteen merkbaar. Slechte omstandigheden binnen de organisatie, zoals een zwakke organisatiecultuur of inefficiente veiligheids- of beveiligingsprocedures, kunnen leiden tot latente gebreken. Hoewel deze lange tijd onzichtbaar kunnen blijven, zijn ze toch constant aanwezig. Door inzicht te krijgen in de werking van de organisatie kunnen de gaten worden gedetecteerd en door middel van risicobeoordelingen kunnen de gepaste maatregelen worden ge"dentificeerd om de gaten te sluiten (Reason et al., 2016).

Het is belangrijk om te vermelden dat het Zwitserse kaasmodel dynamisch is. De gaten kunnen toenemen in grootte of aantal (door fouten of overtredingen), maar ook afnemen (door een adequaat risicomanagement en efficiente tegenmaatregelen). Een grote kracht van het model schuilt in het gebruik van beschermingslagen en -denken. Het is de bedoeling dat de gaten in de barrières



Figuur 6 Het Zwitserse kaasmodel voor beveiliging (gebaseerd op Reason, 1997).

zo klein mogelijk worden gemaakt door het toepassen van adequaat risicomanagement, zowel voor type I (bv. diefstal, sabotage) als type II (bv. terreuraanslagen) beveiligingsrisico's.

2.4. Bipiramide model

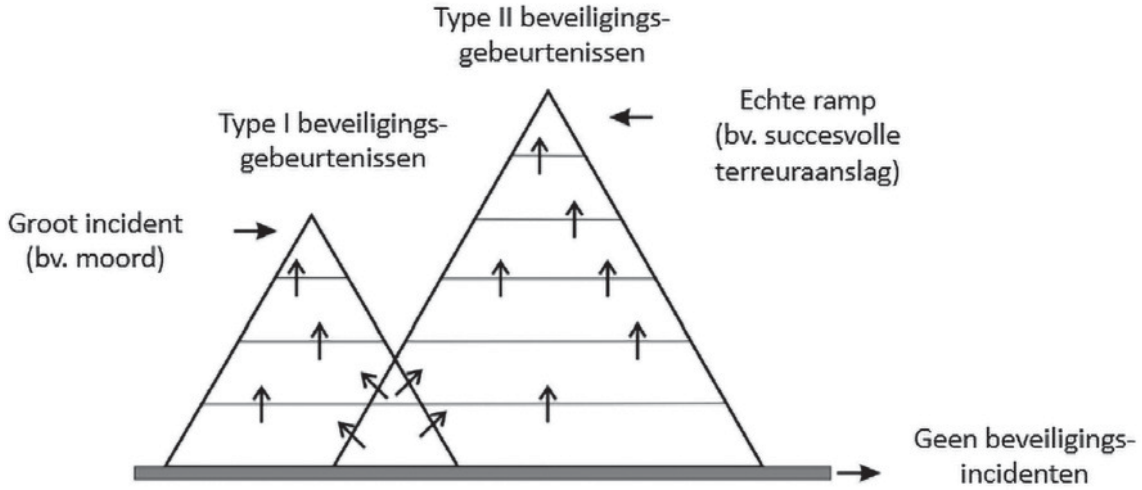
Wetenschappers zoals Heinrich (1950), Bird en Germain (1985) en Pearson, James en Fullman (1994) stelden het bestaan van een kwalitatieve relatie vast tussen het aantal veiligheidsincidenten zonder enige zichtbare verwondingen of schade, deze met eigendomsschade, deze met beperkte verwondingen en deze met ernstige en fatale verwondingen. Deze ongevallenrelatie wordt weergegeven in ongevallenpiramides, waarbij wordt verondersteld dat ongevallen vooraf aangekondigd worden door het plaatsvinden van onveilige situaties. Incidentenanalyses en veiligheidsbewustzijn zijn daarom van groot belang. In verschillende studies werden enkele ratio's gevonden (varierend van 1:300 tot 1:600), afhankelijk van onder andere de industriele sector. Ondanks het feit dat er nooit een statistische relatie tussen de verschillende lagen in de piramides werd bewezen, is het wel zo dat er mogelijk ernstige ongevallen kunnen worden voorkomen door het nemen van preventieve maatregelen gericht op bijvoorbeeld bijna-ongevallen of kleine ongevallen. Een beperkte selectie van de *near-misses* kan immers wel degelijk leiden tot een zwaar ongeval. Deze 'klassieke' ongevallenpiramides zorgen voor een duidelijk inzicht in type I ongevallen waarvoor representatieve statistische data voorhanden is. In ongevallenpiramides moeten type I en type II risico's van elkaar onderscheiden worden.

