Risicogestuurd
Kwaliteitsmanagement

Periodiek van de
Kwaliteitskring Twente

Samen voor verbetering

jaargang 30 • Themanummer 2017

INDUSTRIE FOOD OVERHEID FINANCE BOUW

Symbol
BUSINESS IMPROVEMENT

BUSINESS IMPROVEMENT

ADVIES, TRAINING & IMPLEMENTATIE

Organisatie-ontwikkeling

Proces-verbetering

Kwaliteits-management

Milieu & Veiligheid

WERKEN AAN 'WORLD CLASS PERFORMANCE'

Symbol begeleidt organisaties bij het realiseren van aantoonbare resultaten. We doen dit door het vertalen van de strategie naar een concreet implementatieplan, het uitvoeren en coachen van projecten en het overdragen van kennis. Ervaren (Master) Black Belts leiden medewerkers op in de methodieken en instrumenten van Lean en Six Sigma, en coachen hen in het uitvoeren van hun projecten.

In samenwerking met de LSSA (Lean Six Sigma Academy) en de Universiteit Twente wordt de mogelijkheid geboden om een Europees certificaat te behalen als Lean Six Sigma Green Belt of Black Belt.

Vraag onze trainingsgids aan via: *info@symbolbv.nl*

ENSCHEDE
Palatijn 14
7521 PN Enschede
T +31 (0)53-2030240
F +31 (0)53-2030241

AMERSFOORT
Maanlander 14
3824 MP Amersfoort
T +31 (0)33- 2030200

info@symbolbv.nl

WWW.SYMBOLBV.NL

Informatie over de Kwaliteitskring Twente

De vereniging KKT is op 23 augustus 1972 opgericht en heeft als doel een wezenlijke bijdrage te leveren aan het succes van ondernemingen en organisaties in de regio Twente en daarbuiten. Zij doet dit door de kennis en toepassing van Integrale Kwaliteitszorg en nieuwe managementtechnieken te bevorderen en daarbij nadrukkelijk de mens te betrekken.

Ereleden:

Dhr. M. Pot
Dhr. A. Meirik

Bestuur:

Henk-Jan Wegman	voorzitter
Elize Hulscher	secretaris
Eric van de Straat	penningmeester
Gerard Berendsen	opleidingscommissie
Johan Zemansky	programmacommissie
Nicole Mak	redactiecommissie

Inhoudsopgave

Van de voorzitter

De nieuwe Krul ligt weer voor u. Het is weer een prachtig magazine geworden met zeer veel interessante artikelen over "Risicogestuurd Kwaliteitsmanagement ", het centrale jaarthema waaraan de vereniging het afgelopen jaar haar activiteiten heeft gekoppeld
Vorig jaar zomer, toen wij over het thema nadachten, waren wij ons er niet van bewust dat risicogestuurd denken, niet alleen bij kwaliteitsmanagement een belangrijke rol ging spelen maar ook steeds meer in ons dagelijks leven.
Door de politieke ontwikkelingen en de onrust in de wereld zijn de afweging rondom risico's steeds belangrijker geworden. Durf je nog wel naar een evenement of een stad te bezoeken of schat je het risico te hoog in? Gelukkig doen wij dit nog steeds wel en laten wij ons niet afschrikken. Maar dit komt ook mede doordat wij vertrouwen hebben in het risicomanagement van de organisaties, overheden en bedrijven.
Dit risicogestuurd denken wordt vaak gefaciliteerd en gewaarborgd vanuit het kwaliteitsmanagement. Kennis van technieken en het in staat zijn om mensen te begeleiden, om vanuit hun specifieke expertise en taken, met een risico bril te kijken, dat zijn taken die steeds meer op het bord komen van de kwaliteitsmanager. Zoals reeds aangegeven komt dit niet alleen door de veranderingen in de ISO 9001:2015.
De verharding en polarisatie van de maatschappij, claimcultuur en zeker ook gewoon gezonde bedrijfsvoering vragen om gedegen kijk op risicogestuurd kwaliteitsmanagement.
Dit jaar hadden wij wederom een prachtig programma rondom dit thema, met zeer interessante bedrijfsbezoeken waar we veel hebben geleerd, kennis delende rondetafelgesprekken, en nu een boeiende diepgaande Krul.
Het is de redactie en de vele inbrengers gelukt om het thema van vele kanten te belichten en ook weer praktisch inhoud te geven. Wij mogen trots en dankbaar zijn op iedereen die weer vele uren in dit meer dan boeiend themanummer heeft gestoken.
Veel leesplezier

Henk-Jan Wegman
voorzitter

Van de redactie

Dit jaar heeft de KKT het thema "Risicogestuurd Kwaliteitsmanagement". Tijdens de bijeenkomsten is gebleken dat dit thema erg leeft bij u allen en er is dan ook al veel over dit onderwerp gesproken en gepresenteerd. Uiteraard staat ook de jaarlijkse uitgave van de Krul in het teken hiervan. De redactie en de schrijvers hebben hard gewerkt om u een inkijkje te geven in verschillende aspecten van risicogestuurd kwaliteitsmanagement.
Ook dit jaar is er weer een enorme diversiteit aan onderwerpen. Logisch, want risico's zijn overal. Zo krijgt u een kijkje achter de schermen bij het hanteren van risico's bij het hijsen en vervoeren van grote complexe installaties, bij medische hulpmiddelen, het gebruik van computers en internet en nog veel meer.
Bij deze wil ik de redactie leden, auteurs en adverteerders bedanken voor hun bijdrage aan dit themanummer.
Ik wens u allen veel leesplezier!

Nicole Mak

Een toelichting op ISO 9001:2015 vanuit de praktijk

Auteur: Onno Coster - Freelance adviseur van Coster Consult

10 Oktober 2015. Op het NEN-congres in Utrecht worden met feestelijk vertoon de nieuwe ISO-normen 9001 en 14001 gepresenteerd. De overgangstermijn voor reeds gecertificeerde organisaties bedraagt dan nog 3 jaar. Inmiddels zijn we anderhalf jaar verder. Auditors beginnen aan de nieuwe normen te wennen, veel organisaties hebben de nieuwe normen al geïmplementeerd en sommige andere organisaties worden zenuwachtig omdat ze uiterlijk volgend jaar toch echt 'over' moeten gaan om hun certificering te behouden.

In de afgelopen anderhalf jaar heb ik veel ervaring met ISO 9001:2015 opgedaan als adviseur bij industriële bedrijven. In dit artikel licht ik enkele begrippen van de norm toe, die in mijn praktijkervaring de belangrijkste zijn gebleken bij implementatie van de norm.

De basis van ISO 9001:2015

Het gedachtengoed van ISO 9001:2015 kan in drie vragen en acties worden samengevat.

- Waar wil je naar toe? Pas beleid toe dat stuurt op doelen.
- Waar ben je? Voer een context- en stakeholdersanalyse uit.
- Wat zou er onderweg kunnen gebeuren? Denk risicogebaseerd en pas hier je acties op aan.

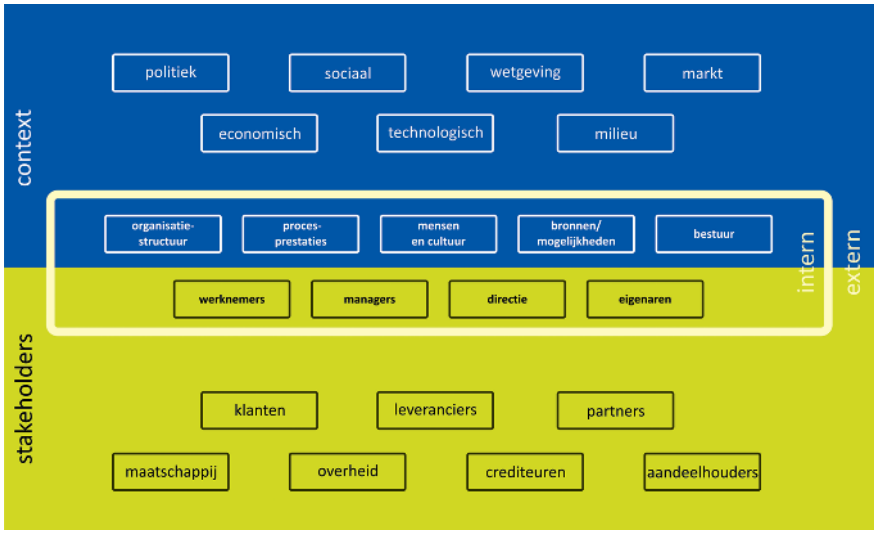
In essentie vormen deze uitgangspunten van de norm de basis voor een kwaliteitsmanagementsysteem. Als je dit op de juiste manier toepast, sluit het naadloos aan bij de principes van een goede bedrijfsvoering. Dat is ook logisch want kwaliteit wordt afgemeten aan de tevredenheid van klanten en de invloed op stakeholders, volgens de definitie uit ISO 9000. En tevredenheid van klanten is een voorwaarde voor continuïteit van je bedrijf.

Een toelichting op de uitgangspunten van de norm

De organisatie**doelen** zijn essentieel voor het te voeren beleid. Doelen maken resultaatgericht werken mogelijk. Zonder resultaten geen omzet. Zorg voor het vaststellen van heldere doelen op organisatieniveau en rol die uit via de managementlagen naar het uitvoerende niveau. Hier vinden namelijk de acties plaats die het resultaat zullen moeten vormen.

De **context** van de organisatie is het speelveld waarin de organisatie zich bevindt. Je kunt spreken van een externe context (zoals politiek, economisch, cultureel) en een interne context (zoals structuren, cultuur, kennis, technische mogelijkheden). Belanghebbenden (doorgaans **stakeholders** genoemd) zijn partijen waarmee je in deze context van doen hebt. Vanuit de context komen risico's op de organisatie af. Afbeelding 1 toont een overzicht van diverse aspecten van de context en van mogelijke stakeholders, zowel intern als extern. Een dergelijk overzicht kan gebruikt worden als inspiratiebron om de context en stakeholders van de organisatie vast te leggen.

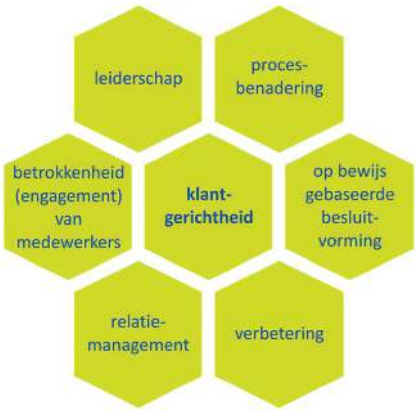
Risico's zijn effecten van onzekerheden. Onzekerheden kunnen voortkomen uit gebeurtenissen in de context.



Afbeelding 1 – Overzicht van context en stakeholders

Het mogelijke effect is dat ze het behalen van doelen positief of negatief kunnen beïnvloeden. Breng risico's in kaart en ga hier bewust mee om. Zet hiervoor bijvoorbeeld een risicotabel op; dit blijkt in de praktijk een handig hulpmiddel. Als een risico groot is, bepaal dan acties die zijn gericht op het optimaliseren van gewenste gebeurtenissen en gevolgen danwel op het voorkomen van ongewenste gebeurtenissen en het beperken ongewenste effecten. De risicotabel is dan een levend plan van aanpak voor het beheersen van risico's. Tip: denk ook aan de positieve risico's, ofwel kansen.

De managementprincipes van ISO 9001:2015



Afbeelding 2 – De 7 managementprincipes van ISO 9001:2015

ISO 9001:2015 geeft 7 managementprincipes waarmee invulling kan worden gegeven aan het kwaliteitsmanagementsysteem.

- Klantgerichtheid
- Leiderschap
- Procesbenadering
- Betrokkenheid (engagement) van medewerkers
- Op bewijs gebaseerde besluitvorming
- Relatiemanagement
- Verbetering

De kwaliteit van producten en diensten kun je afmeten aan de de tevredenheid van klanten. Benadruk bij het integreren van kwaliteit in de bedrijfsprocessen en het kweken van kwaliteitsbewustzijn dan ook dat het gaat over **klantgerichtheid** en het tevredenstellen van klanten en stakeholders. Een tevreden klant is niet alleen het resultaat van, maar ook een voorwaarde voor een succesvolle bedrijfsvoering. Overigens hebben interne processen ook interne klanten die tevreden moeten worden gesteld. Is de interne klant niet tevreden, dan is er een intern kwaliteitsprobleem.

Belangrijk bij het integreren van kwaliteit in de organisatie is een betrokken directie; deze heeft daarmee ook directe invloed op de betrokkenheid van medewerkers. Enkele kernbegrippen van goed **leiderschap**: zichtbaar zijn, een goede voorbeeldfunctie uitoefenen, heldere doelen stellen en communiceren, daadkrachtig aansturen, kwaliteitsbewustzijn tonen, maar ook luisteren naar de stakeholders en de organisatiecontext kennen en begrijpen. Naadloos zou de rol van het management hierop moeten aansluiten, de neuzen moeten dezelfde kant op staan. Missie, visie, strategie en beleid moeten eenieder helder voor ogen staan en er dient naar te worden gehandeld. Goede interne communicatie is hierbij van essentieel belang. Overigens is het principe van 'the golden circle' van Simon Sinek een leuke inspiratiebron voor het invullen van missie en visie (kijk maar eens op YouTube).

Kies bij het inrichten van de organisatie voor een **procesbenadering**, in plaats van de klassieke afdelingsbenadering. Bepaal wie de proceseigenaren zijn en wie de overige stakeholders zijn. Dit kunnen interne klanten of leveranciers zijn. Zorg voor gesmeerde communicatie en samenwerking tussen afdelingen om processen goed te laten functioneren.

Eigenaarschap verhoogt de **betrokkenheid van medewerkers**. Geef de proceseigenaar de controle over zijn proces, binnen de doelen en context van de organisatie. Laat de proceseigenaar het proces bepalen en beheersen, en laat hem verantwoording afleggen over resultaten.

Voor **op bewijs gebaseerde besluitvorming** heb je de juiste input en KPI's nodig waarmee je richting je doelen kunt sturen en belangrijke kwaliteitsrisico's kunt monitoren; niet meer, niet minder.

Op het gebied van **relatiemanagement** zou je kunnen zeggen dat de norm strenger is geworden. Er wordt van de organisatie niet alleen verwacht dat deze zijn leveranciers volgens de juiste criteria selecteert en evalueert, maar ook dat er relaties met leveranciers worden opgebouwd. Help je leveranciers met het leveren van de door jouw organisatie gevraagde kwaliteit; hiermee kweek je betrokkenheid bij de leverancier. Stel daarbij ten doel dat er minder uitval plaatsvindt in de keten (leverancier – afnemer) en dat er minder ingangscontrole nodig is in de eigen organisatie. Ook hier is goede onderlinge communicatie uitermate belangrijk.

Maak de PDCA-cyclus van **verbetering** rond door ook monitoring en evaluatie van geplande en ingezette acties uit te voeren. Wordt een actie vastgesteld om een risico te verkleinen? Monitor dan de uitvoering van die actie en evalueer of de actie effectief was. Gebruik de opgedane kennis om het proces nog beter aan te sturen. Zorg dat alle processen van dergelijke terugkoppellussen zijn voorzien. Ook hier kan de risicotabel als praktisch hulpmiddel worden ingezet.

Enkele andere aspecten van ISO 9001:2015

In ISO 9001:2015 wordt niet meer vereist dat de organisatie een **kwaliteitshandboek** heeft. Je bepaalt zelf op basis van de belangrijke uitgangspunten (doelen, context en stakeholders, risico's) wat nodig is om vast te leggen. Dit hoeft niet noodzakelijkerwijs in de

vorm van een kwaliteitshandboek. In de praktijk blijkt echter dat dit wel handig kan zijn om bijvoorbeeld directie, personeelsleden, auditors en potentiële klanten inzicht in en een overzicht van het kwaliteitsbeleid te bieden.

Ondanks dat de nieuwe norm geen procedure 'documentbeheer' meer vraagt, dient er wel degelijk '**gedocumenteerde informatie**' te worden bijgehouden. Enerzijds eist de norm bepaalde gedocumenteerde informatie, anderzijds bepaalt de organisatie zelf wat er nog meer nodig is om goed kwaliteitsmanagement te kunnen voeren. Ook hier geldt dat je dat kunt bepalen op basis van de uitgangspunten van de norm: doelen, context en stakeholders, risico's. Tip: een documentmanagementsysteem is een handig hulpmiddel om de gedocumenteerde informatie overzichtelijk te beheren.

Eisen aan de aspecten **kennis en competentie** zijn in de nieuwe norm verder aangescherpt. Kennisborging is een vorm van risicobeperking. De juiste competente werknemer op de juiste plek eveneens. Auditors vragen dan ook onverminderd naar competentie-overzichten. Als uitbreiding hierop bevat de norm nu ook een paragraaf 'Bewustzijn'. Personeel dient niet alleen de juiste kennis en competenties te bezitten, maar zich ook bewust te zijn van de invloed van hun werk op kwaliteit oftewel klanttevredenheid (zowel intern als extern).

Tot slot

ISO 9001:2015 is een norm die effectief kwaliteitsmanagement stimuleert. Goed kijken naar de organisatie en bewust omgaan met hierbij verkregen inzichten zal een positieve uitwerking hebben op de bedrijfsvoering. 'Goed kijken' betekent dan het kijken naar doelen, context, stakeholders en risico's van de organisatie en haar processen.

Externe auditors van certificerende instanties zullen meer moeite moeten doen dan bij de oude norm om dit 'goed kijken' en 'bewust omgaan met' te kunnen beoordelen. Er wordt bij audits dan ook steeds meer gekeken naar de processen zelf, en het daaraan gerelateerde kwaliteits- en risicobewustzijn, dan naar de vastlegging daarvan.

Mits goed geïmplementeerd komt komt het werken volgens de nieuwe ISO 9001 in de praktijk neer op meer bewustzijn, meer helderheid en minder overbodige regels en vastleggingen. Dit werkt prettiger en draagt bij aan tevreden klanten, de juiste omgang met stakeholders en een beter bedrijfsresultaat.

