Princetonlaan 6
3584 CB Utrecht
Postbus 80015
3508 TA Utrecht

www.tno.nl

T +31 88 866 42 56
F +31 88 866 44 75

TNO-rapport

TNO 2016 R10096

Opkomende risico's voor arbeidsveiligheid als gevolg van IT-koppelingen van en tussen arbeidsmiddelen

Datum	19 januari 2016
Auteur(s)	Wouter Steijn; Johan van der Vorm; Eric Luijf; Raphäel Gallis; Dolf van der Beek (contactpersoon)
Exemplaarnummer	
Oplage	
Aantal pagina's	44 (incl. bijlagen)
Aantal bijlagen	1
Opdrachtgever	
Projectnaam	Opkomende risico's voor arbeidsveiligheid als gevolg van IT-koppelingen van en tussen arbeidsmiddelen
Projectnummer	060.17532

Inhoudsopgave

1 Inleiding

De toenemende integratie van nieuwe technologieën in arbeidsmiddelen wordt ook wel gezien als de vierde industriële revolutie[1] en naar verwezen als *smart industry*[2]. Denk hierbij aan automatisering door middel van embedded software, het op afstand bedienen van zwaar materiaal en de koppeling van arbeidsmiddelen aan lokale en publieke netwerken waaronder het internet (zie kader volgende pagina voor voorbeelden). Naast de mogelijkheden die deze ontwikkelingen met zich meebrengen voor de industrie, ontstaan ook nieuwe dreigingen. Denk bijvoorbeeld aan personeel dat tussen robots of automatisch rijdende vrachtwagens moet manoeuvreren of kwaadwillenden die van afstand computers en computernetwerken binnen kunnen dringen en daardoor processen kunnen verstoren of stilleggen. De focus in dit rapport ligt op de koppeling van arbeidsmiddelen en ”cyberspace” waaronder koppelingen met lokale en publieke netwerken zoals het internet.

Industrial Control Systems (ICS)[3] zijn in toenemende mate te vinden in cruciale bedrijfsprocessen[4]. ICS worden ook steeds vaker gekoppeld aan interne bedrijfsnetwerken en direct of indirect met publieke netwerken zoals het internet. ICT en ICS hebben daardoor een steeds belangrijkere rol in de aansturing en besturing van processen en arbeidsmiddelen in bedrijven en organisaties, en zelfs in de woonomgeving. Daarmee raakt cybersecurity direct aan arbeidsveiligheid. Het op orde hebben van de cybersecurity van deze systemen en netwerken is daarmee tevens noodzaak geworden voor arbeidsveiligheid.

1. Recente krantenkoppen benadrukken het risico: “*Nieuw lek onthuld: 13.656 bedrijven zijn 'eenvoudig' te hacken*” (2012) en “*Russen hacken westerse energiebedrijven*” (2014). Hierbij worden niet alleen individuen en bendes als daders zichtbaar maar groepen die namens of vanuit een staat opereren.

2. In 2010 was Royal Friesland Campina het slachtoffer van een gemodificeerd Conficker virus dat hun ICS verstoorde en een negen uur durend productieverlies opleverde. Het risico voor de kwaliteit van het afgeleverde product is onduidelijk gebleven.

3. In 2005 werd de ICS van een aantal olie- en gasplatformen op de Noordzee getroffen door de Zotob.E worm. Verwijdering van de worm was alleen mogelijk door extra personeel naar de platformen te vliegen. Onduidelijk is het safety-gerelateerde risico.

[1] De eerste industriële revolutie betrof gietijzer en de stoommachine, de tweede industriële revolutie betrof staal, elektriciteit, turbines, en de verbrandingsmotor, en de derde industriële revolutie betrof computers, communicatie, en globalisatie.
[2] Zie ook het initiatief op www.smartindustry.nl
[3] Onder ICS wordt hier het hele palet aan industriële automatisering verstaan waaronder SCADA (en RTUs’), EMS, IACS, DCS, PLC en hun specifieke protocollen en netwerken.
[4] Luiijf, H.A.M., & te Paske, B.J. (2015). *Cyber Security of Industrial Control Systems*: https://www.tno.nl/ics-security/; Luiijf, H.A.M. (2009). *Process Control Security in het Informatieknooppunt Cybercrime*, NICC.

4. In 2014 heeft een cyberaanval tot grote fysieke schade geleid in een ijzerproducerende fabriek in Duitsland. Het safety-gerelateerde risico is evident. [5]

5. Een tiener weet in Lodz, Polen twee trams op elkaar te laten botsen door manipulatie van wissels met een aantal gewonden tot gevolg. [6]

Cybercriminaliteit (waarbij de schade in termen van assets en informatie kan worden geuit) is echter niet het enige risico dat de vierde industriële revolutie met zich meeneemt. Bij de integratie van ICT en arbeidsmiddelen ontstaan zowel emerging risks (i.e., "*Black Swans*"[7] of onbekende onbekende risico's[8]), als emergent risks (i.e., al bekende risico's die op een onverwachte manier veranderen en met onverwachte consequenties). Sommige van deze risicofactoren zullen ook een directe invloed hebben op de arbeidsveiligheid van de werknemers die werken met deze middelen. Denk hierbij bijvoorbeeld aan de toename en complexiteit van embedded software wat tot nieuw en onvoorspelbaar gedrag van de technologie (met effecten in de fysieke wereld) kan leiden en het van buiten het bedrijf af kunnen beïnvloeden van ICS door cyberaanvallen (malware of hacking) en daarmee de besturing van een of meer machines ongeautoriseerd beïnvloeden.

Uit een snelle inventarisatie door TNO blijkt dat deze problematiek internationaal nog voornamelijk "terra nova" is. Ook het Nederlands bedrijfsleven is, ondanks enkele inhaalslagen, slecht voorbereid op deze ontwikkelingen. Vandaar dat het Ministerie van SZW in 2015 de volgende kennisvraag aan TNO gesteld: *Voor het domein arbeidsveiligheid, waar bestaan de risico's op de genoemde gebieden en welke beheersmaatregelen (vooral technische) zijn denkbaar om de genoemde risico's te beheersen?*

TNO zal zich binnen het kader van deze kennisvraag vooral richten op de risico's voor arbeidsveiligheid ten gevolge van de koppeling van en tussen arbeidsmiddelen met (telecommunicatie-)netwerken waaronder het internet. Cybersecurity is op het moment zowel in de privésfeer, de private- en de publieke sector een belangrijk onderdeel van de maatschappelijk discussie. Toch wordt de discussie vooralsnog hoofdzakelijk gevoerd vanuit het oogpunt van de cyber security van assets en informatie. Het effect van falende cybersecurity bij de ICS van risicovolle bedrijfsprocessen op arbeidsveiligheid is nog grotendeels onbelicht. De voorbeelden in het kader laten zien dat het internet en telecommunicatie in combinatie met ICS al in veel vormen en manieren worden toegepast binnen de industrie.

---

[5] BSI (2014), Cyberattack on a German iron plant, Bonn, Germany. Online: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2014.pdf

[6] John Leyden (2008), "Polish teen derails tram after hacking train network: Turns city network into a Hornby set", The Register, UK. Online: www.theregister.co.uk/2008/01/11/tram_hack

[7] Taleb, N.N. (2007). *The Black Swan: The Impact of the Highly Improbable.* Random House

[8] To quote Donald Rumsfeld (2002): "There are known knowns. These are things we know that we know. There are known unknowns. That is to say, there are things that we know we don't know. But there are also unknown unknowns. There are things we don't know we don't know."