Wanneer men naar deze piramides kijkt vanuit beveiligingsoogpunt en men type I en type II incidenten in beschouwing neemt, kan de ongevallenpiramide voorgesteld worden in de vorm van een soort 'beveiligingsincidentenpiramide'. Bij het interpreteren van deze piramides moet het volgende in beschouwing genomen worden:

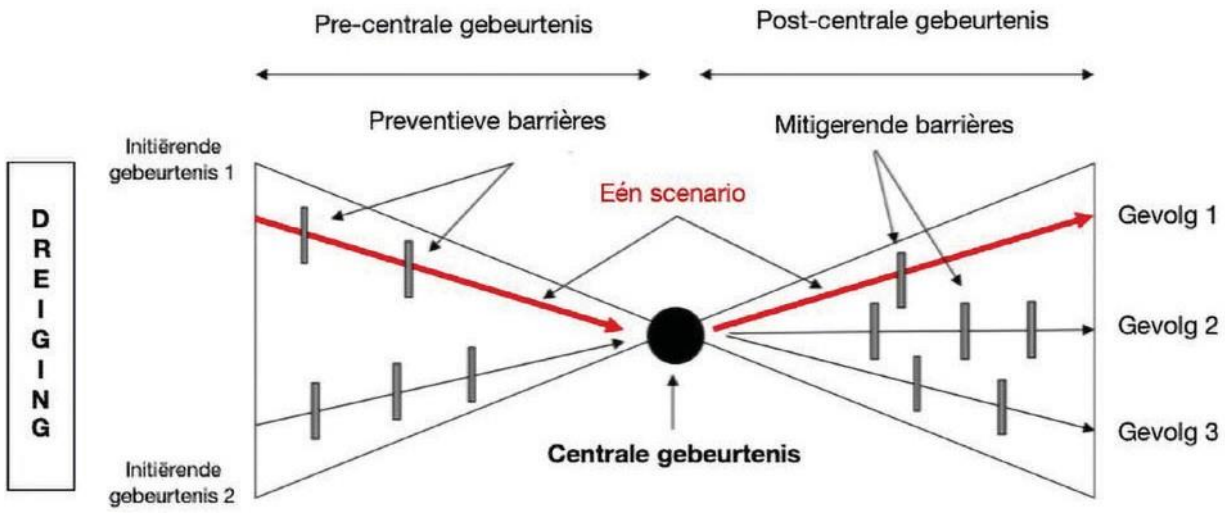
- Niet alle beveiligingsincidenten met een relatief kleine impact (type I) hebben hetzelfde potentieel om uit te monden in beveiligingsincidenten met een grote impact (type II). Ook omgekeerd ontstaat slechts een kleine subgroep van beveiligingsincidenten met een relatief kleine impact uit kwetsbaarheden die aan de basis liggen van beveiligingsincidenten met een grote impact;
- Beveiligingsincidenten met verschillende impact kunnen verschillende onderliggende oorzaken hebben;
- Het beperken van beveiligingsincidenten met een grote impact vereist vaak een andere aanpak dan het reduceren van incidenten met een relatief kleine impact;
- Strategieen die beveiligingsincidenten met een grote impact (zoals terrorisme) beperken, kunnen slechts in sommige gevallen gebruik maken van data die verkregen werd uit de analyse van incidenten met een relatief kleine impact.

Figuur 7 geeft de beveiligingsincidenten bipiramide weer, welke kan voorgesteld worden als twee piramides die elkaar deels overlappen. De linkse piramide geeft de type I beveiligingsrisico's aan die leiden tot ernstige incidenten (bv. een moord), maar niet tot een grote catastrofe. De rechtse piramide stelt de type II beveiligingsincidenten voor die kunnen leiden tot een echte intentionele ramp (bv. een terreuraanslag).

De bipiramide toont aan dat er een verschil is tussen de type I en type II beveiligingsrisico's. Dit houdt in dat relatief kleine beveiligingsincidenten met een grote waarschijnlijkheid, zoals diefstal, niet verward mogen worden met eerder grote maar minder waarschijnlijke incidenten, zoals terrorisme. Niet alle relatief kleine beveiligingsincidenten hebben de potentie in zich om tot een ramp te leiden, enkel een minderheid van deze incidenten eindigt in een beveiligingsgerelateerde catastrofe. Bijvoorbeeld: een diefstal van een toxisch product kan er toe leiden dat dit product later wordt gebruikt bij een terreuraanslag. Om grote catastrofes te vermijden, moet beveiligingsrisicomanagement zich richten op de twee types bevei-



Figuur 7 Het bipiramide model voor beveiligingsincidenten.



Figuur 8 De bow-tie techniek/metafoor toegepast binnen het beveiligingsdomein.

ligingsrisico's en niet enkel op de meest waarschijnlijke beveiligingsrisico's met een minder grote impact.

