Safety & Security. Is er synergie voor bedrijven? Of moet het apart blijven?

Verslag CGC-NVVK-bijeenkomst 21 januari 2010

Mat Jongen en Paul Swuste

Met de terroristische aanslagen van de laatste decennia is een nieuwe dimensie toegevoegd aan het veiligheidsdenken, zeker in tak van de industrie die grote hoeveelheden gevaarlijke stoffen produceert, transporteert of gebruikt. Vooral in de delen van West-Europa met veel chemische industrie, zoals bijvoorbeeld in Nederland, België en Duitsland, speelt dit een grote rol.
Safety' en 'security' zijn twee aspecten van veiligheid voor 'kwetsbare' bedrijven. Voor veiligheid is in de afgelopen decennia een groot aantal methoden ontwikkeld om het veiligheidsmanagement te verbeteren met ongevalanalysemethodieken, veiligheidscultuurprogramma's, leren van incidenten, etcetera. Hetzelfde geldt voor securitymanagement. De Nederlandse en Europese overheden stellen al lang veel eisen aan het veiligheidsmanagement van bedrijven veel met gevaarlijke stoffen wordt gewerkt. Inmiddels geldt dit ook steeds vaker voor het securitymanagement van die bedrijven. VNCI en het ministerie van VROM hebben hierover in 2009 zelfs een convenant afgesloten. Security-kwesties spelen een steeds belangrijkere rol, naast de al bestaande veiligheidssystemen.

Het thema van deze middag is de vraag of er synergie mogelijk is tussen deze twee aspecten van het managementsysteem van bedrijven. Zijn ontwikkelingen op veiligheidsgebied toepasbaar op security en andersom? De sprekers gingen in op de overeenkomsten en verschillen tussen de twee vakgebieden, de praktijk van een security-bedrijf, onderzoek naar security en de ontwikkelingen in hun vakgebied die interessant zijn voor het andere vakgebied.

Coen van Gulijk van de Safety Science Group van de TU Delft gaf een verhandeling over de historische ontwikkeling van de managementmodellen voor zowel safety als security, waarbij de traditie van security veel verder terug gaat dan die van safety. Safety komt op met het begin van de industrialisering aan het einde van de 19de, begin 20ste eeuw. Het doel hiervanis productieverlies en verlies van mensenlevens in bedrijven te voorkomen. Security in algemene zin gaat terug tot het beschermen van belangen waarbij je kunt denken aan alle militaire ontwikkelingen, de ontwikkeling van de politie, bedrijfsbeveiliging, etcetera. Hierbij hebben diverse specialistische gebieden zich redelijk zelfstandig ontwikkeld in de afgelopen decennia. Hij noemt dit de blauwe (politie), witte (medische hulpdiensten), rode (brandweer) en groene (militaire) kokers, naast die van de bedrijfsveiligheid.
Gemeenschappelijk factoren van security en safety zijn het voorkomen van ongewenste effecten op een bedrijf of de samenleving in het algemeen. Tegelijkertijd zijn ze beide volkomen los van elkaar ontwikkeld. Het gaat om zeer verschillende actoren en werkwijzen. Als je wil weten of er synergie mogelijk is, kun je twee benaderingen toepassen: (1) nagaan welke managementmodellen er bestaan voor security en safety en of daar overlap in zit, of (2) proberen om de actoren in de twee kolommen - in ieder geval op bedrijfsniveau - te laten samenwerken. In zijn presentatie doet Van Gulijk een poging om de verschillende modellen naast elkaar te zetten. Voor security maakt hij daarvoor gebruik van een recent overzicht van best practices van Talbot et al. uit 2008[1], Waarin het Security Risk Management Body of Knowledge (SRMBOK) wordt behandeld. Hierin worden alle aspecten van security-management benoemd. Kernpunt hierbij is "asset protection", het beschermen van bezittingen. Dit omvat de vijf vakgebieden informatiebeveiliging, fysieke beveiliging, ICT-beveiliging, beveiliging van personen, en management van het geheel. Daarnaast wordt wat in Nederland bekend is als de veiligheidsketen van informatieverzameling, preventie, reageren op incidenten en het herstel na security incidenten (naar analogie van proactie-preventie-preparatie-repressie-nazorg) besproken. "Business resilience" is het onderdeel van dit model waarin de weerbaarheid of het weer opstarten van productieprocessen na een security-incident aan de orde komen.