TNO zal hieronder een eerste stap zetten in het beantwoorden van de kennisvraag door middel van het uitvoeren van een inventarisatie van gevaren en bedreigingen en het in kaart brengen van maatregelen ter voorkoming aan de bron of mitigatie van het risico. Hierbij richten wij ons specifiek op de maatschappelijke ontwikkelingen omtrent de toenemende koppeling van en tussen arbeidsmiddelen via het internet of telecommunicatie. De doelstelling binnen dit project wordt daarom als volgt samengevat in de volgende onderzoeksvraag:

Welke beheersmaatregelen kunnen worden aangedragen om de kwetsbaarheden voor emerging en emergent risks met betrekking tot arbeidsveiligheid die veroorzaakt worden door de koppeling van en tussen arbeidsmiddelen via het internet of telecommunicatie te minimaliseren?

Met het oog op het in dit onderzoek samenlopen van security- en arbeidsveiligheidsaspecten van arbeidsmiddelen en de systemen waar zij deel van uit maken, zal waar nodig het begrip bedreiging en kwetsbaarheid worden geïntroduceerd. Dit om te benadrukken dat we ook het concept gewilde onveiligheid en kwetsbaarheid van de gevolgen daarvan te benoemen.

In dit rapport presenteren wij de gevolgde methodiek om deze kennisvraag te beantwoorden en het resulterende overzicht van kwetsbaarheden en beheersmaatregelen. In hoofdstuk 2 geven wij uitleg over de gebruikte methodologie: interviews en een workshop met experts vanuit verschillende domeinen. In hoofdstuk 3 presenteren wij de resultaten van de interviews en in hoofdstuk 4 de resultaten van de workshop. In hoofdstuk 5 geven wij vervolgens een korte discussie van de belangrijkste resultaten opgenomen met een aanvulling vanuit de expertise van TNO. In hoofdstuk 6 presenteren wij tot slot de uiteindelijke inventarisatie van kwetsbaarheden en beheersmaatregelen voor bedrijven in de vorm van een kenniskaart.

1.
Kader

De vierde industriële revolutie kenmerkt zich door de integratie van nieuwe technologieën en arbeidsmiddelen. Hieronder vind u enkele voorbeelden.

2.
De koppeling van en tussen arbeidsmiddelen met het internet

Dankzij het internet staan in het dagelijks leven steeds meer apparaten onderling in verbinding, denk hierbij aan computers, mobiele telefoons en de televisie. Ook in de industrie ontstaat er een internet of things (IoT) waarbij installaties en machines met elkaar in verbinding worden gebracht. Dit ter bevordering van machine-to-machine communicatie bij langere en complexe processen, maar ook om het mogelijk te maken om op afstand installaties te bedienen. Denk bij dit laatste bijvoorbeeld aan het op afstand kunnen monitoren van een offshore windmolenpark. Deze toename van interconnectiviteit door middel van publieke netwerken zoals het internet brengt echter ook nieuw risico met zich mee, zoals cybercrime, cyberactivisme en ultiem de dreiging van cyberconflicten, en de noodzaak voor industrieën om hun infrastructuur hier tegen te wapenen*.

Figuur 1. Offshore windmolenpark

Op afstand bedienen van arbeidsmiddelen

Draadloze bediening van arbeidsmiddelen stelt arbeiders steeds vaker in staat om op afstand arbeidsmiddelen te bedienen tijdens gevaarlijke handelingen of op gevaarlijke locaties. Tegelijkertijd brengt het ook weer nieuwe kwetsbaarheden met zich mee omtrent de arbeidsveiligheid. Een draadloos signaal kan haperen of verstoord worden wat kan leiden tot ongecontroleerd gedrag van een voertuig of machinerie. Of de arbeider kan zich in het pad van het voertuig of onveilig werkingsgebied van een machinerie bevinden. Verder is het risico denkbaar dat de controle over het te besturen arbeidsmiddel wordt overgenomen door een hacker of risicovol wordt beïnvloedt door malware of iemand die ongeautoriseerd met deze technologie aan het “spelen” is.

Figuur 2. Op afstand bestuurbare wals ‘Fikkie’.

3.
Embedded software in arbeidsmiddelen

Embedded software refereert naar de integratie van software in een machine om deze ‘intelligenter’ gedrag te laten uitvoeren. Voorbeelden in de auto-industrie zijn bijvoorbeeld het ABS dat automatisch het remmen ondersteunt, of climate control dat automatisch de temperatuur in de auto regelt. Automatisering lijkt het sleutelwoord te zijn. Een belangrijke toepassing van embedded software is om machines zo kosteneffectief mogelijk zelfstandig (i.e., automatisch) bepaalde handelingen te laten uitvoeren. Denk hierbij bijvoorbeeld ook zelfrijdende transportwagens die de containers verplaatsen in de APM-terminal op Maasvlakte-2. Men kan zich afvragen welke risico’s die meebrengt voor arbeiders die ter plekke moeten werken. Ook hier is er het risico dat een hacker het script van een zelfrijdende transportwagen kan aanpassen of dat malware zorgt voor gevaarlijke voertuig- of kraanbewegingen.

Figuur 3. Geautomatiseerde transportwagen op de APM-terminal Maasvlakte 2

* Hier is al aandacht voor zo blijkt ook uit een toezegging van het Havenbedrijf Rotterdam om de strijd aan te gaan tegen cybercrime (http://www.distriparkbotlek.nl/?EventID=2).

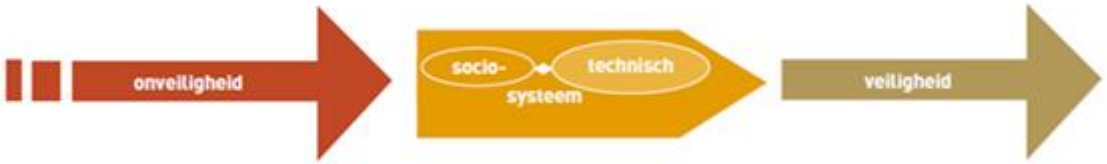
4.

2 Methode

Om de onderzoeksvraag te kunnen beantwoorden, moet er een inventarisatie van risico's en kwetsbaarheden worden gemaakt, en mogelijke beheersmaatregelen in kaart worden gebracht. Hierbij richten wij ons op een integrale aanpak met zowel safety als security elementen op beheersmaatregelen tegen ongeautoriseerde beheersing van arbeidsmiddelen met name door cybercriminaliteit (d.w.z. criminaliteit met ICT als middel en doelwit binnen de industrie). Wij richten ons daarbij in het bijzonder op de risico's en kwetsbaarheden met betrekking tot arbeidsveiligheid die ontstaan in relatie tot het gebruik en onderhoud van de koppeling van en tussen arbeidsmiddelen via lokale en publieke netwerken waaronder het internet te minimaliseren. Deze focus en onderzoeksvraag in acht genomen, is het volgende werkplan opgesteld:

1) Via een korte internet en literatuurscan wordt een framework ontwikkeld waarbinnen de relevante risico's, kwetsbaarheden en beheersmaatregelen kunnen worden beschreven. Tevens voorbereiding op stap 2.
2) Interviews worden gehouden met experts op gebied van veiligheid. Een actoranalyse van relevante partijen voor deze interviews zal worden gedaan op basis van het framework dat in stap 1 is bepaald. Tevens voorbereiding op stap 3.
3) Een workshop zal worden georganiseerd waarbij de resultaten uit de interviews worden teruggekoppeld aan experts uit de praktijk, en deze resultaten verder worden aangevuld.