Onno Coster
Onno Coster is als zelfstandig consultant werkzaam op het gebied van ISO 9001, CE-markering van machines en documentatie. Na voltooiing van zijn studie Werktuigbouwkunde aan de Universiteit Twente in 1992 is hij gaan werken als consultant op het gebied van machineveiligheid. Hierbij heeft hij veel industriële bedrijven vanbinnen gezien en veel ervaring opgedaan met technische risicobeoordelingen. Vanaf 2000 heeft hij kwaliteitsfuncties bekleed in het bedrijfsleven, sinds 2005 als QA-manager. In deze functies heeft hij kwaliteitssystemen opgezet en geoptimaliseerd. De meeste opdrachtgevers van zijn huidige adviesbureau 'Coster Consult' zijn industriële maakbedrijven (MKB) in de regio Twente. Onno's passie ligt in het op eenvoudige wijze realiseren van een op de opdrachtgever toegespitst kwaliteitssysteem dat effectief is voor het bedrijf en tevens voldoet aan alle eisen van ISO 9001.

Over risicogestuurd kwaliteitsmanagement

Het jaarthema 2016-2017 van Kwaliteitskring Twente is 'Risicogestuurd Kwaliteitsmanagement'. Dit heeft te maken met de prominente plaats die risico's in ISO 9001:2015 innemen. Is dit risicodenken nieuw? Nee, niet helemaal. In de 2008-versie van ISO 9001 werd gesproken van 'preventieve maatregelen'. Deze werden in de praktijk door de meeste organisaties echter correctief toegepast. Als adviseur heb ik menig discussie gevoerd om dat besef door te laten dringen. In de nieuwe norm zijn de preventieve maatregelen onderdeel geworden van het 'risicogebaseerd denken'. Martin van Staveren beschrijft in zijn gelijknamige boek het 'risicogestuurd werken', als alternatief voor het traditionele risicomanagement. 'Risicogestuurd werken' is een pragmatische aanpak die het aantal regels en voorschriften binnen een organisatie tracht te beperken. In plaats daarvan wordt risicobewustzijn gekweekt. Dat een overdaad aan regels averechts kan werken wordt trouwens treffend beschreven in het boek 'Verdraaide organisaties' van Wouter Hart.

Het voorkomen van schade aan kabels en leidingen

Je staat er niet vaak bij stil, maar in Nederland bevindt zich ondergronds een netwerk van ruim 300.000 kilometer aan kabels en leidingen. Deze kabels en leidingen zijn van groot belang voor het functioneren van de maatschappij.

Met het toenemen van het netwerk steeg ook het aantal schades.
In 2015 waren er bijna 33.000 schades, bij elkaar goed voor een kostenpost van 26 miljoen euro.

Het percentage schadegevallen is de laatste jaren stabiel. De in het verleden opgestelde richtlijnen leken daarmee hun eindpunt te hebben bereikt. Omdat het hoge schadebedrag het belang van verdere reducering van schades onderstreept, is vanuit de sector via het Kennisplatform CROW een initiatief opgestart om de processen opnieuw te bekijken en te komen tot een nieuwe richtlijn. In deze werkgroep waren zowel aannemers, opdrachtgevers als netbeheerders vertegenwoordigd. Vanuit deze werkgroep is de CROW 500 richtlijn ontstaan: Schade voorkomen aan kabels en leidingen.

Waar in voorgaande versies de nadruk lag op het vergaren van informatie en het doen van graafmeldingen aangevuld met een voorgeschreven werkwijze, zien we in deze richtlijn de focus op de ketenverantwoordelijkheid.

Het ontstaan van schade is te herleiden naar twee oorzaken:
1) De graafwerkzaamheden worden niet correct uitgevoerd;
2) De beschikbare informatie is onvolledig en/of onjuist.

In de regel ontstaan de schades bij graafwerkzaamheden in de ondergrond. Dat graven in de ondergrond noemen we grondroeren en omvat werkzaamheden zoals mechanisch graven, heien, baggeren en het slaan van damwanden.

Van alle graafmeldingen leidt circa 6% tot schade aan kabels en leidingen. Op het moment dat schade aan kabels en leidingen ontstaat kan de impact erg groot zijn. Denk bijvoorbeeld aan een ziekenhuis dat niet meer van elektra en water wordt voorzien. De impact op het normaal functioneren is enorm zoals men zich kan voorstellen. Ook is een impact op de veiligheid een reeël scenario wanneer bijvoorbeeld een (hogedruk) gasleiding beschadigd raakt. Deze scenario's maken al snel duidelijk hoe noodzakelijk dit netwerk is.

Door in het voortraject voldoende tijd te nemen om werkzaamheden in kaart te brengen, wordt de kans op schade tijdens de uitvoering verkleind. Ter verduidelijking is in de richtlijn het proces verdeeld in 5 fasen. In elke fase wordt omschreven wie wat doet en wat de output is ten behoeve van de volgende fase. Daarbij wordt rekening gehouden met de eisen vanuit de Wet Informatie-uitwisseling Ondergrondse Netten (WION). In deze wet is opgenomen:
- De opdrachtgever zorgt dat het grondroeren waartoe hij opdracht geeft op zorgvuldige wijze kan worden verricht;
- De grondroerder voert deze werkzaamheden op zorgvuldige wijze uit;
- De netbeheerder verstrekt informatie over de ligging en relevante eigenschappen van de kabels en leidingen.

De richtlijn heeft in het bouwproces de volgende 5 fasen benoemd:

Initiatieffase

Wanneer besloten is een project uit te voeren, wordt gestart met de initiatieffase. Gedurende deze fase stelt de initiatiefnemer/opdrachtgever de randvoorwaarden op en inventariseert de eisen en wensen van het project.

Het resultaat van deze fase is dat het grondroeren expliciet wordt opgenomen in het uitvoeringsbesluit en dat er tijd en geld voor beschikbaar wordt gesteld. Het grondroeren wordt daarmee een onderdeel van de standaardprocessen.

Onderzoeksfase

Op basis van de eerste fase worden tijdens de onderzoeksfase de benodigde onderzoeken uitgevoerd. Naast bodemonderzoek is het van belang te onderzoeken wat in de uitvoering haalbaar is, daar waar het gaat om kabels en leidingen, en welke variaties mogelijk zijn. Tevens wordt een oriëntatieverzoek gedaan om gebiedsinformatie te verkrijgen. De gebiedsinformatie geeft inzicht in de theoretische ligging

en de kenmerken van het ondergrondse netwerk.

Uitgangspunt is dat de verkregen gebiedsinformatie juist is. De gebiedsinformatie is de basis van een risico-inventarisatie waarin alle grondroeringen in beeld gebracht worden. Hiermee zijn conflicten op voorhand zichtbaar. Op het moment dat sprake is van een conflict, wordt een beheersmaatregel opgesteld die tijdens de uitvoering het conflict opheft.

Voorbeelden van beheersmaatregelen zijn onder meer het (tijdelijk) verleggen van een kabel of leiding of deze beschermen door deze van een bekisting te voorzien.

De uitkomst van deze fase is een risico-inventarisatie en een plan van aanpak met beheersmaatregelen voor conflictsituaties. In overleg met de netbeheerder worden de beheersmaatregelen opgesteld en gemaakte afspraken vastgelegd.

Ontwerpfase

In de ontwerpfase wordt op basis van het programma van eisen uit de voorgaande fasen het ontwerp bepaald. Indien het ontwerp leidt tot een wijziging van de risico-inventarisatie wordt met de netbeheerders opnieuw overeenstemming gezocht over de te nemen maatregel.

In deze fase wordt ook de theoretische ligging, zoals vermeld op de gebiedsinformatie, getoetst aan de werkelijkheid. De kabels en leidingen worden buiten gelokaliseerd. De ontwerper bepaalt welke kabels en leidingen daadwerkelijk gelokaliseerd worden. Het gaat met name om het krijgen van een beter beeld van conflictsituaties die voor het ontwerp van belang zijn.

Nadat deze fase is uitgewerkt, is een definitief maatregelenplan beschikbaar waarin naast de beheersmaatregelen ook de afspraken met de netbeheerders zijn vastgelegd. Bij het maatregelenplan wordt ook een kabel- en leidingentekening meegeleverd waarin de gelokaliseerde kabels en leidingen zijn opgenomen.

Werkvoorbereidingsfase

In de werkvoorbereidingsfase verschuiven de werkzaamheden van de opdrachtgever en netbeheerder naar de aannemer die de werkzaamheden uitvoert. De werkvoorbereiding van de aannemer gaat aan de slag met het maatregelenplan en de tekeningen. Voor elk conflict is een individuele maatregel benoemd. Voor elke maatregel wordt een werkinstructie geschreven die specifiek gericht is op het risico. In die werkinstructies wordt benoemd wie wanneer welke handeling verricht.

Tijdens deze fase doet de werkvoorbereiding ook de wettelijk verplichte graafmelding. Minimaal 3 dagen en maximaal 20 dagen voor aanvang van de werkzaamheden wordt de gebiedsinformatie opgevraagd, zodat men over de meest actuele informatie beschikt. Op een project met een langere doorlooptijd kan het voorkomen dat meerdere graafmeldingen worden gedaan.

De grondroerder mag ervan uitgaan dat de gebiedsinformatie juist is. Dit ontslaat hem echter niet van de verplichting de verkregen informatie te beoordelen. Indien een verschil geconstateerd wordt tussen de huidige gebiedsinformatie en eerder opgevraagde gebiedsinformatie, neemt de grondroerder contact op met de netbeheerder en de opdrachtgever om dit te bespreken.

Uitvoeringsfase

Voor aanvang van de werkzaamheden wordt een startwerkbespreking georganiseerd, waarin de gebiedsinformatie en werkinstructies worden besproken. Bij deze startwerkbespreking zijn alle medewerkers van zowel de aannemer

als eventuele onderaannemers op het project aanwezig. Wanneer nieuwe medewerkers op het project aan de slag gaan, wordt voor hen een startwerkbespreking georganiseerd.

Bij de uitvoerder in de keet hangt een keetkaart met daarop een reminder aan alle benodigde informatie die aanwezig moet zijn voordat gegraven mag worden. Aan deze keetkaart is een 'Veilig graven' app gekoppeld. Deze app geeft informatie over juist gebruik van de KLIC melding en biedt toegang tot instructiefilmpjes over zorgvuldig graven.

Om tijdens de uitvoering van het project aandacht te houden voor het zorgvuldig roeren, kan een toolbox over dit onderwerp georganiseerd worden. Tijdens de dagelijkse Last Minute Risico Analyse (LMRA) is het zorgvuldig grondroeren ook onderdeel van de analyse.

Mocht onverhoopt toch een kabel of leiding beschadigd worden, dan wordt contact opgenomen met de netbeheerder en de persoon die intern bij de grondroerder de schades behartigt.

Na afloop van het project evalueert de opdrachtgever samen met de grondroerder en de netbeheerder het gehele proces om tot eventuele toekomstige verbeterpunten te komen. Het project wordt opgeleverd en overgedragen aan de opdrachtgever voor ingebruikname.

Wat verandert er nu wezenlijk door deze richtlijn?

Door op voorhand rekening te houden met knelpunten, is de verwachting dat tijdens de uitvoering een onjuiste werkwijze wordt voorkomen. Door samen verantwoordelijkheid te dragen is in ieder geval meer aandacht voor dit onderwerp. Niemand veroorzaakt opzettelijk een kabel- of leidingschade. Grondroerders zijn vakmensen die weten waar ze mee bezig zijn. Desondanks kan men altijd een misser maken, zeker wanneer een verdwaalde kabel of leiding opduikt.

Door het melden van weeskabels en -leidingen, via de opdrachtgever aan het Kadaster, worden de KLIC meldingen meer betrouwbaar en is het risico op onverwachte voltreffers kleiner. Dat effect wordt pas op de lange termijn zichtbaar.

Wat in de toekomst ook een positieve bijdrage kan leveren, zijn de ontwikkelingen op het gebied van detectie, bijvoorbeeld middels een grondradar. Wanneer middels deze methode met hoge nauwkeurigheid de ligging en diepte vastgesteld wordt, is het graven van proefsleuven en aanpikken van leidingen nagenoeg niet meer nodig.

Kortom:
Door deze richtlijn ontstaat nieuw bewustzijn en gezamenlijke verantwoordelijkheid. In combinatie met de ontwikkelingen in de markt, daar waar het gaat om detectie, is voldoende potentieel voor het reduceren van het aantal schades. Echter, op korte termijn is het effect (nog) niet zichtbaar.

Sonja Hommels werkt als KAM coördinator voor ReintenInfra, een regionale allround infra & sloop aannemer in het oosten van het land. Hiervoor was zij werkzaam als procescontroller van het Sorteercentrum Brieven in Zwolle en adviseur op het gebied van Arbeidsomstandigheden bij PostNL in de regio Noordoost Nederland.

De toekomstige rol en functie van de managers van zorgsystemen: veiligheid, gezondheid, milieu, beveiliging, continuïteit en kwaliteitszorg.

Er zijn talloze bedrijven die de gevolgen van een megaschade (bijv. brand, milieu, fraude, inbraak, diefstal etc.) niet meer te boven komen, failliet gaan of binnen enkele jaren alsnog failliet gaan. In zijn lange carrière in de internationale veiligheids- en verzekeringsbranche heeft Marcel Hanssen alles meegemaakt. Bedrijven die voldoen aan alle wet- en regelgeving, maar geconfronteerd worden met aanvullende eisen van de verzekeringsmaatschappij of een hoge verzekeringspremie. Ondernemers die hun bedrijfspand tot de grond toe zien afbranden, immers: Life Safety staat (op zich terecht) op één. De brandweer is er niet om je bedrijf te redden.
Het voldoen aan vergunningsvoorwaarden en eisen voorkomt zulke scenario's niet. Niet opgevolgde adviezen en aanbevelingen gedaan door de interne specialist maken de zaak alleen maar erger, maar ontslaan ook de specialist-adviseur niet van verantwoordelijkheid en daarmee zelfs rechtsvervolging.
Langzaam maar zeker schuiven we richting een "claimcultuur" waarbij niemand gespaard blijft.
Dat alles heeft ook gevolgen voor de rol en positie van de staffunctionaris in zijn (tot nu toe) adviserende rol.

Nieuwe positionering van de traditionele KAM-manager

In dit artikel wordt de positie van de KAM-manager in de breedste betekenis bedoeld. Alle denkbare "conformance-processen" of bedrijfszorgsystemen worden hier voor het gemak aangeduid met de afkorting VGMCBK: veiligheid, gezondheid, milieu, continuïteit, beveiliging en kwaliteitszorg. Dit zijn functies binnen een organisatie die indirect invloed hebben op de primaire bedrijfsresultaten (omzet, marge etc.) en afhankelijk van de grootte van de organisatie kan bestaan uit één enkele manager tot en met hele stafafdelingen.

In de komende jaren zal de functie van managers van bedrijfszorgsystemen zijn veranderd van een staf- naar lijnfunctie, waarbij overeenkomstige taken, verantwoordelijkheden en (nog belangrijker) bevoegdheden zijn samengebracht om die functionaris de "toolbox" te geven om deze verantwoordelijkheid naar behoren uit te kunnen voeren. Met een lijnfunctie ontstaat voor die functionaris dan meteen ook een medeverantwoordelijkheid voor het algemene beleid én de realisatie van andere bedrijfsdoelen zoals maatschappelijk verantwoord ondernemen (MVO) maar ook bedrijfscontinuïteit, omzet en marge. Die medeverantwoordelijkheid komt sluipenderwijs dichterbij en vertaalt zich ook meteen in een aansprakelijkheid. Dat blijkt uit het feit dat alvast de veiligheidskundigen zich al voor de rechter moeten verantwoorden voor hun rol in de aanloop naar en tijdens ernstige incidenten waarbij sprake was van overlijden of letsel en milieuschade. Per geval zal de uitkomst verschillen, maar voorlopig is er wel sprake van aanhouding en voorgeleid worden aan de rechter-commissaris.

Door de tendens naar meer juridische aansprakelijkheid en de daar uit volgende betrokkenheid en verantwoordelijkheid ontstaat ook de kans om met een efficiënt zorgprogramma een aantoonbare bijdrage te leveren aan verbeterde bedrijfsresultaten. De manager kan door zijn beleid de totale risicokosten reduceren én een vervolging door het OM afwenden. Het in financiële termen aantonen van de bijdrage vereist nog een slag in het denken en handelen van de experts die zich binnen bedrijven bezig houden met voornoemde thema's (VGMCBK). Ook het aantoonbaar reduceren van risico's (bijvoorbeeld in de vorm van claims) vermindert aantoonbaar de totale risicokosten.

Het is zaak om bij de (her-, bij-) scholing van deze specialisten het nieuwe juridische én financiële kader te benoemen waarin zowel de verwijtbaarheid, aansprakelijkheid en de beheersing van de totale risicokosten meer onder de aandacht komen.

In dit artikel wordt op twee thema's nader ingegaan.

- Juridisch: wordt de deskundige (VGMCBK) sneller en in grotere mate (mede) verantwoordelijk gehouden in geval van letsels, slachtoffers en grote schades?
- Financieel: kan de deskundige beter aantoonbaar maken welke bijdragen geleverd worden aan de bedrijfsresultaten?

Op beide vragen is het antwoord bevestigend. Voorlopig staat dat echter nog in schril contrast met de gemiddelde realiteit. Vast staat wel dat beide ontwikkelingen nieuwe dimensies

toevoegen aan de tot nu toe geaccepteerde functie-inhoud van betreffende experts op het gebied van VGMCBK.

Gemeenschappelijke consequenties

De verschillende zorgsystemen (VGMCBK) vertonen een aantal overeenkomsten. Allereerst komen ze nadrukkelijk in beeld (zeker in de media) tijdens ongewenste incidenten met aanvankelijk alleen directe schade als gevolg. Doorgaans is er sprake van grote maatschappelijke verontwaardiging. Er is daarnaast niet alleen directe schade binnen het bedrijf of de instelling, maar ook de schade veroorzaakt aan derden in welke vorm dan ook. Dat zal meer en meer leiden tot rechtsvervolging en slepende claims (See you in court!)