2.5. Het bow-tie model voor beveiliging

Het *bow-tie* model, of vlinderdasmodel, is een zeer krachtig model dat werd ontwikkeld binnen het veiligheidsdomein om een inzicht de krijgen in de mogelijke scenario's die gerelateerd zijn aan de 'centrale gebeurtenis' (bv. energieverlies, een lek) die zich in het midden van de *bow-tie* bevindt en leidt tot niet-intentionele verliezen. De *bow-tie* kan, net zoals het Zwitserse kaasmodel, beschouwd worden als een metafoor om ongevalsscenario's te visualiseren. De aanpak is ontstaan in de jaren '90 en wordt wereldwijd gebruikt bij de analyse van (grote) arbeidsveiligheids- en procesveiligheidsincidenten.

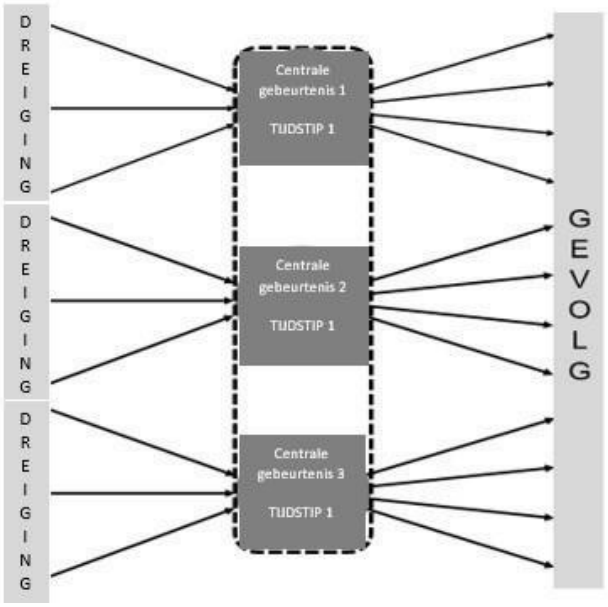
Wanneer we het model toepassen binnen het beveiligingsdomein kan er meer inzicht verkregen worden in alle oorzaken (dreigingen) en gevolgen (potentiele intentionele verliezen) van een specifieke ongewenste beveiligingsgerelateerde gebeurtenis (bv. een explosie door een succesvolle terroristische aanslag op doelwit X). De methode combineert de foutenboom met de gebeurtenissenboom en stelt verschillende scenario's voor in de vorm van de oorzaken van de centrale gebeurtenis, de gevolgen. De sterkte van de metafoor is het gebruik van barrieres: barrières die kunnen verhinderen dat de centrale gebeurtenis plaatsvindt (preventieve barrieres) en barrieres die de gevolgen mitigeren als er toch een centrale gebeurtenis plaatsvindt (mitigerende barrieres). In beveiligingstermen kan de *bow-tie* worden beschouwd als een metafoor voor een potentiele reeks van aanvalsprocessen met kwaadaardige acties die tot een reeks van potentiele gevolgen kan leiden. De *bow-tie* techniek wordt weergegeven in Figuur 8.

Om de betekenis van de 'centrale gebeurtenis' goed te begrijpen, is het belangrijk dat de relatie tussen het *bow-tie* model en de fysieke beveiliging wordt uitgelegd. Bij fysieke beveiliging ontstaat er een dreiging door het misbruik van de 'tegenstander', die een intentionele aanval op een doelwit uitvoert, bijvoorbeeld het laten vrijkomen van een gevaarlijke stof of energie (bv. in de vorm van een schokgolf). De 'centrale gebeurtenis' is in dit geval een situatie waarbij de dreiging (bv. het opzettelijk vrijlaten van een schadelijke stof of energie) oncontroleerbaar is geworden. Zoals reeds werd aangegeven is het gevaar het intrinsieke vermogen om elke vorm/type van verliezen te veroorzaken (van intentionele of niet-intentionele aard). Cockshott (2005) beschrijft gevaar als een conditie die zou kunnen leiden tot verwondingen of schade aan eigendommen of de omgeving. Wanneer de initiele oorzaak vrij wordt vertaald naar een effect, wordt het effect weerspiegeld in de centrale gebeurtenis en kan dit worden gedefinieerd als het directe resultaat van het vrijkomen van een gevaar. Aan de rechterkant van de *bow-tie* ontwikkelt het scenario zich verder richting de uiteindelijke gevolgen, zoals bijvoorbeeld slachtoffers, gewonden, schade of productieverliezen. Het is belangrijk om op te merken dat er op het vlak van beveiliging gelijktijdig meerdere centrale gebeurtenissen kunnen plaatsvinden (zie Figuur 9). Zo kunnen er op hetzelfde moment bijvoorbeeld drie installaties tot ontploffing worden gebracht (van Nunen et al., 2019).