Gelet op het samenlopen van het arbeidsveiligheids- en (cyber)security aspect van de veiligheid van machines en arbeidsmiddelen is een gezamenlijk begrippenkader nodig. Uitgangspunt is dat we het samenspel van mens en machine, gevaar en dreiging beschouwen als een socio-technisch systeem (zie figuur 1).



Figuur 1. Veiligheid als een socio-technisch systeem.[9]

Om de mate van veiligheid te kunnen benoemen is naast het traditionele risicobegrip als de kans dat een potentieel gevaar resulteert in een daadwerkelijk incident en de ernst van het letsel of de schade die dit tot gevolg heeft[10], ook het begrip dreiging en kwetsbaarheid nodig.

[9] VROM (2008). *Handreiking Security Management*.
[10] Wikipedia: https://nl.wikipedia.org/wiki/Risico (23-12-2015)

In het vervolg van dit rapport hanteren wij daarom de volgende definities voor de gehanteerde concepten. Voor risico hanteren wij de traditionele definitie zoals hierboven

beschreven, behalve dan dat we gevaar met dreiging vervangen en kwetsbaarheden toevoegen als beïnvloeder van de kans dat een dreiging daadwerkelijk tot een incident leidt. Dreiging definiëren we hier in lijn met de definitie van de Privacycommissie[11] als "*elke onverwachte of onverhoopte gebeurtenis die aan een onderneming schade kan toebrengen*". Het omvat dus de gewilde en ongewilde mogelijkheid om bedrijfsprocessen zodanig te beïnvloeden dat schade en of letsel wordt veroorzaakt. Anders dan gevaar omvat het begrip dreiging ook het gewild toebrengen van schade en/of letsel. Kwetsbaarheid kan in lijn daarmee worden gedefinieerd als een zwakte (binnen een organisatie of andere entiteit) die kan worden benut door een dreiging[12].

Het komen tot deze begrippen lijst is een dynamisch proces geweest tijdens dit project. Vandaar dat deze begrippen niet geheel eenduidig worden gebruikt bij de besproken interview en workshop-resultaten. Met dreiging wordt in dit kader vooral de gewilde onveiligheid benoemd als aanvulling op het concept arbeidsrisico's dat vooral uitgaat van ongewilde onveiligheid.

2.1 Literatuur- en internetscan

Allereerst hebben wij een korte literatuur- en internetscan uitgevoerd. Het doel van deze scan was tweeledig. Ten eerste wilden wij een framework vinden op basis waarvan wij de dreigingen, kwetsbaarheden, en de beheersmaatregelen konden benaderen en betekenisvol categoriseren. Ten tweede wilden wij een overzicht creëren van relevante partijen die interessant zouden zijn om te betrekken bij de interviews.

Uit deze scan kwamen de arbeidshygiënische strategie en de levenscyclus van een arbeidsmiddel als bruikbare frameworks naar voren om in het bijzonder de beheersmaatregelen te categoriseren. Op basis van deze frameworks kunnen wij een gestructureerd hiërarchisch onderscheid maken in welke beheersmaatregelen de voorkeur zouden moeten hebben. Ook kan men daarmee aangeven waar in de levenscyclus en door welke partijen, de beheersmaatregel moet worden toegepast. Hieronder zullen beide frameworks kort worden toegelicht. Vervolgens laten wij zien hoe wij op basis van de levenscyclus tot een actoranalyse zijn gekomen om relevante partijen te betrekken bij de interviews.

2.1.1 Arbeidshygiënische strategie

De arbeidshygiënische strategie[13] maakt gebruik van de volgende hiërarchie aan mogelijke beheersmaatregelen zoals beschreven in de Arbowet[14]:

[11] Lexicon van de Commissie voor de bescherming van de persoonlijke levenssfeer (CBPL): https://www.privacycommission.be/nl/lexicon#letter_d
[12] Hafkamp, W.H.M. (2008). Als alle informatie telt: een onderzoek naar kwetsbaarheden- en incidentenresponse bij ICT-organisaties. PhD dissertatie, Universiteit van Amsterdam: http://dare.uva.nl/document/2/54173
[13] Arboportaal: http://www.arboportaal.nl/onderwerpen/arbeidshygienische-strategie

- Bronmaatregelen (o.a., elimineren en isoleren van gevaar).
- Collectieve maatregelen (o.a., afschermen van een groep van gevaar).
- Individuele maatregelen.
- Persoonlijke beschermingsmiddelen.

Volgens de arbeidshygiënische strategie moet deze hiërarchie nadrukkelijk gevolgd worden bij het toepassen van beheersmaatregelen. Dat wil zeggen, een organisatie moet beginnen met bronmaatregelen en wordt geacht pas als laatste oplossing persoonlijke beschermingsmiddelen te gebruiken. De arbeidshygiënische strategie moedigt echter ook aan om meerdere maatregelen van verschillende niveaus te combineren (het redelijkerwijs-principe).

Gelet op de complexiteit van de safety-security problematiek en de noodzaak deze meer vanuit een systeem- of ketenperspectief op te lossen, is de ontwerp- en ontwikkelfase van producten en installaties de aangewezen fase om tot een optimale oplossing te komen. Denk daarbij aan een systeemperspectief: het geheel van netwerken van alle onderdelen en relaties van personen, machines, computers, logische koppelingen en communicatiemiddelen. Hoewel paradoxaal in de context van arbeidsveiligheid is vanuit security perspectief ook het weren van personen een bronmaatregel.

Voor het versterken van de arbeidsveiligheid dient dan ook de hele levenscyclus van een product of installatie te worden meegenomen en het afvoeren van overtollige/afgeschreven producten niet te worden genegeerd.

2.1.2 Levenscyclus

Emerging risks zijn al bekende risico's die zich op een onverwachte manier manifesteren met onverwachte consequenties, en emergent risks zijn de onbekende onbekende risico's (i.e., de black swans). Hier zullen wij de mogelijk nieuwe risico's benaderen vanuit het perspectief van de levenscyclus van de arbeidsmiddelen. Deze benadering houdt in dat we de toepassingen van arbeidsmiddelen benaderen van: a) ontwerp/engineering, b) productie/leverantie/installatie, c) gebruik, d) onderhoud, e) vernieuwing, tot en met f) afvoeren. Voor cybersecurity worden vergelijkbare fasen in de gehele cyber security levenscyclus onderkend: a) ontwerp en ontwikkeling, b) installatie, systeemintegratie, in gebruik name, c) gebruik, d) onderhoud, e) upgrade, en f) afvoer.

2.1.3 Actoranalyse

Om tot een overzicht van dreigingen, en beheersmaatregelen te komen voor deze levensfasen, zullen experts worden benaderd die elk in één of meer fases expertise hebben. Hierbij kan worden gedacht aan ontwerpbureaus, producenten, onderhoudsbedrijven, en de industrie zelf. Daarnaast identificeren wij een drietal partijen die een invloed kunnen hebben op ieder onderdeel van de levensfase:

1) Kennisontwikkelaars; bijv. universiteiten en andere kennisinstellingen.