Op het terrein van veiligheid, gezondheid en milieu zijn er voorbeelden te over, al is de aanhouding en vervolging door het OM van verantwoordelijke experts (VGWM) zeker een recente nieuwe trend. Wanneer het gaat over continuïteit, beveiliging en kwaliteit zijn de voorbeelden van indirecte schades mogelijk minder bekend. Ter illustratie:

Bedrijfscontinuïteit: Een willekeurig incident leidt tot bedrijfsstilstand. De directe gevolgen voor het eigen bedrijf zijn snel in kaart te brengen. Echter, het overige deel van de gehele "supply chain" wordt door toenemende integratie ook geraakt. De bedrijfsvoering bij toeleveranciers en afnemers stokt ook vrijwel meteen en hebben schade.

Beveiliging: Een plofkraak verwoest niet alleen het eigen gebouw, maar ook de bovenliggende panden en of de winkelstraat. Een omvallende bouwkraan veroorzaakt een ravage. Winkels blijven dicht, alternatieve huisvesting moet worden gevonden en infrastructuur is onbruikbaar.

Kwaliteit: Vanuit de voedselindustrie komen producten op de markt die niet aan de specificaties voldoen. Er zijn directe kosten (product recall) maar ook de hele distributieketen wordt aangetast. Tussenpersonen en eindleveranciers zullen schade ondervinden, bijv. in de vorm van imagoschade en daardoor omzet verlies.

In alle gevallen worden de volgende vragen gesteld:

- Had dat voorkomen kunnen worden?
- Ja?
- Heeft de beheerder/eigenaar/expert wel alles gedaan om de nadelige effecten te voorkomen?
- Nee?

In dat geval zijn het OM samen met andere eisers in aantocht.

Alle disciplines(VGMCBK) hebben in potentie een zeer groot maatschappelijk bereik en daarmee een grote maatschappelijke impact. Incidenten worden simpelweg niet meer geaccepteerd; niet door het publiek en ook niet door de getroffen partijen. Gevolg: rechtszaken en claims. De maatschappelijke verontwaardiging en de belangen zijn dermate groot dat ongeacht wie een verantwoordelijkheid had voor het incident ter verantwoording zal worden geroepen.

Aansprakelijkheid

"Je stond erbij en keek ernaar zonder in te grijpen" wordt straks misschien wel één van de meest verwijtbare beschuldigingen aan het adres van de verdachte; waarbij de verdachte ook de adviserende staffunctionaris kan zijn zoals recentelijk is gebleken bij o.a. Chemie-Pack. Professionals worden aangesteld of ingehuurd omwille van het feit dat zij deskundig zijn en op die grond worden aangesproken. Aansprakelijkheid zal doorgaans in zicht komen wanneer een willekeurige partij zich benadeeld voelt en inschat dat compensatie geëist kan worden. Historisch gezien betekent dat een breuk. Onze maatschappij kende geen "claimcultuur". Dat is echter aan het veranderen en zal sneller toenemen dan menigeen verwacht.

Veelal worden claims via een aansprakelijkheidsverzekering afgehandeld. Na een incident is het vaak maar hopen dat deze én alle (gevolg)schade is gedekt. Vaak blijkt dat niet het geval. Echter, ook zonder aansprakelijkheidsdekking verdwijnt de claim niet. Uit de praktijk blijkt dat er in vrijwel alle gevallen sprake is van langdurig slepende zaken met veel persoonlijke ellende en waarbij het schadebedrag en de uitkeringstermijn een langdurige onzekerheid op de budgetten voor alle partijen veroorzaken (reserveringen). Zoals hiervoor aangegeven verschuift de aansprakelijkheid duidelijk in de richting van de deskundige, zelfs wanneer zijn of haar rol in eerste aanleg puur adviserend is. Het is te verwachten dat deze verschuiving van toepassing zal zijn op alle disciplines (VGMCBK).

Vergunningsvoorwaarden en opvolging

Het is een misverstand dat het al dan niet voldoen aan vergunningsvoorwaarden bescherming tegen vervolging geeft. Het zelfde geldt voor een garantie op uitkering bij schade. Vergunningseisen staan los van aansprakelijkheid. Het niet voldoen aan de vergunningseisen of voorwaarden kan leiden tot juridische of bestuurlijke maatregelen zonder dat dat daar een ongeval, schade of verlies in het algemeen aan vooraf gegaan is. Bij schade zal de belangrijkste vraag zijn of het incident te voorkomen was. Een expert zal beamen dat de vergunningsvoorwaarden maar een beperkt aantal basisoorzaken voor ongeval of schade adresseren.
In geval een bedrijf preventie-aanbevelingen naast zich neerlegt, zal het OM bij een incident dit aangrijpen als blijk van onverantwoord en onkundig bestuur, ongeacht de beste intenties van het betreffende bedrijf. Indien een dergelijke conclusie wordt getrokken, is de kans groot dat ook de verzekeraars dit aangrijpen om te wijzen op slecht huisvaderschap: nalatigheid dus.

Oplossingen en kansen

Het grote probleem van een claimcultuur is de tendens naar meer doofpot-gedrag. De lerende organisatie heeft juist behoefte aan meer openheid van bestuur en transparantie in het algemeen. De stelregel "mensen maken fouten en van fouten kun je leren" wordt "mensen maken fouten en iedereen moet er van leren". "iedereen" is binnen en buiten de organisatie. Vaak zijn incidenten het gevolg van een bizarre samenloop van omstandigheden. Experts in risicopreventie leren vooral van voorvallen elders. De toenemende aandacht voor risico's – dus ook voor de expert/specialist zelf – biedt ook kansen. In ieder geval zal de druk om deze kansen te benutten uit het oogpunt van bedrijfsresultaat toenemen. Dat vraagt om een aanpassing van het profiel van de expert.

De eerste stap begint bij het besluitvormingsproces binnen de organisatie. Zolang reguliere businessbeslissingen op korte termijn gerichte bedrijfseconomische gronden worden genomen, zullen optimalisaties met betrekking tot VGMCBK te weinig worden meegenomen. Zo schitteren de VGMCBK-deskundigen ook erg vaak in afwezigheid bij de behandeling van vraagstukken rondom risicofinanciering. Risicofinanciering is een brede term. Als eerste wordt gedacht aan verzekeren. Maar met het uitgangspunt dat 100% dekking niet bestaat (er is altijd ongedekte neven- en gevolgschade) komen meteen andere kosten om de hoek kijken. Bij optimalisatie in besluitvorming wordt het begrip Total Cost of Risk & Insurance (TRCO&I) gehanteerd. Uit eigen ervaring van de auteur blijft het verbazingwekkend hoe weinig dergelijke functionarissen worden betrokken bij …… Dat is bijzonder, zeker wanneer je bedenkt dat het verbeteren van VGMCBK toch echt iets is waar grootzakelijke (vaak internationale) verzekeraars geïnteresseerd in zijn én waar jaarlijks miljoenen Euro's in omgaan. Op de vraag aan de VGMCBK – experts óf en hoe vaak zij met de interne beheerder van de verzekeringsportefeuille overleggen komt doorgaans een teleurstellend antwoord.

TCOR&I

In onderstaande tabel zijn ter illustratie enkele elementen weergegeven die bijdragen aan de (reductie van) de TCOR&I.

Total Cost Of Risk & Insurance in balans en onder controle?	
1. Verzekeringspremies en kosten	2. Preventiekosten • Veiligheidssystemen • Beveiligingssystemen (Security) • Business Continuity planning • Etc.
3. Directe eigen kosten • Eigen RM activiteiten (VGWM afdeling). • Consultants / Loss Prevention Programma's. • Studies / analyses. • Afhandeling schades, claims etc. • Etc.	4. Verliezen (onverzekerd / onverzekerbaar) • Eigen risico. • Marktverlies / imagoschade / juridische acties. • Product Recall. • Onderzoekskosten. • Etc.

Verzekeraars zullen doorgaans bij twijfel over de wijze waarop het risicoprofiel is opgesteld (bijvoorbeeld interne auditrapporten die niet beschikbaar worden gesteld) – toch al betrekkelijk eenvoudig een premieverhoging doorvoeren. Onduidelijkheid over het beheer van de risico's (goed huisvaderschap) betekent onzekerheid in de verzekeringswereld en dat is nu eenmaal duur. Men wil wél verzekerd zijn maar laat de verzekeraar (als risicodrager) in onzekerheid. Dat is een strijdigheid, maar vooral een beleid met een fors prijskaartje. Voor de juristen van het Openbaar Ministerie is dit koren op de molen. De behandelaars van de schadeclaims gaan zich vervolgens ook beroepen op verwijtbaarheid (slecht huisvaderschap).

Tegenover deze mogelijke kostenverhoging, dreiging van claims en/of rechtsvervolging bestaat ook de mogelijkheid om een aanzienlijke kostenreductie te realiseren door met een doordacht integraal veiligheidsplan te komen. Wanneer de Verzekeringsmanager van deze wereld zich vaker samen met de VGMCBK verantwoordelijke eens goed buigen over het relevante beleid binnen de organisatie, kan er betrekkelijk eenvoudig over reductie van TRCOR&I worden gesproken waarbij de verzekeringskosten en eigen ongedekte kosten en reservering (kwadrant 1 en 4) fors naar beneden kunnen worden bijgesteld; zeker wanneer inderdaad blijkt dat er minder schades zijn geweest. Afhankelijk van de bedrijfsgrootte, gaat het hier toch al snel over tienduizenden Euro's op jaarbasis.

Er valt dus een aantoonbaar voordeel te behalen. Grootzakelijke verzekeraars en makelaars hebben afdelingen met gespecialiseerde Risk Consultants/Engineers: professionals die de kans op incidenten afzetten tegenover de te verwachten maximale schades en uit te keren verzekeringsgelden. Wanneer een expert vanuit het bedrijf zelf (heeft de meeste kennis) een bijdrage kan leveren aan het verlagen van de kans óf de impact, dan is een verzekeraar hierbij gebaat. Dat moet zich dan ook kunnen vertalen in verbeterde polisvoorwaarden, en/of premies en/of andere componenten van de TCOR&I. Kort en bondig: een aantoonbaar effectieve investering in een van de kwadranten (2 en 3) moet zich vertalen in een reductie van de kosten in 1 en 4. Deze optimalisatie krijgt nauwelijks aandacht. Dat wil zeggen binnen een aantal bedrijven wordt dit zeer professioneel opgepakt, maar het merendeel niet.

Samenvattend.

Met dit artikel wordt aandacht gevestigd op een nieuw speelveld dat voor iedere VGMCBK – professional aan het ontstaan is. Hij zal zijn rol bij beleidsbeslissingen, geruggesteund door een toename van claims, moeten leren opeisen. Toegang wordt mogelijk bereikt met het begrip TCOR&I.

Waarschijnlijk kunnen IVK'ers (integraal veiligheidskundigen) als eersten een brug slaan tussen VGMCBK professionals en de op – kosten versus baten-georiënteerde bestuurders. Allen zullen zich dit "spel" eigen moeten maken. De juridische weerbaarheid en de besparingen zullen toenemen.

Voorbeelden van positieve beïnvloeding van het risicoprofiel en de (verzekerde) verliesscenario's.

Risk Management programma element	Impact	Gerelateerde verzekering
VGWM & Q	Reductie van ongevallen, verzuim, milieuschade, productaansprakelijkheid en imagoschade	Opstal, bedrijfsstilstand en Aansprakelijkheid
Loss Prevention (bijv. Fire Safety)	Verlaging van maximale schadescenario's (MPL/EML)	Opstal, Bedrijfsstilstand en Aansprakelijkheid
Bedrijfscontinuïteit (Business Contingency) en voorbereiding noodsituaties	Reductie van kans & effect van bedrijfstilstand (MPL/EML). Reductie van maximale uitkeringsperiode bij bedrijfsonderbreking.	Opstal, Bedrijfsstilstand en Aansprakelijkheid
MVO	Verhoogde weerbaarheid bij claims en/of juridische acties.	Aansprakelijkheid, Errors & Omissions

Marcel Hanssen is Senior Associate bij KMS energy consulting. Hij adviseert op het gebied van Safety, Risk and Risk Finance. KMS energy consulting is een onderdeel van de KMS energy group, een organisatie die een bijdrage levert aan de energie gerelateerde uitdagingen waarmee onze en toekomstige generaties worden geconfronteerd. Daarbij horen veiligheid en continuïteit in de werkomgeving. Daarvoor heeft hij o.a. 18 jaar gewerkt bij Aon (Makelaars in Assurantiën en Risico Adviseurs) Rotterdam. Als hoofd van de afdeling Risk Control was hij verantwoordelijk voor o.a. de coördinatie en uitvoering van Property Damage en Business Interruption programma 's met name voor grote internationale bedrijven.

Risico management in de medische sector

In de nieuwe ISO9001:2015 wordt veel nadruk gelegd op risico management. In de ISO norm voor medische hulpmiddelen (ISO13485) is al jaren aandacht voor risico beheersing, de aanpak is echter op een aantal punten wel heel verschillend, hieronder gaan we in op die verschillen.

Wet- en regelgeving voor Medische hulpmiddelen.

In Nederland moeten medische hulpmiddelen net als in de rest van Europa voldoen aan de Europese regelgeving. Deze regelgeving is vastgelegd in de volgende richtlijnen: 93/42/EEG voor medische hulpmiddelen, 90/385/EEG voor actieve implantaten e 98/79/EG voor in-vitro diagnostische hulpmiddelen. De richtlijnen zijn door de jaren aangevuld en aangepast. De richtlijnen geven aan welke stappen men moet zetten om medische hulpmiddelen op de Europese markt te mogen brengen. Eén van de eisen is dat een CE markering aangebracht wordt (in bepaalde gevallen inclusief een registratienummer) wat aangeeft dat het product voldoet aan de regelgeving. Het aanbrengen van een CE markering moet in de meeste gevallen geverifieerd worden door daartoe aangestelde organisaties, de zogenaamde Notified Bodies. Voor nederland zijn dat *DEKRA Certification (v/h KEMA)* en *DARE!! Medical Certifications*. Deze notified bodies staan op hun beurt weer onder toezicht van de *Inspectie voor de Gezondheidszorg (IGZ)*.

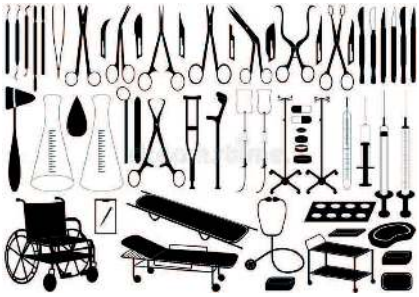
Bedrijven die medische hulpmiddelen op de markt brengen moeten aantoonbaar voldoen aan de Europese wetten. Een manier om dit aan te tonen is het behalen van een ISO13485 certificaat. De nieuwste versie van deze norm is van 2016 en is een aanpassing op de versie van 2003 die op haar beurt is afgeleid van ISO9001:2000. Om de ISO13485 norm een volledige weerspiegeling

van de Europese regels te laten zijn is een speciale Europese versie uitgebracht: EN ISO13485, hierin zijn een aantal bijlages (ZA, ZB en ZC) opgenomen met aanvullingen uit de Europese richtlijnen. Omdat deze norm nog is afgeleid van de 2000 versie van de ISO9001 valt deze nog niet onder de nieuwe High Level Structure. In de nieuwe versie van ISO13485 van 2016 zijn al wel een aantal eisen op het gebied van risico opgenomen.

Norm voor risico analyse van medische hulpmiddelen.

Een al bestaande eis in de medische norm is dat de uitkomsten van de product risico analyse als input meegenomen moeten worden voor het ontwerp en de ontwikkeling van medische producten en ook als later nieuwe risico's worden geïdentificeerd moet overwogen worden of opnieuw begonnen moet worden met het ontwerp. Door het volgen van de in ISO13485 aangeroepen *EN ISO14971: "Medische hulpmiddelen – Toepassing van risicomanagement voor medische hulpmiddelen"* kan invulling gegeven worden aan de formele Europese regels voor risico management.

Deze gedetailleerde EN ISO14971 norm kan dus toegepast worden voor risicomanagement voor medische hulpmiddelen. Hieronder wordt uitgelegd dat de norm één van de betere normen voor risico management is en dat de



industrie hiermee een uiterst geschikte en toepasbare norm heeft.

In de norm staan de volgende definities:

Risico (Risk)	• Combinatie van de waarschijnlijkheid van optreden van schade en de ernst van die schade
Gevaar (Hazard)	• Potentiële bron van schade
Gevaarlijke situatie (Hazardous situation)	• Omstandigheid waarin mensen, eigendommen of het milieu worden blootgesteld aan een of meer gevaren
Ernst (Severity)	• Maatstaf voor de mogelijke gevolgen van een gevaar

De informatieve Annex D (Risico concepten toegepast op medische hulpmiddelen) van de norm geeft een tweetal analyse methodes aan als

voorbeeld: de kwalitatieve analyse en de semi-kwantitatieve analyse.

Semi-kwantitatieve analyse.

Omdat de kwalitatieve analyse geen concrete niveaus gebruikt is deze minder makkelijk te hanteren, daarom gaan we iets dieper in op de tweede genoemde methode: de semi-kwantitatieve analyse. Hoewel het voor de hand ligt is het bepalen van risico's in termen van gevaren ongebruikelijk in andere normen en sectoren. Zo komt het weglaten van de factor ernst in de definitie van risico wel veel vaker voor. Ook wordt risico vaak gedefinieerd als het rekenkundig product van waarschijnlijkheid en ernst wat kan leiden tot minder logische risicoprioriteiten. De methode in de EN ISO14971 norm geeft een meer beschrijvende, niet rekenkundige classificatie van ernst, dit kan zijn: geen medische

interventie vereist, medische interventie vereist, ziekenhuisopname, levensbedreigend enz.

De beoordelingen worden gemaakt op basis van een relatieve waardering voor ernst (severity), hierbij wordt niet gepoogd dit in een cijfermatige schaal uit te drukken. In de praktijk kan Ernst moeilijk gekwantificeerd omdat de waarde van overlijden of blijvende invaliditeit of een verwonding die medisch ingrijpen nodig maakt lastig in getallen uitgedrukt kan worden.

In onderstaand voorbeeld voorbeeld wordt een 5 bij 5 matrix gebruikt. De niveaus voor ernst (severity) en waarschijnlijkheid (probability) zijn respectievelijk in tabel D3 en D4 aangegeven.