Naast dit algemene model komen in security de volgende modellen voor, die ook in de veiligheidskunde van belang zijn, van het "Zwitserse kaas model" waarin op een schematische manier de lekken in verschillende barrières tegen ongewenste gebeurtenissen wordt uitgebeeld, het vlinderdasmodel ("bow tie") voor incidentonderzoek, het LOPA-denkmodel ("layers of protection"), de foutenbooom-methodologie, systeemanalyses, de veiligheidsketen, leermodellen (van onbewust onbekwaam tot onbewust bekwaam), bestuursstructuren van ondernemingen, tot het gebruik van een risicomatrix waarin de effecten van ongewenste gebeurtenissen worden afgezet tegen hun waarschijnlijkheid van optreden.
De conclusie van de presentatie is dan ook dat veel van de denkmodellen in principe hetzelfde zijn, maar dat ze

[1] *Talbot, J., Jakeman, M. (2008) SRMBOK, Riskmanagement Institution of Australasia Limited, Australia. John Wiley and Sons, New Jersey, USA*

inhoudelijk anders worden ingevuld, en dat beide velden van elkaar kunnen leren. Zo kan veiligheid leren van het resilience model dat voor security is ontwikkeld. Aan de andere kant zijn de verschillen in openheid, de afkomst uit verschillende tradities en het grote verschil in actoren oorzaak van het feit dat er in de praktijk niet veel van synergie is waar te nemen.

Martijn Neef van TNO Defensie & Veiligheid presenteerde de laatste ontwikkelingen uit het security-onderzoek van TNO, over ontwikkelingen die mogelijk toepasbaar zijn bij het hanteren van complexe veiligheidsystemen in de industrie. Zijn stelling is dat deze "genetwerkte systemen" snel in aantal toenemen, ook daar waar grote risico's aanwezig zijn. En juist daar moeten vaak op korte termijn belangrijke beslissingen worden genomen. Het is van groot belang dat bedrijfsprocessen, organisatiestructuren en mensen daarin mee groeien. Het kernmerk van deze systemen is dat mensen beslissingen moeten nemen op basis van gegevens van tal van technische systemen waarin terugkoppelingen met andere systemen plaatsvinden. Voorbeelden zijn de interactie tussen de mens en steeds intelligenter wordende auto's, de interactie tussen mensen, robots en computersystemen, de cockpit van ingewikkelde systemen zoals vliegtuigen of andere grote plants/installaties, en het gebruik van ruimtevoertuigen op grote afstand van de aarde. Naast het ontwikkelen van de techniek vergt dit aanpassingen van bedrijfsprocessen, organisatiestructuren en de mensen die met die systemen om moeten gaan. Een belangrijke boodschap van deze presentatie is dat het voor zowel safety- als securitysystemen van groot belang is dat mensen en machines goed kunnen samenwerken, omdat er grote risico's zijn en omdat er snel en goed geïnformeerd moet worden gehandeld bij incidenten of afwijkingen van de normale gang van zaken. Systemen waarin mensen en techniek nauw moeten samenwerken, moeten eigenlijk ook gelijktijdig worden ontworpen: co-ontwerp! Martijn Neef geeft een voorbeeld van hoe zo'n co-ontwerp er theoretisch uit zou moeten zien. Het voorbeeld omvat vijf ontwerpfasen, voorbeelden van gebruikersvragen, het opstellen van een programma van eisen waarin ook taken en gewenste gedragingen van het systeem worden vastgelegd, een model van de structuur en tot slot een ontwerp voor de implementatie. Hij laat drie basismodellen van de samenwerking tussen (teams van) mensen en intelligente sensornetwerken zien. Dit loopt uiteen van een model waarin alle mensen samenwerken met alle sensornetwerken (zelforganiserend netwerk), een model waarin de mensen de interactie met de sensornetwerken via één persoon laten lopen (hybride team met taakverdeling bij de mensen) en een model waarin de mensen afspreken wie met welk sensornetwerk contact houdt (team met sensor netwerk).