[14] Arbeidsomstandighedenwet, on-line: http://wetten.overheid.nl/BWBR0010346

2) Beleidsontwikkelaars & toezichthouders; bijv., Inspectiediensten of certificeerders.
3) Dienstverleners; bijv. verzekeraars of telecomproviders.

Tabel 1. Actoranalyse op basis van de levenscyclus van arbeidsmiddelen

	Organisatie		**Organisatie**
Levenscyclus arbeidsmiddel		**Beleidsontwikkelaars & Toezicht**	
Ontwerp	Triodor	Overheid	Beleidsafdeling SZW
	Total productivity		Inspectie ISZW
Productie/leverantie/installatie	Alewijnse		SODM
	Croon		DCMR
Gebruik	APM-terminal Maasvlakte 2		HSE
	ENECO (offshore windmolenpark)	Certificeerders	Lloyds
	FloraHolland Aalsmeer		Aboma
	Smart welding factory		TUV
	Scania		DNV
	VDL		
	BMP8500 (Fikkie)		
	Havenbedrijf Rotterdam		
	Tatasteel		
Onderhoud	Stork		
	Alewijnse		
	Kone Cranes		
	Cofely		
Vernieuwing	-		
Afvoeren	-		
Kennis ontwikkelaars		**Dienstverleners**	
Universiteiten	TU Delft Safety & Security Science section	Verzekeraars	Van Lanschot Chabot
	Radboud Universiteit		Verbond van Verzekeraars
	TILT Tilburg University		
Normalisator	NEN	Deskundigen	NVVK
Kennisinstituten	Smart Industry	Adviseurs	Fox-IT
	Rathenau instituut		PSJ Advies
	CIO Platform Nederland		Tebodin
	TNO	Telecomproviders	KPN

2.2 Interviews

Op basis van bovenstaande lijst (tabel 1) zijn 64 experts van verschillende organisaties benaderd om deel te nemen aan een interview. Uiteindelijk hebben dertien experts meegedaan, zie tabel 2

De interviews vonden plaats tussen 10 en 24 november 2015. De interviews duurde circa 45 minuten en zijn telefonisch afgenomen door twee TNO'ers, waarbij de taak van het interview afnemen en het notuleren verdeeld werden. De interviews waren semi-gestructureerd. De onderstaande vragen vormden de leidraad voor de gesprekken:

- Bent u met het onderwerp bekend? Welke toepassingen kent u/ werkt u mee? Denk aan assemblage lijnen, geautomatiseerde machines zelf of hun besturingssystemen.
- Wat is uw mening over de groeiende integratie van arbeidsmiddelen met het internet en de risico's die daarmee gepaard gaan?
- Wat zijn belangrijke ontwikkelingen m.b.t. dit onderwerp in uw werkveld?
- Welke (nieuwe en bestaande) risico's ziet u voor arbeidsveiligheid als gevolg van de nieuwe technologieën? Welke ziet u als belangrijkste?
  Graag vraag ik u te denken in a. dreigingen en gevaren en vervolgens b. kwetsbaarheden.
- Welke beheersmaatregelen zijn er om deze risico's te beperken?
- Wie zijn de belangrijkste actoren binnen bedrijven en hun leveranciers die daarop invloed hebben?
- Ziet u een rol weggelegd voor de wet- en regelgever? Voor een toezichthouder?
- Waar kunnen nog belangrijke stappen naar oplossingen worden gezet?
- Heeft/kent u (congres)verslagen en/of rapporten m.b.t. dit onderwerp die u met ons wilt delen? Idem voor papers, artikelen en presentaties.
- Kent u mensen die ook een waardevolle inbreng kunnen hebben in het kader van ons onderzoek?
- Dit is een eerste verkennend gesprek geweest. Zouden wij op een later tijdstip eventueel nogmaals contact mogen opnemen voor verdere verdieping? We denken aan alle geïnterviewden een preview op ons rapport te geven en daarop uw reactie te vragen.

Tabel 2. Deelnemers aan de interviews.

Interview	Organisatie	Type
1	Croon Elektrotechniek	Productie/leverantie/installatie
2	Cofely West Industrie	Onderhoud
3	Tebodin	Adviseurs
4	TNO Industrie/www.smartindustrie.nl	Kennisinstituut
5	TNO Industrie/www.smartindustrie.nl	Kennisinstituut
6	Alewijnse Industrial Automation	Productie/leverantie/installatie
7	PSJ Advies	Adviseurs
8	Tilburg Universiteit	Universiteit
9	VDL Steelweld	Gebruik
10	Total Productivity	Ontwerp
11	Academy The Hague (CSA)	Universiteit
12	TNO Information Security	Kennisinstituut
13	CIO Platform Nederland	Kennisinstituut

2.3 Workshop

Op 2 december 2015 is een workshop "*Cyberspace verbindt Safety en Security: ook uw uitdaging! Wat is nodig om de arbeidsveiligheid van morgen aan te pakken*?" gehouden. Geïnterviewden werden direct aan het eind van het interview uitgenodigd en verder is een uitnodiging verstuurd naar dezelfde actorenlijst die gebruikt is voor de interviews. Dit resulteerde uiteindelijk in vijftien deelnemers waarvan vijf projectleden en tien externe deelnemers waarvan 2 geïnterviewden.

Tabel 3. Externe deelnemers aan de workshop.

Organisatie	**Type**
Mercon	Productie/leverantie/installatie
Croon	Productie/leverantie/installatie
Researcher/Specialist Public Safety	Universiteit
TNO Information Services	Kennisinstituut
EXIV	Ontwerp
NEN	Normalisator
Prorail	Gebruik
TNO Information Security	Kennisinstituut
Tebodin	Adviseurs
SZW	Overheid

Het doel van de workshop was om een korte terugkoppeling van de interviewresultaten te geven, om vervolgens de lijst met risico's, kwetsbaarheden en beheersmaatregelen verder uit te werken. Hiervoor werd de groep in tweeën gesplitst die vervolgens in twee parallelle sessies van een half uur brainstormden over ofwel de risico's en kwetsbaarheden, ofwel de beheersmaatregelen. Na een half uur wisselden de groepen van onderwerp voor een 2^{e} ronde van een half uur. Tijdens de sessies werden de deelnemers een kader gepresenteerd waar zij post-its met hun ideeën op konden plakken.

3 Interviewresultaten

Hieronder geven wij een samenvatting van de bevindingen die uit de gehouden interviews naar voren zijn gekomen. Globaal zijn de resultaten in twee onderwerpen verdeeld: kwetsbaarheden voor de dreiging, en de beheersmaatregelen. Onderstaande resultaten zijn allemaal geparafraseerde uitspraken die direct uit de interviews komen. Aanvullingen vanuit TNO zijn expliciet aangegeven met behulp van een voetnoot.