Tabel D.3 – Example of five semi-quantitative severity levels

Common terms	Possible description
Catastrophic	Results in patient death
Critical	Results in permanent impairment or life-threatening injury
Serious	Results in injury or impairment requiring professional medical intervention
Minor	Results in temporary injury or impairment not requiring professional medical intervention
Negligible	Inconvenience or temporary discomfort

Tabel D.4 — Example of semi-quantitative probability levels

Common terms	Examples of probability range
Frequent	$\geq 10^{-3}$
Probable	$< 10^{-3}$ and $\geq 10^{-4}$
Occasional	$< 10^{-4}$ and $\geq 10^{-5}$
Remote	$< 10^{-5}$ and $\geq 10^{-6}$
Improbable	$< 10^{-6}$

(Tabellen afkomstig uit ISO14971)

De definities kunnen best verschillen voor verschillende product families. Fabrikanten kunnen de ene set van definities kiezen voor MRI-scanners en een andere voor steriele wegwerp wond-verzorgings producten. Verschillende mates van waarschijnlijkheid kunnen geschikt zijn, afhankelijk van de toepassing. De mate van waarschijnlijkheid kan bijvoorbeeld "waarschijnlijkheid per gebruik", "waarschijnlijkheid per toestel", "waarschijnlijkheid per uur gebruik" etcetera bevatten.

Verder zijn er verschillende significante factoren en statistieken die belangrijk zijn voor het analyseren van de waarschijnlijkheid van optreden. Deze statistieken kunnen onder ander zijn:

- Hoe vaak wordt een specifiek medisch hulpmiddel gebruikt
- Wat is de levensduur van een medisch hulpmiddel
- Wat is de gebruikers en patiënten populatie
- Hoe groot is de populatie van gebruikers en patiënten
- Hoe lang en onder welke omstandigheden worden gebruikers en patiënten blootgesteld aan gevaren

Een voorbeeld van een ingevulde 5 bij 5 matrix staat hieronder in Figuur D.3. De geïdentificeerde risico's zijn aangegeven als *R1* t/m *R6*.

De geïdentificeerde risico's *R5* en *R6*, zijn volgens de tabel niet acceptabel en moeten met mitigerende maatregelen zo ver mogelijk gereduceerd worden naar niveau AFAP of liever nog op een acceptabel niveau gebracht worden.

Andere matrices naast een 5 x 5 matrix kunnen ook worden gebruikt, echter voor een matrix groter dan 5 x 5 zijn veel meer gegevens nodig om de verschillen tussen de niveaus (levels) aan te geven. Ook moeten de redeneringen achter de meerdere niveaus en hun resulterende scores uitgelegd

Semi-quantitative probability levels	Semiquantitative severity levels: Negligible	Minor	Serious	Critical	Catastrophic
Frequent					
Probable	R_1	R_2			
Occasional		R_4		R_5	R_6
Remote					
Improbable			R_3		

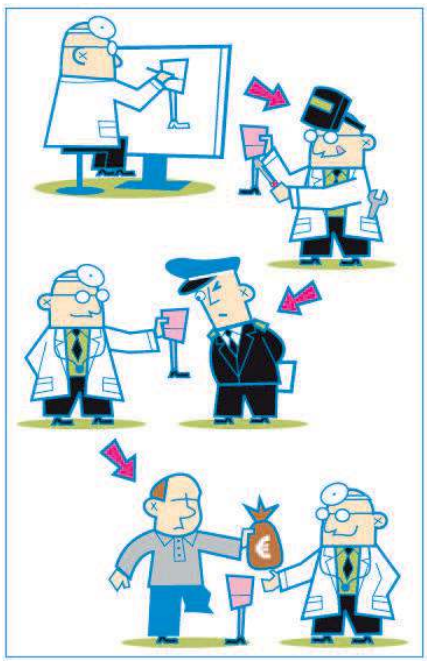
Not acceptable
Reduced as far as possible (AFAP)
Acceptable

Figuur D.3 — Example of a semi-quantitative risk matrix
(Tabel afkomstig uit ISO14971)

en vastgelegd worden. Met een matrix van 3 x 3 kan het zijn dat het onderscheid tussen de niveaus juist weer onvoldoende detail geeft. Overigens is het geen noodzaak dat de matrix symmetrisch is, een 4 x 5 matrix zou ook kunnen.

Aanpak van de risico analyse

De norm dringt aan op een top-down aanpak van de analyse, met andere woorden: begin met een functionele gevarenanalyse. Dit betekent dat alle significante schades of ongewenste situaties die voort kunnen vloeien uit het beoogde gebruik van het product of de gebruikte (productie-) processen geïdentificeerd moeten worden. Voorwaarde is wel dat het beoogde gebruik van het product helemaal duidelijk is. Een risicoanalyse gebaseerd op een gevarenanalyse begint dus met de denkbeeldige schade en gaat terug naar de onderliggende oorzaken, dit kunnen fouten, storingen en combinaties daarvan zijn. De schades of ongewenste situaties kunnen zowel afhankelijk als onafhankelijk zijn van het beoogde gebruik en de gebruikte (productie-) processen. Het accepteren van een restrisico met ernstige schade kan alleen nadat aangetoond is dat de waarschijnlijkheid van optreden van de gevaren of gevaarlijke situaties voldoende laag is. Een groot verschil is ook dat uiteindelijk de voordelen voor de patiënt moeten opwegen tegen overgebleven individuele risico's en ook tegen de combinatie van alle restrisico's. Vooral dit laatste, het feit dat de voordelen voor de patiënt ook moeten opwegen tegen de combinatie van alle restrisico's is specifiek voor de Europese wetgeving en dan ook een specifieke aanvulling van de EN versie van de ISO14971. De analogie "dood door duizend speldenprikken" illustreert dat het voordeel voor de patiënt ook moet opwegen tegen de combinatie van alle restrisico's.



Gebruik van FMEA versus de EN ISO14971 norm

In de praktijk wordt door fabrikanten van medische hulpmiddelen in plaats van een gevarenanalyse vaak een Failure Mode & Effect Analyse (FMEA) uitgevoerd. Vanwege de engineering achtergrond van veel fabrikanten van medische hulpmiddelen kiest men eerder voor de ingeburgerde FMEA dan voor een werkelijke gevarenanalyse. Gevolg is echter wel dat vaak niet volledig aan alle eisen van de EN ISO14971 en daarmee niet aan de eisen van de Europese richtlijn lijkt te worden voldaan. De basis van het onderscheid lijkt de oorsprong te vinden in de verwarrende ogenschijnlijke gelijkenis van de gebruikte terminologieën:

- De EN ISO14971 gevarenanalyse gebruikt termen als risico's, gevaren, gevaarlijke situaties, schade, ernst, waarschijnlijkheid van optreden, aanvaardbaarheid van risico's en risicobeheersing.
- FMEA gebruikt termen als storingsvormen / faalmechanismen, effect van falen, ernst, oorzaken van falen, het optreden, procesbeheersing, detecteerbaarheid, risico prioriteit nummer (RPN) en aanbevolen acties.

Vanwege deze verschillen in terminologie tussen de EN ISO14971 norm

en de FMEA methode kan verwarring ontstaan:

- Gevaren en gevaarlijke situaties klinkt vergelijkbaar met faalmechanismen.
- Schade lijkt vergelijkbaar met effect van falen.
- Risico lijkt vergelijkbaar met het risico prioriteit nummer.

Ondanks de gelijkenis in terminologie tussen gevarenanalyse en Failure Mode & Effect Analyse (FMEA) is het gebruik van de instrumenten totaal anders. Gevarenanalyses dwingen om de kritische factoren die leiden tot schade voor de patiënt of de gebruiker van het hulpmiddel te bepalen in plaats van, zoals bij FMEA, het bepalen van de individuele faalmodes.

Risico Management is in EN ISO14971 gedefinieerd als:

- Risico Management – systematische toepassing van beleid, procedures en praktijken bij het analyseren, evalueren, beheersen en bewaken van risico's.

De ASQ definitie van FMEA is:

- Failure Mode & Effect Analyse (FMEA) is een stap-voor-stap benadering voor het identificeren

van alle mogelijke storingen in een ontwerp, een productie- of assemblage- proces of een product of dienst.

De FMEA methode is dus niet bedacht voor gevarenanalyse en is er ook niet echt geschikt voor. FMEA is dus niet echt een gevarenanalyse methode maar meer een betrouwbaarheidsanalyse. De FMEA is hierdoor dus wel een zeer goed instrument voor evaluatie van de robuustheid van materialen, componenten en onderdelen waar medische hulpmiddelen uit bestaan en van de processen om deze te vervaardigen.

Belangrijke conclusie: gevarenanalyse richt zich niet alleen op fouten (inclusief misbruik) en afwijkingen maar juist ook op gevaren die het gevolg zijn van de beoogde staat van het product of het proces. Een medisch hulpmiddel kan

een bron van schade zijn zelfs als er geen sprake is van afwijkingen van ontwerpspecificaties of fouten in het functioneren.

In de EN ISO14971 norm moet ook gewaardeerd worden dat deze uitgaat van een technisch perspectief in plaats van een juridisch oogpunt. Eigenlijk moet productveiligheid niet beginnen met risico beheersing en overdracht mechanismen maar met een inherent veilig ontwerp. De norm geeft een volgorde van risico beperkende maatregelen aan die leidend moeten zijn tijdens het ontwerp- en ontwikkel proces, van concept tot het op de markt brengen van het medisch hulpmiddel:

- Inherent veilig ontwerp
- Beschermende maatregelen
- Informatie, instructie en/of waarschuwing

De EN ISO14971 is op zich pragmatisch en resulteert in een risico / baten analyse waarbij enige mate van risico voor de patiënt wordt geaccepteerd om bepaalde baten te bereiken. In principe moeten de baten voor de patiënt opwegen tegen (de combinatie) alle (rest) risico's. Producten en activiteiten zonder risico bestaan niet. Vrijwel iedereen in de gezondheidszorg is het eens met dat risico / baten analyses zinvol zijn maar het concept lijkt soms moeilijk te bevatten voor de leek en ook de media. De laatsten prediken 100% veiligheid en richten hun radar op de voorvallen waarbij zich ongewenste situaties hebben voorgedaan. Gevolg hiervan is dat door een angstcultuur bij overheden dit doorschiet in overdreven wet en regelgeving. Een bekend voorbeeld is het debacle met de PIP siliconen implantaten. Hier zijn grote problemen ontstaan doordat de fabrikant frauduleus heeft gehandeld door ongeschikt siliconen materiaal te gebruiken. Hier had de fabrikant een financieel voordeel bij. In reactie op onder andere deze zaak zijn de regels voor leveranciers bewaking aangescherpt en moeten fabrikanten regelen dat hun kritische leveranciers op korte termijn en zonder uitstel bezocht kunnen worden door de toezichthouder.

Wat ook anders is in EN ISO14971 ten opzichte van andere risico management normen is het evalueren van potentiële nieuwe risico's geïntroduceerd door genomen maatregelen naar aanleiding van eerder geïdentificeerde risico's.

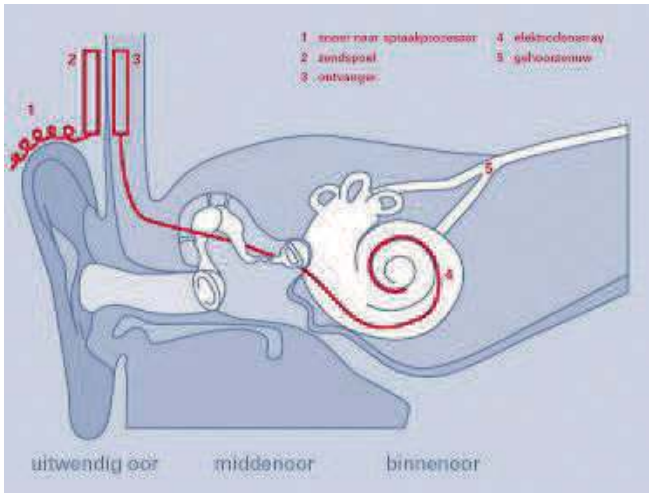
Ook moeten de ingeschatte waarschijnlijkheid en ernst steeds worden getoetst en indien nodig worden aangepast aan de werkelijkheid. Dit moet voortdurend actief worden vervolgd en bewaakt, ook na levering (zgn. Post Market Surveillance). Deze Post Market Surveillance is ook een eis in de eerder genoemde EN ISO13485.

EN ISO14971 staat niet toe dat (de mate van) detecteerbaarheid (detectability) van faalmodes leidt tot vermindering van geïdentificeerde risico's.

Detecteerbaarheid mag alleen worden ingezet voor de mate waarin preventieve maatregelen mogelijk gemaakt kunnen worden.

Conclusies.

Ten opzichte van ISO9001 was in ISO13485 veel eerder aandacht voor risico management. Dit concentreerde zich wel voornamelijk op risico's voor de patiënt en/of het personeel dat met de medische hulpmiddelen moet werken. Het nieuwe High Level Structure format richt zich op risico's in de volle breedte maar voornamelijk toch op risico's voor de organisatie en de uitgevoerde processen.
De risico benadering vanuit de ISO13485 en de daarin aangeroepen ISO14971 leidt tot een hoge kwaliteit van medische hulpmiddelen door de aangereikte methodes en de strikte regels. Een aspect wat hierin vaak als erg lastig wordt ervaren is de afweging van de voordelen voor de patiënt tegen álle restrisico tezamen.



Jelle Winia (HTS Elektrotechniek Leeuwarden, Bedrijfskunde SWOT Enschede) is een quality professional en sinds 1990 actief in verschillende kwaliteitsgerelateerde functies. Hij heeft gewerkt in diverse sectoren als Defensie, Elektronica Assemblage, Automotive, Nucleair, Aerospace. De laatste jaren was Jelle als Quality Manager bij een startend bedrijf in Medische Hulpmiddelen onder andere verantwoordelijk voor het onderhouden van het kwaliteitssysteem. Daar heeft hij ook meegewerkt aan het verbeteren van de processen voor Risico Management. Recent is hij begonnen als Supplier Quality Engineer bij VMI in Epe. Hier is hij verantwoordelijk voor de kwaliteit van leveranciers en koopdelen voor machines die gebruikt worden voor het verpakken van medicijnen per uitgiftemoment. Jelle heeft diverse opleidingen gevolgd op het gebied van kwaliteitszorg, auditeren (lead auditor), Lean Six Sigma (Black Belt) etc.

Samenwerking als antwoord op de risico's bij gespecialiseerd vervoer van complexe installaties

Zeton maakt, naast kleine, ook grote complexe installaties die omwille van het transport modulair worden opgebouwd. Ze worden in de Zeton Constructiehallen samengebouwd en getest. Daarna worden ze weer in transporteerbare modules opgedeeld, verpakt, getransporteerd naar de klant en ter plaatse weer opgebouwd. Voor het transport wordt veelal samengewerkt met de firma Wagenborg uit Hengelo. Wagenborg Nedlift is specialist op het gebied van horizontaal, verticaal en zwaar transport. In combinatie met vakkundige engineering en projectmanagement biedt Wagenborg Nedlift een compleet pakket aan diensten voor hijswerk, zwaar transport en montage. Wagenborg Nedlift is in geheel Europa en daarbuiten actief voor opdrachtgevers uit onder meer de olie- en gasindustrie, de petrochemische industrie, de energiesector en de sector bouw en infra.
Bij het transportproces voor de installaties van Zeton liggen vele risico's op de loer op gebied van financiën, veiligheid en planning. Zaken die een transport risicovol kunnen maken zijn onder andere bijzondere afmetingen en gewichten, lastige bochten, moeilijke, lange trajecten, het combineren van water- en wegtransport, door een dak of het uitvoeren van een zogenaamde blinde hijs waarbij het object niet zichtbaar is voor de operator van de hijskraan. Ook komt het soms voor dat moet worden gewerkt in de directe nabijheid van een werkende fabriek in de petrochemische industrie. Samen weten Zeton en Wagenborg deze complexe transporten steeds weer tot een succesvol einde te brengen. Wat maakt deze beide organisaties hierin zo succesvol?

Complexe projecten

Toen we in oktober 2016 met de KKT bij Zeton op bezoek waren werd er druk gewerkt aan een indrukwekkende installatie voor het project 1334J. Met dit project werd voor de klant van Zeton een "kraamafdeling voor nieuwe plastics" gerealiseerd. Tot nu toe experimenteerde en testte deze klant uitsluitend op lab-schaal' waarbij in een lab-opstelling enkele kilo's per uur van een gewenst product werden gemaakt. Nu kunnen ze testen op grotere schaal en kan het proces van een commerciële fabriek worden geïmiteerd. Daarbij zijn alle stappen van het proces geïntegreerd achter elkaar gezet en kan aan zowel product- als procesontwikkeling worden gewerkt. Deze installatie was 20 meter breed en diep en 28 meter hoog. Dat is hoger dan de constructiehal van Zeton waardoor er zelfs een opening in het dak moest worden gemaakt en de proeffabriek naar buiten stak. Hier overheen was een witte tent geplaatst die al van grote afstand te zien was. De aflevering van een dergelijke installatie op locatie bij de klant is een project op zich waar veel risico's aan verbonden zijn. Zeton en partner Wagenborg Nedlift weten dit elke keer weer trefzeker tot een goed einde te brengen. Samen inventariseren ze de factoren die hiervoor van belang zijn.

Niet nadenken maar voordenken

Wanneer Zeton een opdracht voor een grote installatie verwerft wordt dit project volgens een vaste methodiek afgewikkeld. Scrum wordt toegepast op het gebied van planning. Voor V&G (Veiligheid en Gezondheid) wordt voor elk project een V&G plan opgesteld. Voor werkzaamheden met een verhoogd risico wordt vooraf een Taak Risico Analyse (TRA) gedaan. De risico's voor een dergelijk project zijn groot en hier moet dan ook goed naar gekeken worden.

De installatie wordt zodanig in modules verdeeld dat de afzonderlijke delen later geschikt zijn voor transport. Binnen de engineeringsafdeling van Zeton is specifieke kennis aanwezig over de algemene regels voor afmetingen en gewicht.