In zijn presentatie ging Martijn Neef in op de verschillende elementen waaruit zo'n gecombineerd systeem van mensen en machines kan bestaan in verschillende maten van complexiteit, met daarbij aangegeven wat de sterke en zwakke kanten van mensen en machines zijn in zo'n systeem en de daarbij behorende organisatie-, sociale en interactiemodellen. In het zogenaamde "Field Lab" onderzoekt TNO wat de rolveranderingen voor mensen en machines zijn in deze nieuwe samengestelde systemen. Zijn conclusies, die zowel voor safety- als voor security-systemen gelden, zijn dat de technologische ontwikkelingen ons dwingen om naar een integrale ontwikkeling van mens-machine-organisaties te kijken met co-ontwikkeling van techniek, organisatie en werkprocessen. Belangrijke aspecten hierin zijn hoe je afspraken maakt over de mate van autonomie van onderdelen, verdeling van taken en verantwoordelijkheden, en de mate van beheersing van de geautomatiseerde systemen. Hierbij moet geen overmatig vertrouwen zijn in de goede werking van technische systemen.

Het onderzoek wordt uitgevoerd in een drietal programma's: Programma Intelligente Sensor Netwerken van TNO, Delft Collaboration on Intelligent Systems (D-CIS), en in een groot multidisciplinair consortium onder de naam Interactive Collaborative Information Systems (ICIS).

Erik de Vries, Manager Consultancy van G4S, tevens voorzitter van het Benelux-chapter van de American Society for Industrial Security (ASIS), bespreekt het gebruik van organisatie(modellen) die gebruikt worden in het security-vakgebied. Er zijn uiteenlopende definities van de twee veiligheidsbegrippen security en safety. Kenmerkend is dat onveiligheid (voor security) door mensen wordt gecreëerd. In het geval van veiligheid in de zin van safety spelen meerdere factoren (zoals techniek) een rol. Basis is immers dat bij security-problemen menselijk opzet - en dan ook nog met kwade bedoelingen - het meest significante verschil is. Hij behandelt de diverse domeinen en denkmodellen die worden gebruikt voor security-management, waarbij opvalt dat er twee domeinen zijn die bij safety meestal minder aandacht krijgen, namelijk informatiebeveiliging en wettelijke aspecten. De denkmodellen die binnen security worden gebruikt zijn een risicoanalysemodel, een model voor het plannen van security-maatregelen, een "layered defence" model vergelijkbaar met het LOPA-model voor industriële veiligheid, en eem "systeem en dreiging"-model dat veel overeenkomsten vertoont met het vlinderdasmodel ("bow tie") model voor veiligheid. Een belangrijk verschil dat door diverse modellen heen loopt is dat bij veiligheid wordt gewerkt met kansberekeningen, iets dat bij security nauwelijks werkt omdat opzettelijke actie cq. dreiging moeilijk in kansberekeningen is te vatten. Bij veiligheid wordt gewerkt met normen zoals de kosten van ongevallen met letsel of het aantal ongevallen per miljoen gewerkte uren, iets dat bij security niet kan. Bij security lijkt perceptie van veiligheid daarom een grotere rol te spelen. Hij geeft vier voorbeelden van modellen die voor security worden gebruikt. Twee modellen zijn door ASIS ontwikkeld voor security management: een Amerikaanse nationale standaard voor de organisatie van resilience op security gebied (Hoe kan een bedrijf zijn continuïteit zo goed mogelijk waarborgen?), en de ISO 280001 voor securitymanagementsystemen met een plan-

do-check-cyclus. Een ander voorbeeld is het convenant dat in Nederland is afgesloten tussen de petrochemische industrie en de Nederlandse overheid in mei 2008, met afspraken over securitymanagement. Tenslotte behandelt hij het zogenaamde SRMBOK-model, dat probeert een integrale aanpak van securitymanagement te beschrijven, met alle in- en externe factoren die voor een bedrijf meespelen.