3.1 Risico en kwetsbaarheden

In de interviews is er met actoren van verschillende disciplines gesproken over de nieuwe risico's als gevolg van de koppeling van en tussen arbeidsmiddelen met het internet of met behulp van andere vormen van telecommunicatie, zoals telemetrie en radiografische besturing. Verschillende voorbeelden worden aangedragen zoals de recente 'stuxnet' aanval in 2010 op een Iraanse uraniumverrijkingsfabrieken en het gebruik van crypto-virussen, hackware en stoorzenders om systemen te verstoren of onbruikbaar te maken. Alle voorbeelden zijn echter te herleiden tot één duidelijke thematiek: *De mogelijkheid dat een of meerdere individuen ongeautoriseerde toegang krijgen tot bedrijfssystemen in de arbeidsomgeving en deze dusdanig verstoren dat er (potentieel) een arbeidsonveilige situatie optreedt.*

Door de geïnterviewden wordt dit risico voornamelijk gezien als een bijeffect van de focus van bedrijven die nog voornamelijk op de mogelijkheden en het gebruiksgemak van nieuwe technologische ontwikkelingen ligt. Het past zogezegd in de huidige tijdsgeest en de toenemende bruikbaarheid van nieuwe communicatie- en machinetechnologie. Zo willen managers of medewerkers bijvoorbeeld van huis uit of onderweg processen kunnen bekijken. Leveranciers (denk aan onderhoudsservices) willen er van buiten bij kunnen om onderhoud te plegen of storingen uit te lezen en deze op te lossen om zo de 'time-to-fix' te minimaliseren. Ter gedachtebepaling wordt als voorbeeld ook de autonome auto gegeven. De discussie rondom de zelfrijdende auto is vaak gericht op de mogelijkheden en de beperkingen in de technologie die nog moeten worden opgelost. Intussen komen wel berichten in de media naar voren dat onbevoegden zich toegang weten te verwerven tot de software van auto's [15].

Met andere woorden, het risico vanuit het oogpunt van cybersecurity lijkt in de context van de levenscyclus van producten vaak alleen een gedachte achteraf te zijn in dit soort veiligheidsdiscussies, in plaats van dat ze vanaf het begin van het innovatie- of design proces worden opgenomen.

[15] Tweakers (21 juni, 2015). '*Hackers kunnen op afstand remmen uitschakelen op Chrysler-auto's.'* http://tweakers.net/nieuws/104341/hackers-kunnen-op-afstand-remmen-uitschakelen-op-chrysler-autos.html

Tabel 4. Overzicht van de kwetsbaarheden die in de interviews genoemd zijn. Met een korte samenvatting van belangrijkste elementen die uit de interviews naar voren komen.

Kwetsbaarheid	**Samenvatting**
3.1.1 Snelle technologische ontwikkelingen	De technologische ontwikkelingen van wat mogelijk is zorgen ervoor dat de software en beveiliging van arbeidsmiddelen snel verouderd. Eveneens neemt met de technologische mogelijkheden de complexiteit van systeemprocessen toe.
3.1.2 De “afstand” tussen de IT-afdeling en overige afdelingen die functioneel verantwoordelijk zijn voor arbeidsmiddelen (waar in toenemende mate ICT verstopt zit)	De IT afdeling is vaak nog een gescheiden wereld van de overige afdelingen waaronder die waar ICS wordt ingezet. Hierdoor wordt er nog geen integraal risicomanagement uitgevoerd waarbij rekening wordt gehouden met elkaars werelden.
3.1.3 Kosten cybersecurity	De huidige concurrentiemarkt zorgt ervoor dat met name kleine bedrijven niet willen investeren in cybersecurity en in plaats daarvan focussen op functionaliteit. Onderliggende factor hierbij is dat er nog maar weinig (publiekelijk bekende) grote incidenten zijn geweest.
3.1.4 Weinig besef over welke impact van security/safety dreiging eigenlijk mogelijk is	De cybersituational awareness en de kennis over wat hackers kunnen en wat hackers willen, is nog betrekkelijk laag bij de meeste organisaties. Een onderliggende factor hierbij is dat er schroom is om incidenten te melden (en er zo vervolgens van te kunnen leren als maatschappij).
3.1.5 Onbewust onbekwamen	Zelfs als security technologisch gezien goed geregeld is. Kan deze door onbewust onbekwame handelingen van medewerkers alsnog teniet worden gedaan, waardoor systemen kwetsbaar blijven. Huidige risicoanalyses nemen dit risico vaak niet mee en gaan uit van de juiste intentie in handelen van hun medewerkers.

De geïnterviewden geven aan dat ze enerzijds wel begrijpen waarom er door organisaties gebruik wordt gemaakt van nieuwe technologische middelen, maar vinden het anderzijds schokkend dat diezelfde organisaties relatief weinig aandacht aan het inherente risico wordt gegeven en veiligheid te weinig vanuit systeemperspectief wordt beoordeeld. Dit temeer omdat er meerdere factoren en actoren worden geïdentificeerd die het risico vergroten. Op basis van de interviews hebben wij een vijftal categorieën geïdentificeerd van de factoren die de kwetsbaarheid voor het risico van ongeautoriseerde toegang tot ICS en ICT-netwerken in de arbeidsomgeving vergroten. In Tabel 4 is een samenvatting van de resultaten opgenomen. Hieronder bespreken wij deze categorieën in willekeurige volgorde waarbij het eveneens duidelijk wordt dat er ook overlap en interacties tussen de factoren zijn.

3.1.1 Snelle technologische ontwikkelingen

Een vaak gehoord cliché is dat tegenwoordig de moderne technologische ontwikkelingen razendsnel gaan. Daartegenover staat dat binnen de industrie bepaalde arbeidsmiddelen maar zelden worden vervangen. Het besef lijkt er niet altijd te zijn hoe snel veiligheids- en ICT-systemen en ICS kunnen verouderen waardoor men weer blootgesteld is aan nieuwe dreigingen van buitenaf. Zo worden er voorbeelden aangehaald van installaties die nog op MSDOS lopen met

inbelsystemen waarbij men alleen al onbewust operationele processen om zeep kan helpen.
Hierbij lijkt de verantwoordelijkheid bij de beheerder en gebruiker van de arbeidsmiddelen te worden neergelegd. Leveranciers en installateurs geven aan dat ze veilige en up-to-date installaties en software aanleveren, maar dat het vervolgens bij de afnemer ligt om deze systemen up-to-date te houden. Een belangrijke onderliggende reden waarom het niet altijd voor de hand ligt dat installaties up-to-date wordt gehouden is de complexiteit van het updaten van installaties van kritische processen die 24/7 moeten draaien[16] (zie ook factor 3.1.2).
Verder zorgen de technologische mogelijkheden ervoor dat de complexiteit van de systeemprocessen toeneemt. Aangegeven wordt dat hierdoor niemand meer het overzicht heeft over het totale systeem, en er steeds meer een situatie ontstaat waarbij processen een 'black box' worden. Ook de verantwoordelijkheid voor veiligheid en beveiliging wordt daarbij diffuus. De vraag wordt opgeworpen hoe we diegene die beslissingen over deze 'black box' moeten nemen kunnen helpen. Hierbij wordt nog vaak in oude paradigma's gedacht, die echter niet meer van toepassing zijn voor de huidige situatie.
Echter, de technologische ontwikkelingen creëren ook nieuwe dreigingen. Bij een gebouw kan redelijk worden ingeschat welke externe factoren een invloed hebben op de fysieke staat van het beton, deuren en ramen. Deze zijn factoren redelijk constant: de kans dat er morgen opeens een nieuw soort betonvretende neerslag valt is nihil. Daarentegen kunnen er wel nieuwe ICT-functies (aanvallen) worden ontwikkeld waardoor bestaande veiligheidsfuncties niet meer adequaat zijn.