3. Beveiligingsbeginselen op basis van het safety domein

3.1. Het inherente veiligheids-/beveiligingsbeginsel

De eerste en belangrijkste aanpak om met veiligheids- en beveiligingsproblemen om te gaan, is het wegnemen van het gevaar of de dreiging. Wanneer het gevaar of de dreiging niet aanwezig is, kan er geen ongewenste gebeurtenis meer plaatsvinden, of deze nu wel of niet op een intentionele wijze wordt veroorzaakt. Daarnaast leidt inherente veiligheid ook tot inherente beveiliging: als er geen gevaarlijke precondities meer bestaan waarvan de tegenstander gebruik kan maken, zal het doelwit niet meer als aantrekkelijk worden beschouwd en zullen er



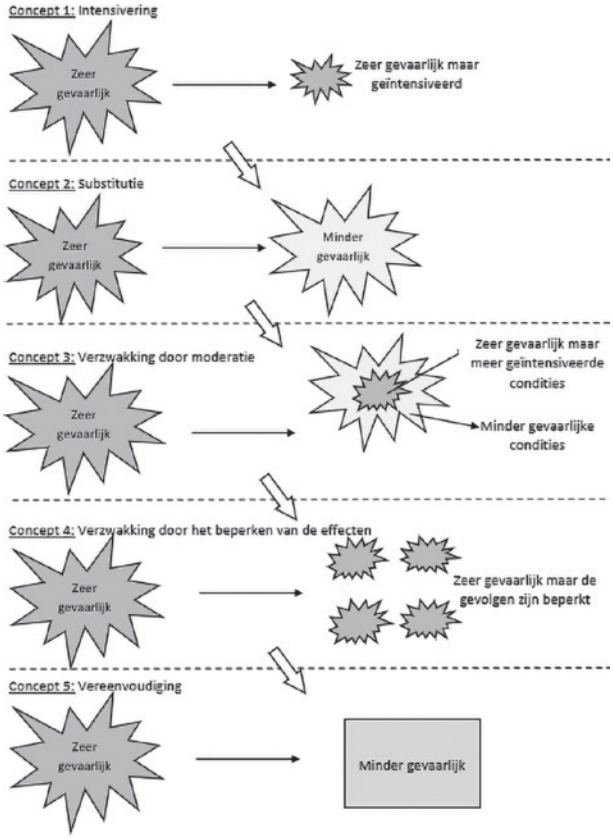
Figuur 9 Gelijktijdige centrale gebeurtenissen bij security gerelateerde gebeurtenissen, overgenomen van van *Nunen et al. (2019).*

geen dreigingen meer zijn. Dit houdt in dat er in dit geval geen beveiligingsrisico's en geen beveiligings-gerelateerde gevaren bestaan. Het uitgangspunt van inherente veiligheid bestaat uit vijf concepten: intensivering, vervanging/ substitutie, verzwakking door moderatie, verzwakking door een beperking van de effecten en vereenvoudiging. De concepten worden weergegeven in Figuur 10.

Deze concepten werden ontwikkeld door Kletz (1998) binnen een veiligheidscontext en verder verbeterd door Kletz en Amyotte (2010). Toegepast op beveiliging houdt het eerste concept, intensivering, in dat de beveiliging kan worden verhoogd door een verbetering van de activiteiten en/of processen (bv. door een verminderd gebruik van toxische producten of het aanbieden van meer *security awareness* trainingen). Het is bij dit concept belangrijk dat er geverifieerd wordt dat er geen risicohomeostase plaatsvindt aangezien verschillende bedrijfsomstandigheden kunnen leiden tot andere risico's of een verplaatsing van het risico (bv. snelle uitbreiding van het bedrijf waardoor *security awareness* trainingen niet consistent aan nieuwe werknemers worden gegeven). In dit laatste geval blijft het gehele risico bestaan. Het tweede concept, vervanging, houdt in dat stoffen en procedures worden vervangen door minder gevaarlijke varianten. Dit kan bijvoorbeeld door water te gebruiken voor vloeistof-vloeistofextractie in plaats van een ontvlambaar solvent. Er dient ook hier echter mee rekening gehouden te worden dat het risico niet zomaar kan vervangen worden aangezien vervanging nieuwe risico's kan inhouden door het aanpassen van de bestaande processen en activiteiten. Het derde concept, verzwakking door moderatie, houdt in dat de beveiliging verbeterd wordt door het creeren van betere omstandigheden. Het gaat hier bijvoorbeeld om een verbeterde/ sterkere persoonlijke uitrusting of het beperkt toegankelijk maken van bepaalde ruimtes. Het vierde concept, verzwakking door het beperken van de effecten, houdt in dat het altijd beter is om het totale aantal potentiele gevolgen van een ongewenste gebeurtenis zoveel mogelijk te reduceren. Het uitgangspunt hierbij is dat het beperken van de gemeenschappelijke verliezen van een gebeurtenis de ernst van elke andere ongewenste gebeurtenis zal beperken. Dit kan bijvoorbeeld door afscheiding via het splitsen van de eenheden met een hoog beveiligingsrisico. Een andere manier is het dupliceren van kritische eenheden die essentieel zijn voor het voortbestaan van een bedrijf (bv. computerservers met klanteninformatie voor een bank). Het vijfde concept, vereenvoudiging, vertrekt vanuit de eenvoudige observatie dat complexe processen en situaties altijd gevaarlijker zijn dan eenvoudige. Dit is te wijten aan het feit dat het veel makkelijker is om hiaten in de beveiliging van complexe faciliteiten te vinden dan in eenvoudige.