Op tijd aanmelden

Voor de risico's die gerelateerd zijn aan het transport wordt al vroeg in het project contact gezocht met Wagenborg. Wagenborg analyseert de mogelijke routes en adviseert Zeton

over de meest optimale keuze voor de wijze van transport (over water, over de weg). Bij de analyse wordt rekening gehouden met zaken als bomen, bruggen, intensiteit van dagverkeer, maar ook met zaken als hoogwater en gepland onderhoud aan bruggen en wegen. Zo kan het voorkomen dat een lading niet onder een brug door past. Wanneer er geen bruikbaar alternatief is kan er dan zelfs voor worden gekozen om de lading voor de brug op te hijsen en aan de andere kant weer op het schip terug te plaatsen.

Elkaar kennen en durven aanspreken

Een van de factoren die sterk bijdraagt aan een veilig en efficiënt verloop van het laden, het transport en het lossen en plaatsen van de installatie is de nauwe samenwerking tussen de twee bedrijven. Bij de analyse van het hijsongeval in Alphen aan de Rijn is naar voren gekomen dat slechte communicatie een belangrijke factor bij het ongeval was. Verschillende partijen vertrouwden er ten onrechte op dat zaken geregeld of geanalyseerd waren, dat bleek echter niet het geval.

In de samenwerking tussen Wagenborg en Zeton zijn hier heldere afspraken over gemaakt. Bovendien wordt veelal met dezelfde ploegen gewerkt waardoor mensen elkaar kennen en er korte communicatielijnen zijn gecreëerd.

Wagenborg Nedlift stelt een hijs-tekening op met een uniek nummer. Hierop staan oa de hijsmiddelen en de maten en gewichten van de te hijsen objecten. De specifieke TRA hijsen wordt door Zeton opgesteld op basis van deze tekening en een algemene TRA van Wagenborg. Hierin komt elk te hijsen frame aan bod. Deze TRA's liggen in elkaars verlengde en worden door de teams van Zeton en Wagenborg met elkaar besproken.

Een van de mogelijke risico's is een onjuiste volgorde van aanleveren bij de eindklant. Je kunt de installatie zien als een bouwpakket; de module die er het eerst wordt afgepakt moet er bij de klant weer als laatste worden opgezet. Dit vereist inzicht en begrip bij de transporteur. Op de dag dat een project geladen wordt voor transport kan er, dankzij het feit dat de beide teams goed op elkaar zijn ingespeeld, soepel worden samengewerkt. De hiërarchie en taakverdeling zijn helder en de mensen vertrouwen elkaar en voelen zich vrij om elkaar aan te spreken. Er wordt als één team samengewerkt naar het gemeenschappelijke doel en dat is het goed en veilig transporteren en installeren van de installatie op de plek van bestemming!

De toekomst

De samenwerking tussen Wagenborg Nedlift en Zeton is een mooi voorbeeld van twee internationale bedrijven die lokaal, Twentse nuchterheid combineren met aandacht en respect voor 'noaberschap', kwaliteit en veilig werken. Beide partners hebben de intentie dit nog jaren voort te zetten.

ISO 9001: 2015

Zeton gaat juni 2017 op voor ISO9001:2015 en Wagenborg doet dit een jaar later. Welke visie heeft elk bedrijf hierbij, met name op het risicogestuurd Q-management, wat hebben ze al voor elkaar en welke aanpassingen zijn nodig?

Voor Zeton is risicogestuurd Q-management zeker niet nieuw. Wel nieuw is dat de ISO norm daar nu ook aandacht aan besteedt. Voorheen kon je een ISO certificering krijgen op een vierkante tennisbal. Dat is met de 2008 norm gewijzigd. Toen kwam klantgerichtheid al nadrukkelijker om de hoek. Met de huidige 2015 norm wordt ISO 9001 volwassener en is het management nadrukkelijker aan zet. Natuurlijk werd er altijd al wel aan risico's gedacht, maar in de huidige norm komen risicomanagement en leiderschap nadrukkelijker naar voren.

Zeton heeft DNV GL als certificeringsorganisatie. Het QHSE managementsysteem van Zeton hoefde nauwelijks aangepast te worden, wel heeft men de risico's en kansen voor de organisatie nu gestructureerder in beeld. De daaruit voortvloeiende doelstellingen worden in de organisatie uitgerold.

Gerard ziet veel mensen om zich heen onnodig worstelen met de verschillende ISO normen. "Een ISO norm is een hulpmiddel, geen wetboek". Zelf probeert hij zoveel mogelijk integraal te werken en zijn eigen visie op managementsystemen toe te passen. Hij is van mening dat zo'n systeem primair tot verbetering moet leiden. Een certificering is een brevet van vermogen; door een externe partij is vastgesteld dat het systeem leidt tot verbetering. Als je KAM mensen in je organisatie aanstelt om het certificaat te behouden, ben je volgens Gerard niet optimaal bezig met je managementsystemen. Certificering kan een resultaat zijn, maar moet zeker geen doel op zich worden. Certificaten zijn nuttig om bijvoorbeeld potentiele klanten te laten zien dat je een volwassen organisatie hebt. Het kan bij een klant meewegen om met jouw bedrijf in zee te gaan. Zodra er producten of diensten geleverd worden, telt dat certificaat niet meer, maar telt enkel de kwaliteit van het geleverde.

Voor een audit extra opruimen of medewerkers instrueren vindt Gerard onzinnige activiteiten. "Bij ons krijgt niemand een instructie, we laten zien hoe we zijn en wie we zijn. Iedereen mag zeggen wat hij zeggen wil, geen cosmetische verhalen, dat is de boodschap." Wel is het enorm belangrijk dat auditor en geauditeerde bij elkaar passen. Voor Zeton geldt dat een auditor kritisch moet zijn en gericht op (geleidelijke) verbetering. Daarbij hoort een praktische instelling waarbij het getoonde moet voldoen aan de geest van de norm. Door een dergelijke manier van auditen brengt de auditor de organisatie ook verder. Hierdoor en door de pragmatische benadering van kwaliteit, arbo en milieu binnen de organisatie wordt verbetering binnen de organisatie gerealiseerd.

Ingrid vult aan: De slechtste uitspraak is "We moeten dit doen voor ISO". Deze uitspraak heeft in het verleden vaak geleid tot doorschieten. We moeten goed blijven kijken wat echt verplicht en/of zinvol is en wat niet. Als voorbeeld noemt ze het interne voorschrift om een bepaalde audit elke maand uit te voeren. Bij doorvragen bleek dit ooit ten behoeve van een, inmiddels verouderde, veiligheidsnorm te zijn ingesteld en was dit een eigen leven gaan leiden. Het terugdraaien hiervan stuitte vreemd genoeg op weerstand vanuit de directie. In het algemeen wordt dit vaker gezien: de angst om verouderde en/of overtollige controles en voorschriften te elimineren.

Gerard: Er zijn ook legio voorbeelden van uitspraken die gaan over "mag dat wel van de Arbowet?" Allerlei indianenverhalen doen uiteindelijk de ronde. Van de Arbowet moet één ding: niemand ondervindt nadelige gevolgen van het werk. De Arbowet en –regelgeving is een uitermate nuttig handvat waarmee je de doelstelling van de arbowet beter kunt nastreven. In dat kader is de MVK opleiding (Middelbare Veiligheidskunde) een heel goed middel om te leren omgaan met de Arbowetgeving. Dat heeft Zeton veel gebracht. Je moet goed naar je organisatie kijken en naar waarom je iets wilt bereiken. Zo hebben we de BHV opleiding van onze mensen anders georganiseerd. In het verleden deden we ééns per jaar een dag BHV herhaling. Op dat moment werden alle kennis en vaardigheden in een keer herhaald. De betrokken BHV-ers moesten op dat moment alles in zich op zien te nemen en de rest van het jaar onthouden. Niet erg realistisch natuurlijk. Nu bieden we de stof verdeeld over meerdere momenten per jaar aan en dat werkt veel beter. Onze invulling van de BHV herhaling is gebaseerd op de realistische risico's in ons bedrijf. Zo hebben we er bijvoorbeeld voor gekozen om in plaats van vooraf gepland, een ongeval met Lotus slachtoffer onverwacht te oefenen en dat verspreid over het jaar. Voor een echt ongeval wordt immers ook niet vooraf de agenda getrokken.

Gerard Lansink Rotgerink

Gerard Lansink Rotgerink werkt sinds 2013 als QHSE engineer bij Zeton. Daarvoor was hij in een soortgelijke rol werkzaam bij Actronics in Almelo en Verosol in Eibergen.

Ingrid Voost

Ingrid Voost (Laboratoriumschool Deventer, Bedrijfseconomie, Hoger Veiligheidskundige, Stralingsdeskundige) is allround HSEQ professional en sinds 1991 actief in verschillende HSEQ gerelateerde functies. Ingrid heeft gewerkt in diverse sectoren als Chemie, Transport, Werktuigbouwkunde, Elektrotechniek, Olie & Gas, Nucleair, Defensie en Mobiele Kranen. De laatste jaren is Ingrid Voost werkzaam geweest bij Imtech Industry International als Manager QHSE & Security waar ze veel internationale ervaring heeft opgedaan.
Momenteel is Ingrid werkzaam bij Wagenborg Nedlift in Hengelo, met eindverantwoordelijkheid voor de vestigingen in Nederland, België en Duitsland.
Risico Management heeft in haar gehele carrière als een rode draad door haar werkzaamheden gelopen, echter heeft zich in de loop der tijd en per branche zich telkens weer anders geuit.
Ingrid heeft diverse aanvullende cursussen en trainingen gevolgd. Zo heeft ze in 2016 het certificaat Associate Tripod Practitioner behaald na het succesvol afleggen van de assessment. Het behalen van dit certificaat draagt bij aan het kunnen maken van goede risicobeoordelingen met diepere achterliggende oorzaken. Daarnaast is ze veiligheidstrainer en beheerst diverse talen uitstekend, wat internationaal natuurlijk zeer welkom is.

Theory of Constraints: Is dat echt zo'n goed idee?

TOC is een methode[1], met bijbehorende technieken, voor het opsporen van knelpunten (constraints) in systemen. Het idee is dat er in elk systeem iets te vinden is, dat bepalend is voor (de beperking van) de prestatie van dat systeem. De methode bestaat uit vijf stappen:Het opsporen van de (belangrijkste) oorzaak van de beperkingen in het systeem (root cause),

1. Analyseren van de oorzaak en vinden van een oplossing,
2. Beoordelen van de (voorgestelde) oplossing,
3. Identificeren van wat het implementeren van de oplossing bemoeilijkt en hoe daarmee om te gaan,
4. Definiëren en plannen van de acties die nodig zijn om de oplossing te implementeren.

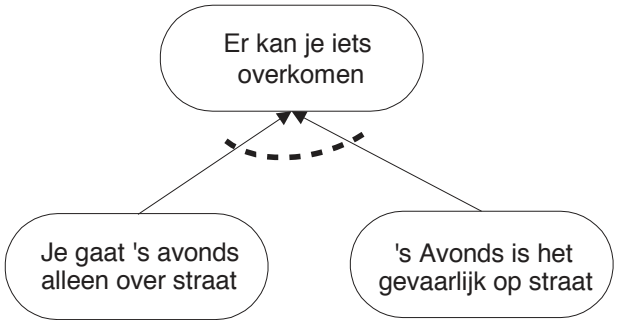
Bij iedere stap, hoort een techniek, een wijze van aanpak. De technieken zijn op zichzelf bruikbaar. Anders gezegd, een specifieke TOC-techniek kan voor een specifieke opgave worden ingezet.
Zo kan de techniek van stap 3 – beoordelen van de (voorgestelde) oplossing – worden gebruikt om de kwaliteit van een idee te onderzoeken. Het volgende gaat over die toepassing. In de appendix komen stappen 4 en 5 kort aan de orde.

Kanttekening:

Uitgangspunt voor het toepassen van Theory of Constraints (TOC) is dat de teamleden voldoende raakvlakken hebben voor het onderwerp dat aan de orde is. Voor onderwerpen die in het dagelijks leven (kunnen) voorkomen, geldt dat in principe voor iedereen. Om die reden, gebruik ik hierna een (verzonnen) voorbeeld uit het dagelijks leven. De techniek is echter algemeen toepasbaar, dus ook voor zakelijke onderwerpen.

Basistechnieken

Het in TOC gebruikte instrument is een zogenoemde 'boom' (tree). Een boom is – uiteindelijk – een consistent geheel van oorzaken en gevolgen (entiteiten). De oorzaken en gevolgen worden weergegeven door uitspraken. In de boom worden die verbonden door pijlen die de oorzaak-gevolg-relatie weergeven.
Figuur 1 is een voorbeeld van de standaard boom. Het is het voorbeeld van een ouder die zich zorgen maakt over zijn dochter die 's avonds alleen over straat gaat. Zijn redenering wordt weergegeven door de boom.



Figuur 1 – Voorbeeld boom

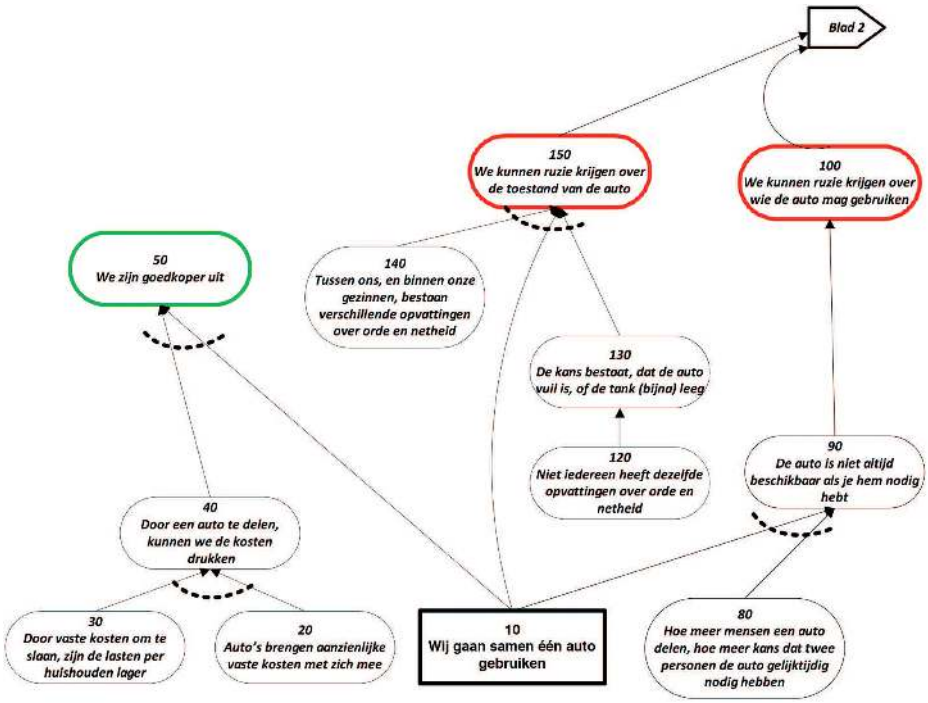
Er staan drie symbolen in de figuur:

- De ballon, met de uitspraak (de entiteit),
- De pijl, oorzaak-gevolg-relatie (in de richting van de pijl),
- De 'banaan', die (in dit geval twee) oorzaak-gevolg-relaties samenvoegt.

De redenering voor het linkerdeel van de boom luidt: Als 'Je gaat 's avonds alleen over straat' dan 'Er kan je iets overkomen'. Die redenering is onvoldoende (evenals de redenering: als ''s Avonds is het gevaarlijk op straat' dan 'Er kan je iets overkomen'). De 'banaan' maakt hiervan: als 'Je gaat 's avonds alleen over straat' en ''s Avonds is het gevaarlijk op straat' dan 'Er kan je iets overkomen'.

De 'bomen' hebben namen. De boom voor stap 3 heet 'Boom van de toekomstige werkelijkheid' (future reality tree, FRT).

1 Binnen TOC bestaat ook nog een aanpak die POOGI, process of ongoing improvement, wordt genoemd. Het valt buiten de bedoeling van dit artikel, om daarop in te gaan.



Figuur 2 – Boom van de toekomstige werkelijkheid

Boom van de toekomstige werkelijkheid

Aan de basis van deze boom staat het idee. De te verwachten gevolgen van het idee worden in de boom weergegeven. Dit wordt gedaan door te redeneren, zoals in het voorbeeld hierboven.

Het idee hier, is dat twee gezinnen gezamenlijk een auto aanschaffen en gebruiken. Links staat het voordeel van die afspraak (er kunnen meer voordelen zijn), rechts staan de (mogelijke) nadelen.

De werkwijze is eenvoudig: bedenk wat de voor- en nadelen (TOC: gewenste en ongewenste effecten) van het idee zijn en verwerk die – op basis van redeneringen en onderliggende overwegingen – in een boom.

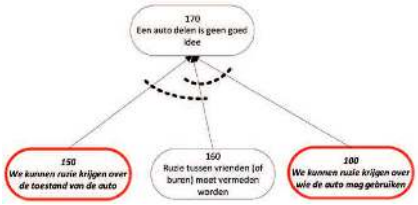
Een paar simpele zaken helpen de boom te lezen en te gebruiken:

- Nummering van de entiteiten (niet opvolgend; dat maakt het gemakkelijker entiteiten bij te plaatsen; een boom kan groter zijn dan één pagina, gebruik dan een off-page connector)
- Randdikte, -kleur en vorm om entiteiten met verschillende betekenis te onderscheiden.

Is dit idee wel zo goed?

Met andere woorden, wegen de voordelen op tegen de risico's (We kunnen ruzie krijgen)?

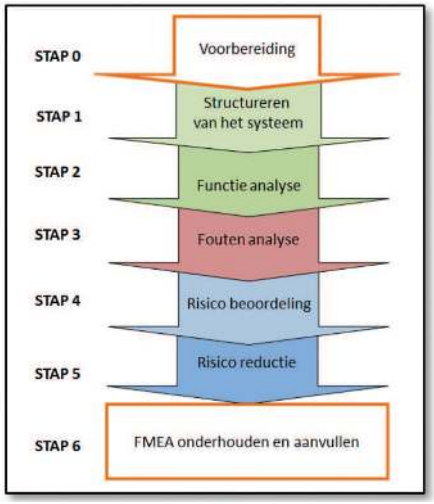
Eddy van Stijn is na zijn studie werktuigbouwkunde en bedrijfskunde aan de THT, voornamelijk bezig geweest op het snijvlak van organisatie, goederenstroombeheersing en automatisering, het laatst bij Atos Origin. Begin negentiger jaren – toen werkzaam bij Holec – in aanraking gekomen met de Theory Of Constraints. Hij is medeoprichter van de TOC Club Nederland en heeft samen met Eli Goldratt en de andere leden van het bestuur van de TOC Club de methode en technieken voor TOC (denkprocessen) ontwikkeld.