3.1.2 De "afstand" tussen de ICT-afdeling en overige afdelingen die verantwoordelijk zijn voor arbeidsmiddelen (waar in toenemende mate ICT verstopt zit)

Regelmatig wordt er verwezen naar de afstand tussen de ICT-afdeling en de werkvloer enerzijds en het topmanagement anderzijds. Zo wordt cybersecurity vanuit het topmanagement puur als een technisch probleem gezien dat ze niet snappen, terwijl de ICT-techneut er uiteindelijk vooral op gericht is om alles zo te installeren dat het werkt. Hierdoor ontstaat mogelijk suboptimalisatie en onterecht vertrouwen dat het met het systeem als geheel goed gaat en worden verantwoordelijkheden impliciet op elkaar afgeschoven.
Er is echter geen integratie van de processen en weinig kennis over elkaars domein (bijv. tussen ICT- en werkvloer-domein of tussen het safety en security domein). Zo wordt er over het algemeen binnen het ICT-domein in bedrijven en organisaties, mede onder druk van accountantscontroles en zichtbaar risico, veel waarde aan cybersecurity gehecht. Binnen bedrijven en organisaties leeft wellicht het besef er misschien wel om de toegang tot ICS en ICS-netwerken voor externen af te sluiten. De praktijk is echter weerbarstiger. Ten behoeve van onderhoud en controle op afstand (denk aan medewerkers die van thuis uit werken of onderhoud door derden) ontstaan er dan algauw hiaten in de beveiliging van netwerken en ICS. Risicomanagement is nog niet 100% geïntegreerd in de organisatie.

[16] Luiijf, E., & te Paske, B.J. (2015). *Cyber Security of Industrial Control Systems*: https://www.tno.nl/ics-security/

3.1.3 De kostprijs van cybersecurity

Een belangrijk aspect dat in veel van de interviews terugkwam is het feit dat cybersecurity geld en tijd kost. Vooral voor kleinere bedrijven kan dit een relatief zware kostenpost zijn. Bij grotere bedrijven is de cybersecurity vaak al beter geregeld. Er wordt door geïnterviewden meermalen verwezen naar de concurrentie in de markt waardoor leveranciers en installateurs zichzelf uit de markt kunnen prijzen als zij te veel focus leggen op cybersecurity en zonder expliciete vraag hiervoor vanuit de industrie kostbare beveiligingsfunctionaliteit willen toevoegen. Er wordt vanuit die partijen geconstateerd dat er vaak vanuit de klant nog te weinig vraag is naar cybersecurity en zeker niet naar de combinatie met arbeidsveiligheid. Bedrijven en organisaties zijn nog weinig bereidheid is om hier (veel) voor te betalen.

In plaats daarvan richt de vraag vanuit de bedrijven en organisaties zich over het algemeen op de operationele functionaliteit, kostenbeheersing en time-to-market. Zij willen in de eerste plaats iets dat effectief en efficiënt werkt, cybersecurity functies zoals firewalls worden dan vanzelf minder belangrijk want zonder deze werkt de installatie ook. Cyberbeveiliging komt hierbij dus pas na de efficiëntie van een systeem of installatie en daar zal eerder op bespaard worden.

Een belangrijke onderliggende factor hierbij is dat er nog te weinig publiekelijk zichtbaar fout gaat waardoor voor bedrijven de urgentie en noodzaak ontbreekt om te willen investeren in cybersecurity. Meerdere geïnterviewden geven aan dat het eigenlijk wachten is tot er iets goed fout gaat (dat ruim in de pers wordt uitgemeten) voordat bedrijven echt willen investeren in cybersecurity.

3.1.4 Weinig besef over welke impact van security/safety dreiging eigenlijk mogelijk is

Uit de interviews komt naar voren dat bij organisaties de cyber-situational awareness over het algemeen nog beperkt is. Er is een gebrek aan kennis, men weet nog niet goed wat eigenlijk mogelijk is. Bijvoorbeeld het besef dat toegang tot de netwerken voor medewerkers van buitenaf ook potentiële toegangskanalen zijn voor ongeautoriseerden. Als de ICS van kritische bedrijfsprocessen onvoldoende zijn afgeschermd kunnen in theorie via deze ook (bewust of onbewust) onjuiste instructies worden geüpload die het proces verstoren. Hier zijn nog geen veiligheidsstrategieën op gebaseerd. Ook is er volgens de geïnterviewden nog weinig bekend over de motieven van hackers: dus niet alleen wat hackers kunnen, maar ook wat zij willen? Zo wordt het voorbeeld gegeven dat er in de "hackergemeenschap" ook jongelui bij zitten die dingen doen "*omdat het kan*".[17] Ze experimenteren hoever ze kunnen komen. Deze groep is vooral geïnteresseerd om te kijken of ze iets plat kunnen krijgen, of in beweging zetten, zonder verdere achterliggende (kwaadwillende) motieven.

Het feit dat er nog maar weinig incidentinformatie over de dreiging en kwetsbaarheid van embedded software en communicatienetwerken wordt uitgewisseld, wordt genoemd als een onderliggende oorzaak voor deze lage cybersecurity awareness. Vaak is er schroom bij organisaties om over incidenten te melden (i.v.m. reputatie). Dit geldt helemaal voor dingen die per ongeluk fout gaan (zie ook 3.1.5.). Hierdoor is weinig publiek bekend van wat er gebeurd, op welke schaal en met welke impact.

[17] Denk hierbij aan scriptkiddies of recreationele hackers (white en black).

3.1.5 Onbewust onbekwamen

In de interviews komt vaak naar voren dat cybersecurity moet beginnen bij de mensen die met de systemen werken. Naast cybercriminaliteit of erger (e.g. terrorisme), heeft men ook te maken met onkunde. Veel geïnterviewden verwijzen naar de zogenaamde onbewust onbekwamen die 'domme' dingen doen. Er worden meerdere voorbeelden gegeven van deze 'domme' dingen. Bijvoorbeeld een medewerker die het ene moment een internetgame op zijn laptop speelt en het volgende moment op diezelfde laptop bij een grote klant inbelt om een procesverstoring te verhelpen; een operator die om zijn mobiel op te laden deze via een usb aansluit aan een bedrijfscomputer, of een medewerker die met een usb de 'air gap' van een gesloten systeem verbreekt. Elk van deze handelingen, die in de praktijk vaak als onschuldig worden beschouwd, kunnen er potentieel voor zorgen dat malware een weg vindt naar veiligheidskritieke bedrijfssystemen ofwel arbeidsmiddelen. Medewerkers zijn zich in dit opzicht nog niet bewust van wat de impact van hun handelen is of ontberen de persoonlijke discipline om privé en werk gescheiden te houden en bijvoorbeeld geen privémail moet openen op de werkplek[18]. Naar de klant toe kan het ook een dilemma zijn tussen veiligheid en gebruikersvriendelijkheid. Bijvoorbeeld, door veel gebruikte semi-veilige software (e.g. Dropbox) niet toe te laten op de geïnstalleerde servers verhoog je wellicht de veiligheid maar zal de klant minder blij zijn en eerder geneigd zijn naar andere shortcuts te zoeken die de veiligheid alsnog kunnen ondermijnen.
Ook bij het (veiligheids-)management ontbreekt nog het besef van de mogelijke gevolgen van onbewust onbekwame of kwaadwillende medewerkers of service/contractorpersoneel. Bij het uitvoeren van HAZOP's wordt er vaak van uitgegaan dat alles goed gaat: dat de mens in het scenario met de juiste intentie ("safety first") handelt. Op deze randvoorwaarden wordt verder geen risicoanalyse uitgevoerd. Echter, een systeem is zo veilig als het veiligheidsbesef en –gedrag van de mensen die er mee omgaan. Het gaat dus niet alleen om de ICT-techniek c.q. ICS maar ook om de methode van werken (procesinrichting), de organisatie en de factor mens (bewustzijn, adequaat handelen).