3.2. Het STOP-principe

Indien het niet mogelijk is om het inherente veiligheids-/ beveiligingsbeginsel toe te passen en het gevaar of de dreiging te verwijderen, moet er geopteerd worden voor veiligheids- of beveiligingsmaatregelen. Dit kunnen technische, organisatorische en, als laatste redmiddel, menselijke/persoonlijke maatregelen zijn.
Op het vlak van beveiliging benadrukt het STOP-principe



Figuur 10 Vijf concepten van inherente veiligheid/beveiliging (Kletz en Amyotte, 2010).

(strategische, technische, organisatorische en persoonlijke maatregelen) (zie Meyer en Reniers, 2016) deze aanpak door prioriteit te geven aan volgende maatregelen:

1) Strategische maatregelen: strategische vervanging van processen of stoffen die tot een minder gevaarlijk/ bedreigend resultaat leiden, het verlaten van een proces of product of het aanpassen van het finale product (wat neerkomt op het inherente veiligheids-/ beveiligingsbeginsel).
2) Technische maatregelen: de technische bescherming tegen gevaarlijke/bedreigende fenomenen die niet geelimineerd kunnen worden, het verlagen van de waarschijnlijkheid dat een aanval op een succesvolle wijze wordt uitgevoerd (Landucci et al., 2017), het reduceren van de aantrekkelijkheid van het doelwit (Argenti et al., 2015), het verminderen van de kwetsbaarheid (Argenti et al., 2018) of het beperken van het bereik van de impact (bv. isolatie of scheiding, automatisering, firewall, EX zones, bewakingsagenten).
3) Organisatorische maatregelen: Organisatorische aanpassingen van het werk zelf of het voorzien van opleidingsschema's, beveiligingsinstructies en informatie omtrent het omgaan met de nog bestaande beveiligingsrisico's (bv. *awareness* trainingen, communicatieplannen, supervisie, waarschuwingstekens)
4) Persoonlijke maatregelen: het beveiligen van mensen door bijvoorbeeld persoonlijke beschermingsuitrustingen, het verbeteren van de beveiligingscultuur en – klimaat, trainingen omtrent beveiliging of communicatie over beveiliging.

Het STOP-principe stelt daarnaast een hierarchie op om bovenstaande maatregelen te implementeren:

1) Focus op de *bron*: in het geval van beveiliging kan de bron worden beschouwd als de aanvaller, de persoon met kwaadaardige bedoelingen. Hij/zij moet zoveel mogelijk uit de organisatie worden gehouden.
2) Focus op de *interface* of het traject tussen de bron en het doelwit: een beperking van de beweegruimte van de dader (bv. door infrastructurele barrieres), de onderschepping of neutralisering van de dader, menselijke controle (bv. door het beperken van toegangswegen of het creeren van bewustzijn) of bewaking (bv. door camera's en sensoren of alarmen).
3) Focus op het *doelwit* en afhankelijk van het type doelwit:
   (i) Infrastructuur: het reduceren van het risico (bv. vervangen van producten of processen, neutralisatie ter plaatse), het beperken van de doelwitrisico's (bv. versterking van het systeem, verlaging van de energieniveaus), voorspellende maatregelen (bv. breekschijf, kleppen), toezicht (bv. camera's en sensoren aan de installaties) en het vergroten van het beveiligingsbewustzijn en sociale controle op de site.
   (ii) Menselijk kapitaal: het verminderen van de kwetsbaarheid (bv. persoonlijke beveiliging en beschermende uitrusting, speciale training), beperken van de blootstelling (bv. automatisering), beperken van de tijd (bv. jobrotatie) en supervisie (bv. individuele blootstelling, biologische monitoring, medische survey, de juiste uitrusting en het volgen van regels).