Figuur 3 – Risico-analyse

Uitvoeren van de PFMEA

Bij het uitvoeren van een PFMEA hanteren we het zeven stappen model:



Figuur 1 – Zeven stappen model

Stap 0: Voorbereiden van de FMEA

Scope

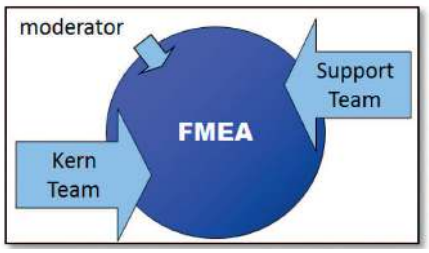
De scope van de FMEA is gelijk aan de omvang van het proces. Deze omvang wordt bepaald door de verantwoordelijkheid van de proces eigenaar.

Team

Het kernteam van de PFMEA bestaat uit de meest nauw bij het proces betrokken specialisten en wordt geleid door de proceseigenaar.

Support-team leden brengen specifieke kennis of ervaring in. Dit kan naar keuze plaatsvinden door aanwezig te zijn bij een of meerdere teamsessies waarbij de onderwerpen worden besproken waaraan zij kunnen bijdragen of in een andere passende vorm.

De moderator leidt de team sessies. Hij is goed bekend met de FMEA-methodiek en heeft als taak het team efficiënt door het FMEA-proces te leiden. Hij zorgt ervoor dat alle teamleden zich vrij voelen om hun bijdrage te leveren en ziet erop toe dat alle relevante informatie op de juiste wijze in de FMEA wordt vastgelegd.



Figuur 2 – FMEA team

Het totale team dat bij een sessie aanwezig is moet niet te groot zijn, een maximum van 5 personen is aanbevolen. De kernteam leden zijn er voor verantwoordelijk dat alle vanuit het supportteam benodigde informatie beschikbaar komt voor het team. Dit kan naar eigen inzicht door supportteam leden uit te nodigen voor een of meerdere sessies maar ook door deze te verkrijgen in een persoonlijk gesprek of op een andere wijze.

Informatie verzamelen

Specificaties

Als eerste moet worden vastgesteld wat het gewenste resultaat van het proces is. Voor het productieproces zijn dat de productspecificatie en de eisen die aan het proces zelf worden gesteld op gebied van kwaliteit, kosten (materiaal en uren verbruik) en snelheid (levertijd). Voor logistieke en ondersteunende processen zal dit per proces moeten worden bepaald en indien nodig gedocumenteerd.

Het is erg belangrijk dat voor het starten van de FMEA de specificaties helder zijn. Hiermee wordt onnodige discussie tijdens de tijdens de FMEA sessies voorkomen en dat delen van de FMEA zelfs opnieuw moeten worden gedaan.

Lessons learned

Voor de volledigheid van de analyse is het belangrijk om ook de lessen uit het verleden, de kwaliteitshistorie mee te nemen. Hiervoor dient te worden gekeken naar het klachtenregistratie systeem, waarin alle interne en externe incidenten zijn vastgelegd. Hierbij is de klachtomschrijving (8D stap 2) gelijk aan het Failure Effect in de FMEA en is de rootcause (8D stap 4) gelijk aan de Failure Cause in de FMEA. De corrigerende maatregelen die worden ingevoerd als stap 6 in de 8D staan in de FMEA als preventieve of detectie maatregelen.

Omdat niet alle verstoringen uit het verleden zijn vastgelegd in de klachtenregistratie is het ook belangrijk om in gesprekken met interne klanten te toetsen in hoeverre de bestaande processen voldoen. In de praktijk blijkt dat fouten en onvolkomenhedenvan een proces door de ontvangende interne partij geruisloos worden gecontroleerd en opgevangen zonder dat dit direkt zichtbaar of merkbaar is. In veel gevallen is dit zodanig ingesleten dat het niemand meer opvalt en daarmee ook niet duurzaam wordt gecorrigeerd en blijven daarmee dubbel werk en dubbele kosten in stand.

FMEA's van vergelijkbare processen

Indien beschikbaar kunnen deze worden gecheckt voor relevante informatie

Overige informatie

Tot slot is het van belang om vooraf te checken of de klant specifieke eisen stelt aan de PFMEA. Dit kan bijvoorbeeld betrekking hebben op de indeling van het formulier, specifieke informatie in de kop, het gebruik van een eigen waarderingscatalogus of de gewenste output.

Stap 1: Structureren van het systeem

De basis voor de PFMEA is de structuur van het proces, ofwel het proces flow schema. In de FMEA worden de processtappen uit het flowschema aangehouden en indien nodig aangevuld met specifieke stappen in de uitvoering.

Wanneer een handeling vaker voorkomt hoeft deze niet elke keer opnieuw in de FMEA te worden vermeld. Deze mag per proces één keer worden vermeld. Bij de kolom processtap moet dan worden ingevuld: Algemeen. Voorbeelden hiervan zijn het hijsen van producten en materialen of het intern transport.

Stap 2: Functieanalyse

Voor een productieproces dienen de meest relevante tekening eisen (product karakteristieken) te worden geanalyseerd. Deze worden vermeld bij de processtap waarbij ze worden gecreëerd.

Stap 3: Foutenanalyse

Start met het invullen van de Failure Mode. Dit is het falen van de specificatie. Er kunnen meerdere fouten mogelijk zijn. Noem alleen de echt relevante fouten. Brainstorm nu per Failure Mode tot welke effecten deze kan leiden en tot slot wat de mogelijke oorzaken ervoor kunnen zijn. Noem ook hier weer alleen de relevante fouten.
NB: Bij elke handeling wordt verondersteld dat de voorgaande handelingen door de eigen en andere afdelingen correct zijn uitgevoerd. Ook wordt aangenomen dat toegeleverde materialen van leveranciers voldoen aan de specificaties.

Stap 4: Risicobeoordeling

Gebruik een goede waarderingstabel om de waarderingen te bepalen. Let erop dat voor elke Failure Cause in de FMEA een RPN wordt berekend en dat er steeds wordt gerekend met het hoogste Severity getal.

Severity
effect op product / resultaat

Klasse	*Score*	*omschrijving*	*Kwaliteit*	*Snelheid*	*Kosten*	*Reputatie*
Zeer hoog	*10*	(levens)gevaar of zeer grote schade primaire functie(s) onmogelijk	volledig falen primaire functie TAO	Levering niet mogelijk gedurende langere tijd hoge boetes / verlies grote order(s)	voortbestaan bedrijf in gevaar	ernstige, langdurige reputatie-schade
hoog	*8*	grote schade primaire functie(s) beperkt	gedeeltelijk falen van primaire functie	Levering niet mogelijk gedurende korte tijd	significant negatief effect op jaarwinst	ernstige, kortdurende reputatie-schade
medium	*5*	schade secundaire functie(s) onmogelijk	falen van secundaire functie verkorte levensduur	grote vertragingen intern vertraging extern >1 dag	significant negatief effect op maand/kwartaal winst	kleine reputatie-schade
laag	*3*	kleine schade secundaire functie(s) beperkt	niet functionele defecten herstelbaar in eigen standaard processen	kleine vertragingen intern vertraging extern > 0.5 uur	klein effect op marge	kleine reputatie-schade in beperkte kring
geen	*1*	geen effect				

Figuur 3 – Waarderingstabel

Stap 5: Risico reductie

Beschrijf hier de verbetermaatregelen die worden genomen tijdens het ontwikkeltraject of die later worden ingevoerd naar aanleiding van klachten, procesoptimalisatie, wijzigingen of om andere redenen. Voor de maatregelen die achteraf worden ingevoerd is het belangrijk om een eenduidige referentie te noemen naar de aanleiding van de update, bijvoorbeeld het klachtnummer.
Bij het vaststellen van het verbeterplan is het doel om tot een plan te komen dat haalbaar en realistisch is binnen de beperkingen van budget/ kostprijs en capaciteit binnen het project. Hierbij mogen plandata voor het afronden van de acties ook buiten het project liggen indien partijen het daarover eens zijn. Voor het bepalen van verbeteracties dient de volgende prioriteit te worden aangehouden:

- Severity 8 of 10: Kijk of voor deze risico's redelijkerwijs voldoende is gedaan om de Failure Causes en Failure Modes te voorkomen
- Relatief hoge SxO score. Hiermee wordt de focus op preventie van fouten gelegd. Bij twijfel over de noodzaak voor extra maatregelen kan de Detectie score hier worden gebruikt om de doorslag te geven.

Stap 6: FMEA onderhouden en aanvullen

Het is van belang dat de FMEA up-to-date wordt gehouden door de relevante verbeteringen en optimalisaties van het proces er steeds in te verwerken.

proces stap / procedure #	functie / specificatie	failure mode	failure effect	Severity	failure cause	Huidige beheersmaatregelen: Occurrence	preventief	detectie	Detection	RPN
Algemene uitgangspunten: xx xx xx										
lassen	deel A verbinden met deel B / treksterkte > xx	treksterkte te laag	levensduur te kort	8	lastemperatuur te laag	5	ervaring lasser	moeilijk lassen	6	240
			scrap	4	lasdruk te laag	5	ervaring lasser	lasvorm niet in orde	5	200
					vervuiling smeltbad	7	ervaring lasser	verkleuring	4	224

Figuur 4 – FMEA structuur

Bij wijziging van het product dient naast de technische goedkeuring door engineering tevens door productie te worden afgewogen of deze significant zijn voor de risicobeoordeling van het proces. Wanneer dat (mogelijk) zo is moet een review van de FMEA worden gedaan voor dit specifieke aspect. Bronnen van wijzigingen kunnen onder andere zijn: het structureel oplossen van een klacht, een materiaal dat niet meer beschikbaar is, interne optimalisatie, een bevinding in een audit.

Het FMEA-formulier

Bij het invullen van het FMEA formulier kan verwarring ontstaan over wat nu precies in de verschillende kolommen moet komen te staan. Daarom hieronder een beknopte omschrijving voor elke kolom.

proces stap / procedure #	functie / specificatie	failure mode	failure effect	Severity	failure cause	Huidige beheersmaatregelen: Occurrence	preventief	detectie	Detection	RPN	Geplande verbeter maatregelen	Verantwoordelijk datum gereed status	uitgevoerde verbeter maatregelen	Rest Risco: Severity	Occurrence	Detection	RPN
lassen	deel A verbinden et deel B / treksterkte > xx	treksterkte te laag	levensduur te kort	8	lastemperatuur te laag	5	ervaring lasser	moeilijker lassen	6	240	(P) automatische lastemperatuur indicatie			8	2	6	96
			scrap	4	lasdruk te laag	5	ervaring lasser	visuele inspectie lasvorm	5	200							
					vervuiling smeltbad	7	ervaring lasser	visuele inspectie verkleuring	5	224							

Figuur 5 – FMEA formulier

Risico's analyseren met een Proces FMEA

PFMEA (Process Failure Mode and Effect Analysis) is een systematische methode om risico's te analyseren in een proces. De methode wordt vooral toegepast op productie processen maar is ook geschikt voor het analyseren van een administratief of logistiek proces. De PFMEA is een stuk gereedschap waarmee de eigenaar van het proces kan vaststellen hoe robuust het proces is ingericht ofwel hoe goed het proces in staat is om het gewenste resultaat op te leveren en welke risico's daarbij spelen. De risico-inventarisatie kan vervolgens worden gebruikt om prioriteiten te stellen voor het verbeteren en optimaliseren van het proces.

De FMEA-methode bestaat al sinds eind jaren 40 van de vorige eeuw toen het Amerikaanse leger een methode ontwikkelde om de effecten van materiaalstoringen op de effectiviteit op het slagveld te onderzoeken. Via de ruimtevaart en de luchtvaartindustrie kwam FMEA in de jaren '70 in de automobielindustrie terecht en vandaag de dag wordt het in vele industrieën toegepast. Ondanks de brede toepassing van de methodiek blijkt het toch lastig om goede FMEA's te maken, op tijd en efficiënt samengesteld en om ze te onderhouden als levende documenten.

Kolom naam	Beschrijving
Proces stap	Naam en/of nummer van de processtap Procedure nummer
Functie	Product-eis die in deze stap wordt gerealiseerd. Dit is de toegevoegde waarde van de processtap.
Specificatie	Specificatie van de functie
Failure Mode	Potentiele fout die kan optreden voor deze functie. Gebruik de specificatie in de vorige kolom als indicatie voor Failure Modes.
Failure Effect	Het gevolg dat kan optreden als gevolg van de Failure Mode. Dit kan betrekking hebben op het product, het proces, de klant, de gebruiker, conformiteit aan de wet of industriële normen. Gebruik hierbij waar mogelijk de omschrijvingen van de waarderingstabel voor Severity. NB: Voor elke Failure Mode kunnen meerdere Effecten optreden.
Severity	Hoe erg is het als het Effect werkelijk optreedt? De score dient door de klant te worden geschat, wanneer dit niet mogelijk is moet het zo goed mogelijk voor de klant worden geschat. De score voor het Effect wijzigt niet door verbetermaatregelen aan het product. Gebruik voor het schatten van de score de waarderingstabel voor Severity. Wanneer er meerdere effecten mogelijk zijn voor een Failure Mode moet deze kolom worden samengevoegd tot een cel waarin de hoogste waarde wordt vermeld. Hiermee wordt straks de RPN berekend voor de verschillende Failure Causes.
Failure Cause	De oorzaak voor de Failure Mode. Gebruik de 5Why methode om de werkelijke oorzaak (root Cause) te determineren, hiervoor zijn extra kolommen uit te vouwen in het formulier. De root Cause is gevonden wanneer hiervoor direct beheersmaatregelen te beschrijven zijn. NB: meestal zijn er meerdere Failure Causes voor een Failure Mode. Noem hier de meest relevante, een per regel.
Huidige beheersmaatregelen	In deze kolommen kunnen de al bestaande/ al in het project voorgenomen maatregelen worden beschreven.
Preventief	Alle maatregelen die erop gericht zijn om het ontstaan van de Failure Cause te voorkomen. (Zie waarderingstabel)
Occurrence	Waardering voor de preventieve maatregelen. Wat is de ingeschatte frequentie van optreden van de Failure Cause met de beschreven preventieve maatregelen? NB: Hierin dient nadrukkelijk ook de werkelijke effectiviteit van de maatregelen voor deze specifieke Failure Cause te worden meegenomen. Gebruik voor het schatten van de score de waarderingstabel voor Occurrence.
Detectie	Alle maatregelen die erop gericht zijn om de Failure Cause of de Failure Mode te ontdekken. (Zie waarderingstabel)
Detection	Waardering voor de detectie maatregelen. Wat is de kans van ontdekken en in welk stadium kan de fout worden ontdekt? NB: Neem hier ook de kwaliteit van de detectie maatregel mee. (Wordt het meetmiddel gekalibreerd, is er een MSA studie op gedaan en wat kwam daar uit,…) Gebruik voor het schatten van de score de waarderingstabel voor Detection.
RPN	Severity x Occurrence x Detection. Elke Failure Cause krijgt een RPN-waarde in het formulier. Let op dat er steeds met de hoogste Severity wordt gerekend!
Geplande verbetermaatregelen	Hier kunnen additionele beheersmaatregelen worden beschreven om het risico te verlagen. Ga hierbij uit van de volgende volgorde: 1. Severity 9 of 10 2. Investeren in preventie. 3. Pas wanneer de occurrence redelijkerwijs niet verder omlaag kan worden gebracht wordt ook gekeken naar een betere detectie. Voor het up-to-date houden van de FMEA worden hier ook verbetermaatregelen vanuit klachten, interne problemsolving, kostenreducties en alle andere wijzigingen aangegeven. Vermeld hierbij altijd een referentie naar de betreffende wijziging of klacht. Begin de omschrijving met (P) of (D) om aan te geven of het een preventie of detectie maatregel betreft.

Kolom naam	Beschrijving
Verantwoordelijk Datum gereed Status	Voor elke verbetermaatregel wordt hier aangegeven wie het uitvoert, wanneer het klaar zal zijn en wat de status van de actie is.
Uitgevoerde verbeter maatregelen	Wanneer een actie gereed en geverifieerd is wordt deze verplaatst naar deze kolom. Let op: hier alleen de laatst ingevoerde verbeteringen laten staan. Wanneer er weer een update is de huidige inhoud van deze kolom toevoegen aan kolommen "Huidige beheersmaatregelen" met vermelding van de referentie.
Rest Risico SOD-SxO/RPN	Hier kunnen de nieuwe scores voor O en D worden genoteerd en de nieuwe RPN worden berekend. Let op: • De Severity blijft gelijk, ongeacht de maatregelen die je treft. • De Occurrence kan alleen veranderen met nieuwe preventieve maatregelen • De Detectie kan alleen veranderen met nieuwe detectie maatregelen

Voor en nadelen van FMEA

Een voordeel van FMEA is dat het een systematische methode is met goede handvaten om risico's te waarderen. Dat is de reden dat het maken van een FMEA binnen steeds meer industrieën verplicht is geworden. Een nadeel is dat FMEA een kwalitatieve methode is. De fouten netwerken in de FMEA geven slechts de potentiele oorzaak en gevolg verbanden aan maar zeggen niets over de kans dat een specifieke oorzaak ook werkelijk tot het potentiele gevolg zal leiden. Ook wordt er niet gekeken naar onderlinge afhankelijkheid van oorzaken zoals in een FTA (Fault Tree AnalysisEr is echter ook een aantal nadelen. Een ander nadeel is dat zonder de juiste kennis en begeleiding een FMEA al snel kan uitgroeien tot een enorme omvang waarbinnen het team verdwaald raakt tussen een enorme hoeveelheid veel te gedetailleerde informatie. Dit heeft FMEA de naam bezorgd van een tijdverslinde bezigheid die weinig oplevert. Door FMEA goed te implementeren, heldere doelen te stellen en de teams te ondersteunen met een kundige moderator kunnen echter mooie resultaten worden behaald.