[18] Zo kwam bijvoorbeeld een schip op de Noordzee stil komen te liggen doordat een Trojaans paard de sprong maakte naar het scheepsvoortstuwingssysteem vanuit een privé-e-mailbox. (bron?)

Tabel 5. Overzicht van de beheersmaatregelen die in de interviews genoemd zijn, onderverdeeld naar sector en thema.

Sector	**Thema's**	**Generieke Beheersmaatregelen**
Algemeen	3.2.1.1 Bewustwording	- Vergroten van besef van de risico's bij het gebruik van netwerken. - Verbeter de communicatie en kennisuitwisseling tussen ICT (cybersecurity) en functioneel verantwoordelijk afdelingen - Management overtuigen van mogelijke impact van risico's. - Procesbeschrijving met oog op mogelijke inbreuken (zowel logisch als fysiek). - Goed gedrag belonen. - Bij andere sectoren kijken naar voorbeelden?
	3.2.1.2 Kadering van het probleem	- Classificeren van sector specifieke risico's. - Risico's formuleren in termen van 'business continuity'.
Publiek	3.2.2.1 Wet- en Regelgeving	- Meldplicht van cybersecurity inbreuken (e.g., datalekken) bij een overheidsinstantie [19] - Niet sturend, maar proces faciliterend handelen
	3.2.2.2 Certificering	- Security aspecten tijdens design/ontwerp verplichten. - Bestaande normen uitbreiden met menselijke factor. - Bestaande normen in begrijpelijke taal formuleren.
	3.2.2.3 Normkaders	- Normkader omtrent veilige bedrijfsvoering opzetten. - Als proces benaderen en niet als eenmalige oplossing.
Privaat	3.2.3.1 Onderling informatie over incidenten delen	- Opstellen van benchmarks voor onderlinge vergelijking. - Institutionalisering van de uitwisseling van incidentinformatie.
	3.2.3.2 Onderhoud en beheer	- Nadruk leggen op noodzaak preventief onderhoud. - Expliciteren waar verantwoordelijkheid ligt voor onderhoud en beheer.
	3.2.3.3 Opleidingen, training en bijscholing	- Aanpassen lespakket basisonderwijs - Bijscholing mogelijk maken van zittende vakmensen. - Verantwoordelijkheid nemen voor deze bijscholing vanuit de publieke sector. [20]

19 De per 1 januari 2016 ingaande meldplicht (ernstige) cyberinbreuken kan dit proces bespoedigen zodra de 'board room' zich het risico van de potentieel zeer hoge boeten realiseert.

[20] Hier zou meegelift kunnen worden met de mogelijke vervolgacties die voortkomen uit het 'Advies aan de Stassen van V&J en OC&W inzake cybersecurity in het onderwijs en het bedrijfsleven.' zoals opgesteld door de Cyber Security Raad (2 nov.2015).

3.2 Beheersmaatregelen

In deze sectie geven wij een overzicht van de verschillende beheersmaatregelen die uit de interviews naar voren zijn gekomen. De beheersmaatregelen zijn ondergebracht in acht thema's die vervolgens onderverdeeld kunnen worden in maatregelen die in het algemeen toepasbaar zijn en maatregelen die meer van toepassing zijn voor ofwel de publieke- ofwel de private sector. In Tabel 5 staat een schematische weergave van de beheersmaatregelen en de onderliggende structuur hiervoor.

3.2.1 Algemene thema's

3.2.1.1 Bewustwording

Alle geïnterviewden waren het erover eens dat er nog belangrijke stappen moeten worden gezet in de bewustwording van de risico's verbonden aan directe of indirecte koppeling van arbeidsmiddelen met het internet of andere vormen van telecommunicatie. Als vergelijkbaar voorbeeld wordt tunnelveiligheid gegeven. Naast wet- en regelgeving was en is er ook veel aandacht vanuit zowel de nationale als de Europese overheid om het belang van tunnelveiligheid te schetsen en zo tunnelveiligheid goed op de kaart te zetten.
Eén geïnterviewde waarschuwt wel voor het feit dat bewustwording vaak als showstopper wordt gebruikt; wanneer management om de tafel komt om (cyber)security issues te bespreken, wordt de conclusie als snel dat medewerkers bewuster moeten worden gemaakt, alsof dit het enige is wat nodig is. De vraag is bovendien of je alles met onderwijs en opleiding kan oplossen en van medewerkers mag verwachten dat ze alle complexe problematiek hieromtrent kunnen begrijpen. Het doel moet echter zijn om de problematiek waar mogelijk te internaliseren en van onbewust onwetend, naar bewust wetend te komen. Dit is echter een lang proces en het is belangrijk om in de gaten te houden wie waar bewust van moet zijn en wie waar verantwoordelijk voor is. Vergroting van het bewustzijn begint bij het verantwoordelijk management en zal zich vooral moeten ontwikkelen bij de mensen die met de systemen werken en de ICS en (machinerie)functionaliteiten met embedded software verwerven.
Uitvoerend personeel kan zowel potentiële slachtoffer zijn als het fout gaat, als deel van het probleem uitmaken (zie ook sectie 3.1.5). Cybersecurity is meer dan alleen een technisch proces: ook hoe medewerkers denken telt mee. Bewustwording moet er hier als eerste voor zorgen dat er geen 'domme' dingen meer worden gedaan en bijvoorbeeld door onvoorzichtigheid malware wordt geïnstalleerd of achterdeuren voor hackers worden opengezet. Het besef moet komen dat het werken met embedded software en netwerken, nieuwe risicofactoren met zich meebrengen. Net zoals dat we weten dat we risico lopen wanneer we een auto instappen, daarvoor onze gordel omdoen en verkeerswaarschuwingen opvolgen. Bij cybersecurity is dit besef er nog niet 100%, waardoor medewerkers "net als thuis" ook in de bedrijfsomgeving nog wel eens op een (malware/phishing) linkje drukken.
Verder wordt ook de ICT- en security-afdelingen genoemd als partijen die bewuster moeten worden van de problematiek. Bijvoorbeeld tijdens crisismanagement worden al vaak knopen doorgehakt, maar is het de vraag of zij het gehele proces wel kunnen overzien. Hierbij is het ook van belang dat deze partijen bij elkaar worden gebracht (zie sectie 3.1.2).

Ook bij het management van organisaties, de uiteindelijke eigenaren van het probleem, moeten nog slagen worden gemaakt met betrekking tot cybersecurity bewustwording in combinatie met safety. Enerzijds geven geïnterviewden aan dat bedrijven over het algemeen wel op de hoogte zijn van (een deel van) hun cybersecurity-risico maar hier vaak nog weinig structureels mee doen. Het gaat hierbij zowel om productiebedrijven als contractors en service suppliers. Zo worden veel cybersecurity issues niet meegenomen in de risicoanalyses. Idealiter houden bedrijven en organisaties echter niet alleen rekening met het uitvallen van ICT-systemen maar ook met de mogelijkheid dat iemand het proces moedwillig verstoort. Hierbij is het belangrijk om overtuigend te demonstreren wat er mogelijk is: als 'wij' een platform kunnen overnemen, dan kunnen anderen dat ook. Als de top overtuigd is van het cyber-gerelateerde risico met name voor hun ICS en embedded software dat het bedrijf of organisatie loopt, komt er beweging. Men ziet dat deze organisaties ook deel gaan nemen aan internationale werkgroepen op het gebied van cybersecurity en gespecialiseerde security managers in dienst hebben. Verder moeten organisaties goed de 'chain of command' (i.e., wie op de hoogte moet zijn wanneer een incident plaatsvindt) en de update schema's van relevante software en installaties op orde hebben. Dit kan het beste vanuit de boardroom worden aangestuurd.