Over het algemeen moeten deze maatregelen gecombineerd worden om het gewenste beveiligingsniveau te behalen, zoals reeds werd weergegeven in het *Rings of Protection* model. Het is belangrijk dat de keuze voor een beveiligingsmaatregel ertoe leidt dat de waarschijnlijkheid, blootstelling en ernst van de dreigende gebeurtenissen wordt beperkt. Zodra de prioriteiten gesteld zijn, is het mogelijk om de juiste methode te selecteren om op een adequate manier om te gaan met elk van de ge"dentificeerde beveiligingsrisico's.

Tabel 2 geeft een samenvattend overzicht weer van de ordening van de maatregelen en de omgeving die in beschouwing wordt genomen, samen met enkele illustratieve voorbeelden voor elke categorie. De richting van deze aanpak gaat van boven tot onder en dan van links naar rechts. Het elimineren van het gevaar is de meest gepaste aanpak om de risico's te beperken; geen gevaar, geen dreiging, geen risico. Vervanging is interessant zolang er geen nieuwe gevaren of dreigingen gecreeerd worden. In het STOP-principe worden eliminatie en vervanging opgenomen in de strategische maatregelen. Ze zijn echter maar zelden mogelijk in praktijk en soms zelf helemaal niet toepasbaar.

Het is belangrijk om op te merken dat in de veiligheidspraktijk persoonlijke beschermingsmaatregelen vaak worden ingevoerd vooraleer de technische en organisatorische maatregelen worden ingevoerd. Redenen hiervoor zijn onder andere de lagere kosten of de makkelijke invoering van persoonlijke beschermingsmaatregelen. Daarnaast is er voor de invoering van technische en organisatorische maatregelen meer tijd nodig om de situatie grondig te analyseren en zorgen deze maatregelen soms voor verlies aan verantwoordelijkheid. In beveiliging is dit niet steeds het geval en wordt de nadruk veelal op technische maatregelen gelegd. Het is echter aangewezen om te investeren in zowel personeel, processen als technologie om beveiligingsrisico's optimaal te beheersen. Om beveiliging op een efficiente en effectieve manier te beheersen, moet de blootstelling van de organisatie aan negatieve gebeurtenissen worden beperkt. Dit kan gebeuren door te focussen op de drie niveaus tegelijk, die strategische, technische, organisatorische en persoonlijke maatregelen inhouden.

4. Discussie

Dit artikel toont aan dat de modellen en metaforen die worden aangewend om veiligheidsgerelateerde (niet-intentionele) gebeurtenissen te identificeren eveneens toepasbaar zijn om intentionele gebeurtenissen op het vlak van beveiliging in kaart te brengen.

Tabel 2 De STOP-tabel voor beveiliging met illustratieve voorbeelden (niet-limitatieve lijst).

	Aan de bron (Buitenste ring)	**Aan de *interface*** (Middelste ring)	**Aan het doelwit** (Binnenste ring)
Maatregelen **S** (strategie)	• Substitutie • Veranderingsprocessen	• Automatisering, telemanipulatie • Ruimtelijke ordening • Redundantie van kritieke systemen • Crime Prevention Through Environmental Design (CPTED)	• Criteria voor de selectie van beveiligingsbewuste operatoren • Afgedwongen infrastructuur
Maatregelen **T** (technologisch)	• Camera's/ intrusiedetectie • Hekken • Bolders en greppels • Intrusiesensoren • Deuren met sloten • Toegangscontrole-systemen • Tourniquets		• Sloten op deuren en kasten • Netwerk firewalls en paswoorden • Bewakingscamera's
Maatregelen **O** (organisatorisch)	• Bewakingsagenten aan de buitenrand van de site • Identiteitscontrole aan de ingang	• Escortbeleid voor bezoekers • Receptionisten in gebouwen • Badgecontroles	• Beveiligingsinstructies • *Intelligence* • Noodplannen • Vernietigen van documenten
Maatregelen **P** (persoonlijk)	• Opleiding/training van bewakingspersoneel	• Informatie/instructies over dreigingen	• Instructies omtrent het gebruik van beveiligingsuitrusting

Er moet opgemerkt worden dat er bij het inschatten van veiligheidsrisico's gesteund kan worden op een grote beschikbaarheid aan data. Hoewel er op het vlak van beveiliging ook enkele databanken kunnen geraadpleegd worden, zoals de Global Terrorism Database (START, 2018), de Repository of Industrial Security Incidents (RISI) (Department of Homeland Security, 2017) of de officiele criminaliteitsstatistieken van de Federale Politie (Federale Politie, 2018), is deze data niet altijd volledig of soms zelfs ongeldig (Reniers et al., 2019). Het vormt een grote uitdaging om met deze gegevens aan de slag te gaan, maar het is toch belangrijk dat de beveiligingsrisico's op een adequate wijze worden beheerst. Hierin schuilt het belang van efficient risicomanagement.