Nicole Mak was na haar studie werktuigbouwkunde en bedrijfskunde werkzaam in verschillende industrieën waaronder de automotive industrie. Daar heeft ze in verschillende rollen veel ervaring opgedaan met de typische automotive tools waaronder FMEA. Sinds enkele jaren ondersteunt Nicole met haar bedrijf smartFMEA als zelfstandig consultant bedrijven met FMEA. Daarnaast is ze gecertificeerd auditor voor de vernieuwde automotive norm IATF 16949 en ondersteunt ze bedrijven met de ISO 9001 norm.

Risicobeheersing voor defensiematerieel

Het beheersen van risico's ten gevolge van falen van systemen speelt vanzelfsprekend ook bij het materiaal dat door de Nederlandse defensie wordt ingezet. Hierover hebben we gesproken met Harmen van Heek, werkzaam bij de afdeling Toezicht Defensie Leveranciers (TDL) onderdeel van de Defensie Materieel Organisatie (DMO). Van Heek is het hoofd van de TDL – vestiging Oost in Enschede.

Taken van het Toezicht.

De belangrijkste taak van het Toezicht is borgen dat geleverde producten aan alle contractuele eisen voldoen. In het verleden werd dit voornamelijk gerealiseerd door het doen, of laten doen, van productkeuringen om vast te stellen of het product geen fouten had. Van Heek: tegenwoordig richt het toezicht zich weliswaar nog steeds op het borgen van alle contractuele eisen, maar kiest men nu voor een risico gebaseerde aanpak waarbij de nadruk ligt op het voorkomen van fouten. Door de risico gebaseerde toezichtaanpak worden de toezichtactiviteiten gericht op de relevante zaken. Daardoor kan nu met minder personele inspanning een beter resultaat bereikt worden, legt Van Heek uit.

Identificatie van Risico's.

Deze risico gebaseerde benadering gaat uit van vooraf geïdentificeerde risico's. Bij het identificeren van risico's staat de volgende vraag centraal "wat kan er fout gaan met een product en wat zijn de ongewenste gevolgen die dat heeft voor het gebruik, de gebruiker en de omgeving". Deze risico's worden "product risico's" genoemd en zijn intrinsiek gebonden aan het product en niet beïnvloedbaar door het toezicht of de leverancier. "De identificatie van de product risico's vindt altijd plaats in samenspraak met alle stakeholders" benadrukt Van Heek. Bij de risico identificatie worden alle omstandigheden meegenomen waaronder het product ingezet kan worden. Dit kan variëren van extreme klimatologische omstandigheden tijdens gebruik bij operaties in het hoge noorden tot vredesmissies in woestijngebieden rond de evenaar. Maar ook die voorkomen tijdens transport, (langdurige) opslag of onderhoud in het inzetgebied.

Alle geïdentificeerde product risico's worden geclassificeerd naar de aard van de gevolgen die het falen heeft op aspecten als veiligheid, inzetbaarheid, onderhoud, milieu etc. De classificatie van het product risico is dus altijd een maatstaf voor de ernst van de impact die het optreden van het risico heeft. Van alle geïdentificeerde risico's wordt vervolgens onderzocht wat ten grondslag kan liggen aan het optreden van dit risico. Dit wordt niet tot op componenten niveau doorgezet maar stopt meestal bij de kleinst mogelijke samenstelling (entiteit) die nog een eigen functionaliteit heeft. Een geschikte methode om door te dringen tot de oorzaak van de fout is de root cause analyse die in combinatie met de 5W ofwel "5 Times Why" methode gebruikt wordt. Hierbij wordt telkens de vraag "waarom het fout is gegaan" gesteld totdat, na ongeveer 5 keer vragen, de oorzaak (root cause) gevonden is.

Risico beheersing in de praktijk.

De expertise van de toezichthouders is het koppelen van de geïdentificeerde risico's en de daarmee samenhangende oorzaken aan ontwerp- en productieprocessen. Van Heek noemt een recent voorbeeld: "Bij één van de defensie leveranciers waarbij wij voor een bepaald product toezicht

moesten houden kwam het falen van een bepaalde lijmverbindig naar voren als root cause resultaat van de risico analyse. Tijdens de daarop uitgevoerde procesaudit bleek dat de leverancier onvoldoende maatregelen had genomen om te voorkomen dat het proces werd onderbroken, het is namelijk zo dat beide onderdelen moeten zijn samengevoegd voordat de aangebrachte lijm begint uit te harden (zogenaamde 'open tijd'). In het geval dat de operator voor een calamiteit weggeroepen kon worden was er geen back-up geregeld. De leverancier heeft nu geregeld dat een andere gekwalificeerde operator de bewerking overneemt als de eerste operator weggeroepen wordt."
Het probleem in het lijmproces was door 5 Times Why geïdentificeerd: het risico is dat van het product deze lijmverbinding tijdens operationeel gebruik bezwijkt. Waarom bezwijkt de lijmverbinding? Omdat deze niet goed is verlijmd. Waarom is deze niet goed verlijmd? Omdat de open tijd van de lijm was verstreken. Waardoor was dit verstreken? Omdat de operator het proces niet op tijd had afgerond. Waarom kon hij het niet op tijd afronden? Omdat hij werd weggeroepen en niemand kon overnemen. Waarom kon niemand overnemen? Omdat dit niet geregeld was!

Risico's tijdens het ontwerpproces.

Ook kan het zijn dat een systeem niet aan de verwachtingen voldoet omdat tijdens het opstellen van de ontwerpspecificaties door de leverancier niet met alle omstandigheden rekening is gehouden. Als bijvoorbeeld bij het opstellen van de specificaties voor een voertuig onvoldoende rekening is gehouden met alle aspecten die kunnen voorkomen in het inzetgebied, zoals het ook moeten kunnen bedienen van bepaalde apparatuur met handschoenen bij extreme koude, dan is het weliswaar niet direct een functionele tekortkoming maar de toekomstige gebruiker zal niet tevreden zijn. Deze

aspecten worden als product risico's ook meegenomen in de toezichtplannen en later getoetst of de ontwerpspecificaties hier in voorzien en of tijdens de productie deze aspecten voldoende geborgd zijn.
Producten voor defensie zijn vanwege hun complexiteit en inzet vaak gevoeliger voor risico's, heel vaak zijn de te ontwikkelen producten of systemen nog niet eerder gemaakt. Dit maakt het extra moeilijk een goede inschatting te maken van de specifieke risico's die kunnen optreden. Het heeft een zeer sterke voorkeur om risico's te elimineren in de eerste fases van het ontwerp, dan kan men keuzes maken die inherent veilig en risicoloos zijn. Als men pas later in een ontwerp of proces risico's identificeert is de weg terug om keuzes anders te maken vaak niet meer te realiseren. Enige optie is dan om iets aan het ontwerp toe te voegen dat het risico wegneemt of reduceert. Daarbij brengt de toevoeging op zich weer nieuwe risico's met zich mee. Het gebeurt ook te vaak dat die nieuwe risico's op hun beurt niet onderkend worden met alle gevolgen van dien. Volgens Van Heek probeert TDL daarom altijd mee te kijken in de ontwerpfase om vast te stellen dat vooral in het begin voldoende gelet wordt op het zo vroeg mogelijk elimineren van risico's.

Gebruikte AQAP normen.

Om defensie toezicht mogelijk te maken wordt in Defensie contracten bijna altijd de NATO norm AQAP-2110 (http://nso.nato.int/nso/zPublic/ap/AQAP-2110_EDD_V1_E.pdf) opgenomen. Deze contractuele norm is een aanvulling op de ISO 9001 en regelt enerzijds de NATO aanvullingen op de ISO 9001 en anderzijds de rechten en plichten van het defensie toezicht. De laatste versie van de AQAP-2110, versie D, is in overeenstemming met de ISO 9001:2015. Additionele eisen in AQAP-2110 zijn onder andere het recht van toegang voor het toezicht tot alle locaties waar activiteiten plaats vinden die voortkomen uit het contract maar ook dat een Quality Plan en een Configuration Management Plan gemaakt moeten worden. Samen met een Risk Management Plan moeten de plannen worden voorgelegd aan de defensie toezichthouder die de plannen mag afkeuren indien ze niet voldoen aan de gestelde criteria.

TDL voert het defensie toezicht uit volgens de AQAP-2070 (http://nso.nato.int/nso/zPublic/ap/AQAP-2070E(B)(3).pdf) norm. In de AQAP-2070 is de methodiek uitgewerkt om risico management uit te voeren. Er wordt gewerkt met Risk Impact en Risk Likelihood, elk met 3 niveaus: 1, 4 en 9. Beiden vormen samen de Risk Index. Bij een Medium Risk Index (> 4) wordt middels proces evaluatie vooraf onderzocht of de risico's voldoende beheerst worden. Bij een High Risk Index (> 16) worden vaak meerdere proces verificaties uitgevoerd in de ontwerp- en productiefase. Bij zeer hoge risico's kan besloten worden een product verificatie te doen of het product volledig aan een keuring te onderwerpen. Het elimineren van risi-

co's eerder in het proces heeft echter steeds de voorkeur.

Langere supplychain.

Wat door Van Heek ook als belangrijk wordt aangemerkt zijn de langer wordende inkoopketens. De prestatie van systemen is zo goed als de zwakste schakel, een snel voertuig kan qua motorvermogen uitstekend aan zijn eisen voldoen, als de ingekochte banden de hoge snelheid niet aankunnen komt men alsnog voor een probleem te staan. Deze regel komt naar voren in de hele keten. Als het ontwerp- en productieproces ergens niet goed wordt beheerst ontstaan zwakke schakels met mogelijk ongewenste gevolgen voor het gebruik, gebruiker of omgeving. Daarom worden, als dit uit de risico analyse naar voren komt, ook de ingekochte delen door het toezicht bij de onderleveranciers gemonitord zowel in binnen- als buitenland.

Toezicht bij buitenlandse leveranciers.

De NATO afspraken voorzien in de mogelijkheid toezicht door een ander NATO-land uit te laten voeren. Het is gebruikelijk dat toezicht op defensieopdrachten wordt gedaan door de toezichthouder van het land waar de opdracht wordt uitgevoerd. Als bijvoorbeeld de Duitse overheid een defensieorder plaatst bij een Nederlands bedrijf dan wordt, als de Duitse overheid dat wenst, het toezicht door Nederland uitgevoerd. De eerdergenoemde AQAP-2070 regelt de wijze waarop de landen onderling het toezicht kunnen uitbesteden. Ook is vastgelegd hoe het toezichtproces moet worden ingericht. Tevens is een uniforme wijze van communicatie tussen de verschillende nationale toezichtorganisaties afgesproken. Toezicht op Nederlandse contracten buiten het NATO-gebied worden door TDL zelf op locatie zelf uitgevoerd.

Hoe ziet de toekomst er uit?

Door de wereldwijde veranderingen en de langere inkoopketens gaan zaken als "maatschappelijk verantwoord ondernemen", "veiligheid en ARBO technische zaken", "counterfeit material" steeds meer meespelen. Deze worden onderkend en steeds vaker meegenomen in de toezichtactiviteiten. In de laatste versie van de AQAP-2110 is zelfs een paragraaf opgenomen (§ 3.3.12) die speciaal gaat over Counterfeit Material en de specifieke maatregelen die er genomen moeten worden door leveranciers. Daarnaast worden defensie systemen complexer en worden doorlooptijden korter waardoor het onderkennen van risico's ook steeds moeilijker wordt. Al deze veranderingen leiden er toe dat ook het defensie toezicht continue mee moet veranderen en dat toezichtprogramma's complexer zullen worden om alle nieuwe ontwikkelingen mee te nemen in de dagelijkse toezicht praktijk.



Harmen van Heek is sinds 1992 werkzaam bij de Defensie Materieel Organisatie afdeling Toezicht Defensie Leveranciers in verschillende functies. Zijn huidige functie is hoofd defensie toezicht vestiging Oost. De afdeling Toezicht Defensie Leveranciers is verantwoordelijk voor het defensie toezicht bij bedrijven die aan defensie opdrachten werken, nationaal en internationaal. Defensie toezicht vestiging Oost is verantwoordelijk voor het toezicht bij bedrijven in Noord Oost Nederland. De afgelopen jaren heeft hij zich intensief bezig gehouden met de overgang van productkeuring naar procesverificaties en heeft hij aan de wieg gestaan van de nieuwe toezicht aanpak "risico gebaseerd toezicht" terwijl recentelijk is gestart is met de invoering van HNW en lean/agile werken.

Waarom een Cyber- & Datarisksverzekering?

De vraag is niet of u slachtoffer wordt van cybercriminelen, maar wanneer… En wist u dat een gemiddelde hackaanval € 300.000 kost? En het forensisch onderzoek naar de hacker gemiddeld € 75.000?

Binnen een cyber- & datarisksverzekering zijn de volgende zaken verzekerbaar:

1. De financiële gevolgen van inbreuk in systemen of (elektronische) data. Denk hierbij aan de volgende kosten:
   - forensisch onderzoek;
   - advies en communicatie met bijvoorbeeld providers, klanten, toezichthouders, justitie, creditmaatschappijen;
   - de extra klantondersteuning, zoals inschakelen van een callcenter, crisismanagement, reputatieherstel;
   - herstel van websites, intranet, netwerk, computersysteem, programma's of elektronische data;
   - kredietbewaking en/of identiteitsbescherming van betrokken benadeelden.
2. Bedrijfsschade vanwege onderbreking of ernstige belemmering van de bedrijfsactiviteiten doordat een hacker of derde de toegang tot de computersystemen, website en machinepark elektronisch blokkeert.
3. Cyber afpersing: het onderzoek, de assistentie en het betaalde losgeld. Denk hierbij aan bijvoorbeeld WannaCry.
4. De opgelegde boetes in verband met het schenden van het recht op privacy of de privacy wetgeving en het schenden van de bedrijfsregels voor betaalkaarten.
5. Extra telecom kosten door toedoen van een hacker.
6. Cyberdiefstal van geld of geldswaarden. Denk hierbij aan de phising e-mails.
7. Cyberdiefstal van goederen.
8. Schade aan de voorraad als gevolg van veranderingen in temperatuur of vochtigheid, door gehackte regelapparatuur.
9. Bescherming als u aansprakelijk wordt gesteld door derden wanneer uw eigen e-mail, intranet, extranet of website schade toebrengt aan een ander.

Wellicht belangrijker nog… de pechhulp bij cyber

Los van de dekking neemt een crisismanager u bij de hand en begeleidt u door de stappen die u moet doorlopen bij een cybercalamiteit. Er worden specialisten ingeschakeld waar nodig. Denk hierbij aan advocaten en IT-specialisten. Ook zijn er verzekeraars die u preventief ondersteunen, door het onderzoeken van uw netwerk naar kwetsbaarheden.

Waar moet u qua premiehoogte aan denken?

Bij bijvoorbeeld een omzet tussen de € 5.000.000 en € 10.000.000 en een verzekerd bedrag van € 500.000 is er al een goede dekking te krijgen tegen een jaarpremie van € 2.050 (exclusief assurantiebelasting).

Thoma Assurantie- en Pensioenadviseurs

Stanley Dijkhuis

T 0573 222 906

M 06 53405868

E dijkhuis@thomagroep.nl

THOMA ASSURANTIE- EN PENSIOENADVISEURS

WWW.THOMAGROEP.NL

Risicobeheersing in de IT

Een compleet nieuw fenomeen in het kader van risicobeheersing is gelegen in de IT. Praktisch geen enkele organisatie kan zonder internet of informatietechnologie. Maar met het in gebruik nemen van deze technologie, wordt tevens een levensgroot nieuw risicogebied betreden. Wereldwijd gaat al veel meer geld om in cybercriminaliteit dan in drugs. Organisaties leren letterlijk door schade en schande. Ze ontdekken deze risico's vooral door ongelukken. Naast technische antwoorden zal het personeel steeds beter moeten worden getraind. Ook de overheid bemoeit zich steeds nadrukkelijker met het onderwerp en vaardigt regelmatig nieuwe richtlijnen en wetten uit. Aan het woord is Stanley Dijkhuis van Thoma Assurantieadviseurs.

Risico's verbonden aan het gebruik van computers zijn globaal als volgt in te delen:

1) Systemen of gegevens worden onbereikbaar (bijv. door DDoS-aanvallen)
2) Gegevens (of hele systemen) komen in ongewenste handen
3) Gegevens worden veranderd, onleesbaar of onbruikbaar gemaakt.

Omdat steeds meer besturingen van apparaten aan internet worden gekoppeld, ontstaat het risico dat onbevoegden deze apparaten ongewenste acties kunnen laten gaan uitvoeren. Met de transitie naar "Smart Industry" of "Industrie 4.0" wordt dit probleem nog prominenter. Immers na een hack kan dan een (groot) deel van de productie tot stilstand komen of beschadigd raken.

Voorbeelden

De creativiteit, gedrevenheid en beschikbare middelen van criminelen kent geen grenzen. Over "geen grenzen" gesproken, deze vorm van criminaliteit is internationaal in optima forma. Globaal zijn criminelen uit Rusland en de voormalige Oost-Europese landen vooral gericht op financiële doelgroepen. Denk hierbij aan ongewenste banktransacties om direct geldelijk gewin te behalen. Criminelen uit Azië, vooral Chinese, zijn meer geïnteresseerd in intellectuele eigendommen. En breken in om geheime Know how te ontfutselen. Daarnaast zijn waarschijnlijk veiligheidsdiensten druk bezig kwetsbaarheden te verzamelen om indien nodig toe te slaan.

DDoS

Bij DDoS-aanvallen worden servers door miljoenen dataverzoeken zodanig overweldigd dat reguliere gebruikers van de servers geen respons krijgen. Dit resulteert dan in onbereikbaarheid of vastlopen van websitepagina's. Op vrijdag 21 oktober 2016 werd er in verschillende delen van de Verenigde Staten melding gemaakt van grootschalige cyberaanvallen waardoor de websites van onder andere Reddit, Amazon, Airbnb, PayPal, Netflix, Twitter, Spotify en de New York Times crashten of urenlang onbereikbaar waren. De storingen werden veroorzaakt door een DDoS-aanval (Distributed Denial of Service) die gericht was op Internetinfrastructuurbedrijf Dyn1 dat kritieke IT-diensten levert aan grote bedrijven. Tijdens de aanvallen werden de directoryservers van Dyn verstoord.