Kijkend naar synergie tussen safety- en securitymanagement komt hij tot de conclusie dat er veel overeenkomsten in systemen zijn, zoals risicoanalyses, audits en bewustzijn versterken. Verschillen zijn dat safety in de praktijk een betere wetenschappelijke onderbouwing heeft, tegenover een meer operationele aanpak voor security. Binnen bedrijven heeft safety een langere traditie dan security. Verder is safety meer aan wettelijke regels gebonden dan security, hoewel dat laatste wel begint te veranderen. De conclusie is dat er op theoretisch gebied veel overlap is, waarbij beide gebieden op sommige punten verder zijn ontwikkeld. Ze zouden elkaars methoden op diverse punten kunnen versterken. In de praktijk blijkt echter dat dit proces nog nauwelijks op gang is gekomen en dat de beide werelden elkaar (nog) nauwelijks begrijpen.

Victor Roggeveen heeft vooral ervaring met de safety-kant van veiligheid. Hij put uit zijn jarenlange ervaring als veiligheidskundige, vooral in de petrochemische industrie. Hij gaat in zijn presentatie dan ook in op de verschillen tussen niet opzettelijk veroorzaakte ongevallen (veiligheid - safety) en wel opzettelijk veroorzaakte ongevallen / incidenten (beveiliging - security). Hij gaat daarbij vooral in op de aard van het incident (bijvoorbeeld diefstal), de drijfveren en houding van de veroorzaker van een incident, de maatschappelijke acceptatie van de verschillende soorten incidenten, en het verschil in maatschappelijk inbedding van safety (wetten, bedrijfsregels, persoonlijk gedrag (“mores”)) en security (veel minder wetten, regels en gedragsregels). Om het verschil tussen safety en security te illustreren gaat hij dieper in op de oorzaken van incidenten. Bij alle incidenten spelen gedragsaspecten een belangrijke rol. En dat gedrag wordt bepaald door de organisatorische context waarin men opereert. Hij ziet ongewenst gedrag/fouten daarom als gevolgen van die context en niet als oorzaken van een incident. Foutieve gedragingen komen voort uit een falend organisatorisch systeem. Hij geeft daarbij een voorbeeld van een incidentanalysemodel dat hij gebruikt om bedoeld en onbedoeld ongewenst gedrag te kunnen onderscheiden, overigens zonder hier het opzettelijk veroorzaken van een incident in mee te nemen. Het betoog maakt duidelijk dat analyse van een incident en de omgang daarmee bij onopzettelijke incidenten weinig raakvlakken heeft met opzettelijk veroorzaakte incidenten. Zijn antwoord op de titelvraag van de bijeenkomst of er synergie moet zijn tussen safety- en securitymanagement is weergegeven in de subtitel van zijn presentatie: “een wereld van verschil”.

Paneldiscussie

In de afsluitende paneldiscussie werd intensief gesproken over de mogelijkheden van integratie van safety en security in het bedrijfsleven. De meningen varieerden van “we moeten van elkaar leren” tot “het zijn volledig gescheiden werelden met andere mensen en een andere cultuur”. In veel bedrijven zijn de stafafdelingen voor kwaliteit, milieu, safety en security binnen één staforgaan ondergebracht, zonder dat dit in de praktijk tot veel synergie in de uitvoering leidt. Het bij elkaar brengen van de twee werelden in het seminar heeft wel geleid tot een betere kennismaking en tot een eerste uitwisseling van kennis. Zowel in het safety- als het security-domein vinden nieuwe ontwikkelingen plaats die voor het andere domein interessant kunnen zijn. Victor Roggeveen (voormalig voorzitter en lid van het bestuur van de NVVK) gaf, de vergadering gehoord hebbende, aan dat hij de indruk had dat het merendeel van de aanwezigen voor integratie van safety en security is. Om die reden reageerde hij positief op het verzoek om het onderwerp in het bestuur van de NVVK aan de orde te brengen om de mogelijkheden tot synergie / kennisuitwisseling te onderzoeken.