Hoewel de domeinen veiligheid en beveiliging veel met elkaar gemeenschappelijk hebben, vereisen ze, zoals reeds werd weergegeven, een verschillende mate van transparantie. Bij het verspreiden van de informatie die voortkomt uit de toepassing van de modellen en metaforen moet daarom rekening gehouden worden met een beperkte mate van transparantie op het vlak van beveiliging. Het niet afschermen van bepaalde informatie kan namelijk voor extra dreigingen zorgen aangezien de kwetsbaarheden en potentiele verliezen van de organisatie worden blootgelegd (Deleuze et al., 2008). De verkregen informatie moet daarom beschouwd worden als een persoonlijk bezit van de organisatie die enkel gedeeld wordt binnen de *trusted community* of de individuen die een *need to know* hebben.

Naast de mate van transparantie verschillen beide domeinen in de aanwezigheid van een kwaadwillige intentie bij de dader. Terwijl veiligheidsincidenten op een niet-intentionele wijze worden veroorzaakt, is er steeds een 'intelligente tegenstander' aanwezig in het geval van een beveiligingsdreiging. De voorgestelde veiligheidsmodellen geven echter slechts beperkt weer welke dader-specifieke elementen meespelen in het tot stand komen van een dreigingsscenario. Het Nationaal Veiligheidsprofiel (NVP), dat werd opgemaakt door de Nederlandse Overheid (Analistennetwerk Nationale Veiligheid, 2016), stelt voor om voor elk soort risico verschillende bouwstenen te integreren. Indien het om gebeurtenissen met moedwillige oorzaak gaat, worden de bouwstenen 'actor' en 'motief' toegevoegd. Dit laat toe beveiligingsmaatregelen zo goed mogelijk af te stemmen op de dader en zijn intentie.

Tot slot omschrijven Reniers et al. (2019) een efficient risicomanagementproces als zeer dynamisch, iteratief en voorbereid op mogelijke veranderingen. De beveiligingssector wordt gekenmerkt door voortdurende verandering. Interne en externe gebeurtenissen zorgen ervoor dat dreigingen snel kunnen wijzigen, minder van belang worden of dat er nieuwe dreigingen ontstaan. Zowel interne veranderingen als externe wijzigingen zoals verschuivingen in het politieke klimaat, verbeteringen in de capaciteiten van de tegenstanders of nieuwe trends in misdaadfenomenen hebben een invloed op het risicomanagementproces. Het is belangrijk dat het bedrijf hierop voorbereid is en dat het risicomanagement niet op een statische maar dynamische manier wordt uitgevoerd (Moore, 2013; Moteff, 2005).

5. Conclusie

In vergelijking met veiligheid is fysieke beveiliging een relatief nieuw wetenschapsdomein. Door de groeiende relatie tussen burgers en de multidimensionale oorsprong van dreigingen die een impact hebben op het industriele

en publieke domein verovert het steeds meer een eigen plaats in de academische wereld. De maturiteit van wetenschappelijk onderzoek naar beveiligingsmanagement staat nog steeds op een laag niveau, maar groeit langzaamaan. Aangezien zowel veiligheid als beveiliging gefocust zijn op het vermijden of verminderen van verliezen, kunnen er analogieen getrokken worden tussen beide domeinen. Net omdat er nog maar weinig wetenschappelijke studies voorhanden zijn met betrekking tot risicoanalysemodellen binnen het fysieke beveiligingsdomein, is het interessant om reeds ontwikkelde modellen en metaforen op het vlak van veiligheid (*safety*) te projecteren op het fysieke beveiligingsdomein (*security*). In dit artikel werden enkele van die centrale concepten, modellen en metaforen uit het veiligheidsdomein toegepast op het beveiligingsdomein, met focus op het beheersen van beveiligingsrisico's.

Literatuur

Analistennetwerk Nationale Veiligheid (2016). Nationaal Veiligheidsprofiel 2016, https://www.nctv.nl/binaries/Nationaal%20Veiligheidsprofiel%202016_tcm31-232083.pdf

Argenti, F., Landucci, G., Spadoni, G., Cozzani, V. (2015). The assessment of the attractiveness of process facilities to terrorist attacks. *Safety Science, 77*, 169-181.

Argenti, F., Landucci, G., Reniers, G., Cozzani, V. (2018). Vulnerability assessment of chemical facilities to intentional attacks based on Bayesian Network. *Reliability Engineering & System Safety, 169*, 515-530.