Zie het themablad van 2009:

Een helder en actueel beeld van de risico's is een voorwaarde om effectieve en efficiënte beheersmaatregelen te treffen. Daarnaast moeten ondernemingen in toenemende mate aan investeerders en andere belanghebbenden aantonen dat zij op de juiste wijze omgaan met deze problematiek.

Definitie van risico:
Risico is de mogelijkheid dat een onzekere gebeurtenis of omstandigheid, met negatieve consequenties voor de doelstellingen van een bedrijf, zich zal voordoen.

Definitie van risicomanagement:
Risicomanagement is een systematisch en regelmatig onderzoek en omvat het identificeren, analyseren en evalueren van risico's met het doel zodanige maatregelen te treffen dat de vermogenspositie in voldoende mate beschermd wordt en tegelijkertijd gestreefd wordt naar het minimaliseren van de totale risicokosten.

Een DDos-aanval wordt in bitsnelheden gemeten, nl. Gigabits per seconde (Gbps). Een aanval kan 200 tot 300 Gbps zijn, maar nemen in grootte steeds meer toe. De grootste aanval tot nu toe oversteeg zelfs de 500 Gbps. Ging het eerder nog om vandalisme van "schooljongens", tegenwoordig worden op professionele manier grote bedrijven aangevallen. DDoS-aanvallen worden steeds vaker uitgevoerd om bedrijven af te persen.
Het bijzondere van bovengenoemde voorbeeld is dat voor het eerst duidelijk werd dat IoT (Internet of Things) hierin een rol speelde. Computers van op het net aangesloten camera's, printers, etc. van met name Chinese makelij, waren gehackt en misbruikt. Wachtwoorden waren vast geprogrammeerd of te simpel ingesteld. In tegenstelling tot gehuurde servers bij een provider zijn deze apparaten in het bezit van particulieren niet even snel van het internet te af te koppelen.

Diefstal

Bij diefstal van gegevens moet niet alleen gedacht worden aan gevoelige persoonsgegevens, zoals creditcard-gegevens, medische gegevens en, zoals hierboven vermeld, intellectueel eigendom. Met de komst van IoT (Internet of Things) kunnen robots, camera's, huiskamerthermostaten, printers, etc. overgenomen worden om beelden en geluiden af te luisteren. Diefstal is aan de orde van de dag en moet tegenwoordig bij de overheid worden gemeld. Diefstal van bijvoorbeeld bankgegevens kan tot een grote kostenpost leiden, bijv. de verplichte monitoring van een jaar van de bankaccounts van de slachtoffers om verdachte transacties vroegtijdig op te merken. De (semi)overheid komt zelf regelmatig in het nieuws: gemeenten, de netwerkbeheerder, ziekenhuizen, etc. Maar er is ook al melding gemaakt van een bekend TV-merk wiens smart-tv's een microfoon hebben die op afstand kan worden afgeluisterd. Er is ook al speelgoed ontdekt met de zelfde kwetsbaarheden.

Met een internet ww42.showdan.com een soort google voor IoT krijgt u een overzicht van alle gevonden (en slecht of niet beveiligde) internetcamera's.

Veranderen en overnemen van sites

Onlangs werden de twitter-accounts van bekende sites overgenomen via een derde partij die als dienst het twitter-verkeer van de bij hun aangesloten klanten in kaart bracht. Via de gehackte accounts werd een politieke boodschap de wereld ingestuurd. Misbruik was duidelijk en heeft wellicht alleen reputatieschade toegebracht aan deze accounts, maar de reputatieschade van de betreffende dienst is aanzienlijk groter.
De Amerikaanse regering, hoge ambtenaren en cyberspecialisten hebben Rusland er onlangs van beschuldigd cyberaanvallen te hebben uitgevoerd. Volgens hen zijn Russische inlichtingendiensten verantwoordelijk voor het hacken van Hillary Clintons e-mails met de bedoeling de presidentsverkiezingen te beïnvloeden. Gezien de "close victory" van de tegenpartij, zijn in dit voorbeeld de gevolgen voor de loop van de geschiedenis niet te overzien maar waarschijnlijk substantieel.
Een paar jaar terug hebben waarschijnlijk Amerikaanse en Israëlische specialisten samengewerkt aan een virus (Stuxnet) waarmee een nucleaire opwerkingsfabriek in Iran werd stilgelegd. Voor Iran moet de schade groot zijn geweest omdat de machines er zelfs door werden beschadigd.
Overgenomen servers worden vaak gebruikt voor het opzetten van de hierboven genoemde DDoS-aanvallen. De eigenaren hebben in het begin niets door. Eerst worden alle gehackte servers tot een botnet of zombieleger geformeerd om vervolgens met één commando alle servers tegelijk te laten aanvallen. Ontdekt de provider dat uw server wordt misbruikt, dan wordt deze direct uitgeschakeld en van het net afgehaald.
Particulieren en het MKB blijken vaak het slachtoffer van ransomware te zijn. Een verkeerd mailtje wordt net te laat herkend en het slachtoffer mag losgeld in de vorm van bitcoins betalen om zijn data weer ontsleuteld te krijgen.

Voorbeelden uit eigen praktijk

Als assurantiemakelaar is Stanley de afgelopen jaren met diverse schadeclaims geconfronteerd. Niet alle schades waren of konden worden gedekt.

1) Een klant ontving een mail van de KPN en opende de bijlage die een factuur zou zijn. Alle bestanden waren versleuteld en er werd losgeld in de vorm van bitcoins gevraagd. Van een dergelijk incident zijn de volgende schades (gedeeltelijk) verzekerbaar: forensisch onderzoek, kosten crisismanagement, PR-campagne voor reputatieherstel, het te betalen losgeld.
2) Een aanmaning van een bekende leverancier ontvangen en te betalen op een andere rekening. Banken doen geen naam-nummer-controle meer. Criminelen maken van deze gebrekkige controle dankbaar gebruik. Het betaalde bedrag is niet zondermeer verzekerbaar.
3) Een telefooncentrale was gehackt en belde eigenhandig in 2 dagen tijd voor meer dan € 25.000 euro aan 0900-nummers. Deze schade is niet standaard gedekt.
4) Van een medewerker van een ziekenhuis is de harde schijf uit zijn auto gestolen. De patiëntengegevens waren niet geanonimiseerd. Verzekerd waren: kosten van informeren van patiënten, claims van patiënten en de boete van de Autoriteit Persoonsgegevens.
5) Door middel van spyware is een transportsysteem gehackt waardoor de goederen afgeleverd werden bij de dief. Schades voor dergelijke diefstallen is maatwerk.
6) Op de kassa's van het Hilton is met malware de gegevens van creditcardhouders gestolen. Acties die moesten worden ondernomen waren: Forensisch onderzoek, slachtoffers informeren met callcen-

ters, crisismanagement, campagne voor reputatieherstel, herstellen IT-systemen, afhandelen van claims van klanten, kredietbewaking van slachtoffers. Bovendien ontving de organisatie een boete.

7) Een kraanbouwer ontdekt op een beurs dat zijn nieuwste ontwerp ook door een Aziatische concurrent wordt getoond. Na onderzoek bleek de data van hun computers te zijn gestolen. Bedrijfsschade door het wegvallen van orders is niet te verzekeren.
8) Bij een opdracht aan een bank was het complete SEPA-bestand aangepast om betalingen anders te laten verlopen dan dat de bedoeling was.

"Uit eigen ervaring blijken infecties van computers vooral te worden veroorzaakt door stagiaires, tijdelijke werknemers en managers en (bestuurders) van de oudere generatie." zegt Stanley

Aanpak

Uiteraard wordt met wisselend succes op de veroorzakers gejaagd. Maar omdat (veiligheidsdiensten van) overheden zelf aan beide kanten van de streep meedoen, is het dweilen met de kraan open. Eén van de reacties van criminelen is om de broncode van hun malware te verkopen of openbaar te maken zodat het gebruik door nog meer criminelen de oorspronkelijke bedenker maskeert. Een eenvoudige "single cause"-aanpak gaat helaas niet werken. QESH-managers die in hun dagelijkse praktijk met risico's worden geconfronteerd, hanteren ongeveer de volgende aanpak:
De algemene aanpak van risico's is:

1) het wegnemen van het risico (uitbesteden),
2) het gebruik van hulpmiddelen en beveiligingen,
3) het opstellen van organisatorische regels en voorschriften voor gedrag
4) het verzekeren van mogelijke schades.

Risico's op gebied van ICT zijn zo divers en complex dat maatregelen op al deze gebieden noodzakelijk zijn. Een voorbeeld van het wegnemen van risico's is door computersystemen los te koppelen van het internet, uitbesteding van de ICT of door helemaal geen computers te gebruiken als dat niet perse nodig is. (Denk bijv. aan het verbieden van smartphones op het werk). Uiteraard is het van computers juist de bedoeling om te communiceren met andere computers, bijv. voor onderhoud. Dan kan bijv. gekozen worden om alleen tijdelijk een verbinding toe te staan. Verder zullen systemen zo moeten worden ontworpen dat zij inherent veilig zijn. Inkopers van systemen moeten zich verdiepen in het hanteren van standaard programma van eisen met betrekking tot veiligheid zodat data-risk geen sluitpost is.

De volgende stap is het installeren van hulpmiddelen: virusscanners, scanners van netwerk verkeer, firewalls, etc. vormen de volgende verdedigingslinie. Inmiddels is een hele industrie van leveranciers op dit gebied ontstaan. De industrie zelf is vrij sceptisch over de ontwikkelingen. Zij suggereren, al dan niet met commerciële motieven, te vechten voor een verloren strijd. Oorspronkelijk bedoeld voor hardware failure zijn goede back ups het enige antwoord op bijv. ransomware.

Daarnaast blijkt in de meeste gevallen de gebruiker de zwakste schakel te zijn. O.a. het te makkelijk openen van phishing-mails, het verliezen van memory-sticks en het gebruik van te simpele wachtwoorden, zijn de moeilijkst uit te bannen risico. Voortdurend opleiden over informatieveiligheid (evt. via internet) en aandacht van het management is hier het cruciale antwoord.

Uit bovenstaande wordt snel duidelijk dat risico's zullen blijven bestaan. Mede daarom is de opkomst van de zogenaamde cyber & data-risk-verzekeringen zeker geen toeval.

Verder is het van cruciaal belang om in een zo vroeg mogelijk stadium, de ontwerpfase, het juiste programma van eisen op te stellen. Vaak is men blij als een complex ontwerp binnen de gestelde tijd überhaupt werkt, laat staan dat men direct begint met het stellen van (data)veiligheidseisen. Vaak verbetert men de veiligheid een aantal lifecycles later. ICT- en KAM- of QHES managers zullen overtuigingskracht moeten ontwikkelen om hogere managers tot meer investeringsruimte te bewegen voordat het spreekwoordelijke kalf is verdronken.

Maatregelen van de wetgever.

De wetgever richt zich op de bescherming van persoonsgegevens en privacy en beveiliging van cruciale maatschappelijke systemen (denk aan nutsvoorzieningen, defensie, stemcomputers, etc.)

Op 25 mei 2018 wordt de Nederlandse Wet bescherming persoonsgegevens vervangen door de Europese Algemene verordening gegevensbescherming. Hoewel belangrijke principes voor de verwerking van persoonsgegevens overeind blijven, verandert er toch het nodige. Nu moeten organisaties verwerkingen melden bij de Autoriteit Persoonsgegevens, straks moeten ze zelf meer gaan vastleggen welke verwerkingen zij doen en op welke gronden.

Overheidsinstanties, bedrijven die op grote schaal over persoonsgegevens beschikken (zoals verzekeraars, banken en gezondheidsinstellingen) en *profilers* moeten dan ook een functionaris voor de gegevensbescherming (FG) aanstellen die onafhankelijk onderzoek kan doen naar gegevensgebruik binnen de organisatie. Bij de ontwikkeling van een nieuw product moet met een Privacy Impact Assessment (PIA) worden vastgesteld wat voor impact het heeft op het gegevensgebruik.

Consumenten krijgen op grond van de nieuwe Europese privacywet meer rechten, waaronder het recht op dataportabiliteit. Dit betekent dat ze gegevens die ze hebben verstrekt aan een organisatie mogen opvragen en overdragen aan een andere organisatie. Verder krijgen consumenten het recht op vergetelheid. Ze kunnen, in bepaalde gevallen, organisaties verzoeken om hun persoonsgegevens zonder onredelijke vertraging te wissen. De nieuwe wetgeving levert voldoende vraagstukken op voor verzekeraars. Hoe ga je bijvoorbeeld om met het verzoek van een klant die zijn persoonsgegevens verwijderd wil hebben? Het Verbond gaat zijn leden bij de overgang ondersteunen. Zo werkt de brancheorganisatie onder meer aan een nieuwe gedragscode.

W. van der Zee
Redactiecommissie

Stanley Dijkhuis is zijn carrière begonnen als Risk Manager bij Wolters Kluwer. Na 12 jaar verruilde hij zijn eerste baan voor een baan in de assurantieen. Na diverse omzwervingen werkt hij de laatste 18 jaar als Commercieel technisch manager bij Thoma Assurantieadviseurs. In deze hoedanigheid heeft hij zijn vakgebied zien groeien door de nieuwe ICT-technologie. Door het gebruik van internet zijn de risico's voor bedrijven enorm toegenomen.

Colofon

Dagelijks bestuur
Henk-Jan Wegman Voorzitter
Eric van de Straat Penningmeester
Elize Hulscher Secretaris

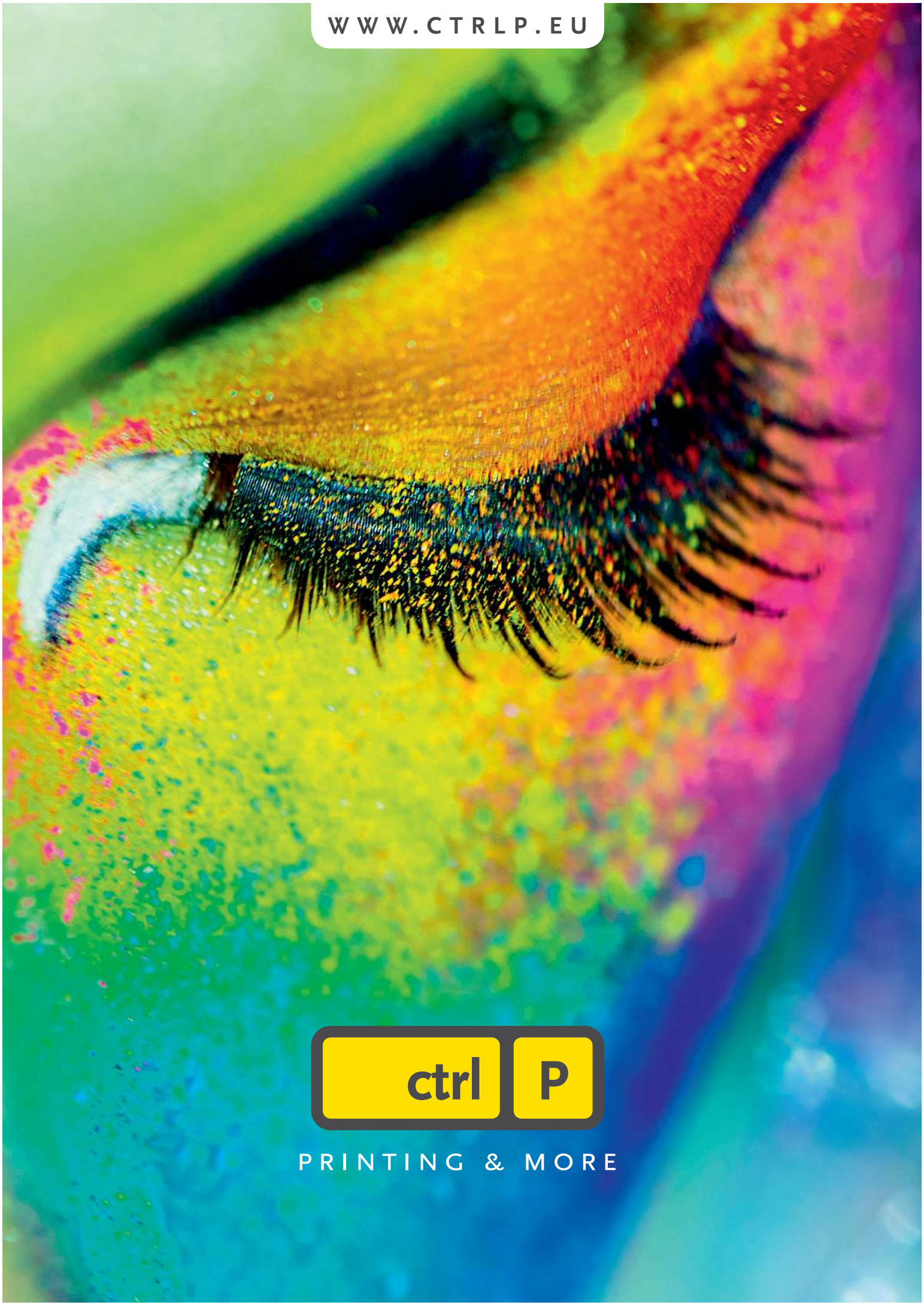
Commissie Opleidingen
Gerard Berendsen (voorzitter)
Patrick de Boer
Jieles van Daalen
Annemarie Denneboom
Rienco Ligtenbarg

Programmacommissie
Johan Zemansky (voorzitter)
Onno Coster
Jaap Hekkema
Rene ter Horst
Rick Nijhuis
Tim Steffens
Kristel Zonder

Redactiecommissie
Nicole Mak (voorzitter)
Sonja Hommels
Jelle Winia
Wouter van der Zee

Secretariaat
Oranda Krupers

Kwaliteitskring Twente
Postbus 8071
7550 KB Hengelo
Telefoon: 06 50850360
E-mail: kantoorkkt@kwaliteitskringtwente.nl
Linkedin: Kwaliteitskring Twente
Twitter: @KKTwente


WWW.CTRLP.EU
ctrl P
PRINTING & MORE