Baybutt, P. (2017). Issues for security risk assessment in the process industries. J*ournal of Loss Prevention in the Process Industries, 49*, 509-518.

Bird, E., Germain, G.L. (1985). *Practical Loss Control Leadership, the conservation of people, property, process, and profits.* Loganville, GA: Institute Publishing.

CCPS - Center of Chemical Process Safety (2000). *Guideline for chemical process quantitative risk analysis.* American Institute of Chemical Engineers - Center of Chemical Process Safety, New York, NY.

CCPS, Center for Chemical Process Safety (2003). *Guidelines for analyzing and managing the security vulnerabilities of fixed chemical sites.* New York: American Institute of Chemical Engineers.

Cockshot, J.E. (2005). Probability Bow-Ties - A Transparent Risk Management Tool. *Process Safety and Environmental Protection, 83*(B4), 307-316.

Deleuze, G., Chatelet, E., Laclemence, P., Piwowar, J., & Affeltranger, B. (2008). *Are safety and security in industrial systems antagonistic or complementary issues?* Paper gepresenteerd op Proceedings of the 17th European Safety and Reliability Conference (ESREL'08).

Department of Homeland Security. (2017). Chemical Facility Anti-Terrorism Standards (CFATS). https://www.cisa.gov/chemical-facility-anti-terrorism-standards

Federale Politie. (2018). Criminaliteitsstatistieken. http://www.stat.policefederale.be/criminaliteitsstatistieken/

Heinrich, H.W. (1950). *Industrial accident prevention.* 3rd Ed., New York: McGrawHill Book Company.

International Organisation of Standardization (ISO) (2009). *Risk Management Standard - Principles and Guidelines.* Geneva, Switzerland: ISO.

James, B., Fullman, P. (1994). Construction safety, security and loss prevention. New York: Wiley Interscience.

Kamoun, F., & Nicho, M. (2014). Human and organizational factors of healthcare data breaches: The swiss cheese model of data breach causation and prevention. *International Journal of Healthcare Information Systems and Informatics (IJHISI}, 9*, 42-60.

Khakzad, N., Khan, F., Amyotte, P., Cozzani, V. (2013). Domino Effect Analysis Using Bayesian Networks. *Risk Analysis, 33*, 292-306.

Kletz, T. (1998). *Process plants. A handbook for inherently safer design.* Ann Arbor, USA: Braun-Brumfield.

Kletz, T., Amyotte, P. (2010). *A handbook for inherently safer design.* 2nd Ed., Boca Raton, USA: CRC Press.

Kortekaas, J. (2005). *Risicoanalyse georganiseerde criminaliteit: Uitwerking instrumentarium en toepassing op ICT-ontwikkelingen.* 's-Gravenhage: Reed Business Information bv.

Landucci, G., Argenti, F., Cozzani, V., Reniers, G. (2017). Assessment of attack likelihood to support security risk assessment studies for chemical facilities. *Process Safety and Environmental Protection, 110*, 102-114.

Meyer, T., Reniers, G. (2016). *Engineering risk management*, 2nd Ed., Berlin: De Gruyter.

Moteff, J. (2005). Risk management and critical infrastructure protection: Assessing, integrating, and managing threats, vulnerabilities and consequences. https://fas.org/sgp/crs/homesec/RL32561.pdf

Reason. (1990). *Human error.* Cambridge, MA: Cambridge University Press.

Reason, J.T. (1997). *Managing the risks of organisational accidents.* Aldershot, UK: Ashgate Publishing Limited.

Reason. (2016). *Managing the risks of organizational accidents.* Routledge.

Sas M, van Nunen K, Reniers G, Ponnet K, Hardyns W. (2019). When safety meets security. *Veiligheidsnieuws Prebes, 204*, 6-10.

START. (2018). Global Terrorism Database. https://datacatalog.worldbank.org/dataset/world-external-geospatial-platforms

Talbot, J., & Jakeman, M. (2008). Security Risk Management Body of Knowledge. Australia: Risk Management Institution of Australasia Limited.

van Nunen Karolien, Reniers, G., Swuste, P. (2019). Verkennende studie naar (petro)chemische clusters en veiligheid: Veiligheidsparameters binnen (petro)chemische clusters en losstaande (petro)chemische bedrijven. Onderzoeksrapport in opdracht van het Nederlandse Ministerie van Infrastructuur en Waterstaat (Mei 2019). https://dv2030.nl/.

van Nunen K, Sas M, Reniers G, Vierendeels G, Ponnet W, Hardyns W. (2018). An integrative conceptual framework for physical security culture in organisations. *Journal of Integrated Security Science, 2*(1), p. 25-32. https://doi.org/10.18757/jiss.2018.1.1986