Op dit moment wordt er nog vaak gezegd '*maar hier gebeurt niks'*. Echter, als je wacht tot er iets gebeurt ben je meer kwijt (geld, imago, tijd) dan wanneer je nu gestructureerd en integraal over risico's gaat denken.
Qua aanpak zou men een procesbeschrijving moeten maken, om vervolgens per onderdeel te kijken welke fysieke en logische inbreuken kunnen plaatsvinden (bijv. een operator die een kraan op afstand bestuurt, kan ook nog fysiek overmeesterd worden door een kwaadwillende die besturing van de kraan wil overnemen).
Voor de bewustmaking van organisaties wordt vooral naar de publieke sector gekeken, maar ook organisaties zelf kunnen hier een rol spelen. Als organisaties hun klanten belonen als zij hun systemen goed op orde hebben zou dat helpen, maar dit gebeurt op het moment nog op marginale schaal. Verder worden door geïnterviewden drinkwaterbedrijven en kernenergiebedrijven aangedragen als voorbeelden waar het cybersecuritybewustzijn al hoog is.

3.2.1.2 Kadering van het probleem

Uit de interviews komt vaak naar voren dat cybersecurity niet als een generiek probleem moet worden gezien. In plaats daarvan moet cybersecurity en de bijbehorende risico's domein- of sectorspecifiek worden gedefinieerd en benaderd. Bijvoorbeeld, voor Defensie gaat cybersecurity om oorlogsdaden en terrorisme via het internet, voor een oliebedrijf gaat het om het risico van bedrijfsspionage en sabotage van olietanks, bij banken gaat het om fraude, bij ziekenhuizen om de privacy van patiënten, en voor de politie gaat het om en informatie beveiliging. Dit heeft allemaal betrekking op cybersecurity , maar betreft geheel andere problematieken. Geïnterviewden geven aan dat je een juiste domeinspecifieke klassering nodig om de mogelijke schade die door een hacker kan worden gedaan in te schatten en correct te kunnen reageren.
Ook de context van eenzelfde situatie kan bepalend zijn van hoe risico's geframed moeten worden. Ter illustratie wordt de analogie van een marineschip in de haven of in oorlogssituatie gegeven: In een haven wil je een protocol dat voorkomt dat een raket gemakkelijk wordt afgeschoten, echter zodra het schip op zee is in een

oorlogssituatie wil je dit juist niet. Hoe moeilijker de context van cybersecurity te omschrijven is, hoe moeilijker het ook is om normen en regelgeving voor te schrijven.

Specifiek voor de industriesector waren geïnterviewden het erover eens dat risico's omtrent cybersecurity moeten worden ingekaderd op basis van 'business continuity'. Met andere woorden, risico's moeten in relevante business termen worden geplaatst zoals '*hoeveel geld verlies je als ICT uitvalt?*'. Het gaat hier om het verlies dat gedraaid wordt en minder om de ICT, de falende ICT is alleen de oorzaak. Cybersecurity op zich levert vaak niks op, dus moet duidelijk worden gemaakt wat er te verliezen is, waar het een verzekering op is. Op deze manier kunnen cyberrisico's vertaald worden naar business problemen waar de boardroom wakker van ligt. Hierbij is ook belangrijk dat de Chief Information Officer (CIO) deze problematiek zodanig kan overbrengen.

3.2.2 Publieke sector

3.2.2.1 Wet- en Regelgeving

Wet- en regelgeving wordt als vanzelfsprekend als een domein van de overheid gezien. Regelgeving kan worden gebruikt als een middel om het gedrag te sturen. Zo kan een wetsvoorstel voor meldplicht van cyberinbreuken ervoor zorgen dat we meer te weten komen over wat er in de praktijk gebeurt (zie ook 3.2.2.3.)[21].
Anderzijds wordt Frankrijk wordt als voorbeeld aangedragen waar met wet- en regelgeving bepaalde (cyber)security maatregelen verplicht zijn gesteld met strafrechtelijke gevolgen als die niet worden nageleefd.
Wel wordt er opgemerkt dat het belangrijk is dat de overheid niet direct in detail zou moeten leiden maar vooral het proces moet faciliteren. Eén geïnterviewde stelt dat de overheid eisen zou moeten stellen waar een systeem minimaal aan moet voldoen, maar niet alles exact willen laten voorschrijven. Anders heb je het risico dat bedrijven en organisaties meer aan compliance gaan denken dan aan risicomanagement. Dat wil zeggen dat aan de regels voldoen (om bijvoorbeeld strafrechtelijke gevolgen te voorkomen) belangrijker wordt dan echt risico's uit te bannen. Een andere geïnterviewde maakt de analogie met het verkeer: de overheid zorgt voor een goede infrastructuur en voor de verkeersregels, maar het is uiteindelijk aan de burger om zijn rijbewijs te halen en zich aan de regels te houden. Dan gaat alles goed, en een soortgelijke situatie wil je voor het internet.
Verder wordt de notitie gemaakt dat de ontwikkelingen zo snel gaan dat deze mogelijk niet zijn bij te houden met wet- en regelgeving. Inzet van andere beleidsinstrumenten is daarom ook nodig.

3.2.2.2 Certificering

Veel geïnterviewden gaven aan dat cybersecurity al in een veel eerder stadium moet worden meegenomen in het maakproces, bijvoorbeeld al in de ontwerp- en designfase van een arbeidsmiddel. Vanuit de publieke sector (e.g., de overheid, certificeerders, en brancheverenigingen) kan hierin gestuurd worden door middel van certificering en standaarden om eisen te stellen waaraan systemen moeten voldoen. Bijvoorbeeld door het opstellen van een keurmerk met verschillende niveaus naar gelang de beveiliging in relatie tot kwetsbaarheid en impact van het risico. Of het bij arbeidsmiddelen verplicht stellen dat bepaalde, niet noodzakelijke

[21] Een dergelijk wetsvoorstel gaat per 1 januari 2016 in.

handelingen onmogelijk zijn (bijv. geen- of afgesloten usb-ports als deze niet nodig zijn voor het beheerproces).
Enkele specifieke voorstellen voor aanvulling van normen zijn geopperd tijdens de interviews. Bijvoorbeeld om de menselijke factor te introduceren in IEC 62443 (ex-ISA 99)[22]. Dit document gaat over het gebruik van veilige IACS (Industrial Automation and Control Systems). De mens is vaak nog de zwakste schakel in het systeem maar komt nog niet aan bod in de aanpak. Hierbij moet dan wel rekening gehouden worden met culturele verschillen internationaal, en ook de benodigde opleidingen om met dit soort systemen te werken kunnen concreet worden opgenomen. Ook wordt de ISO 55000[23] genoemd als startpunt om verder te verbreden met cybersecurity issues.
Men geeft aan dat men zich aan voorgeschreven normen houdt. Er worden echter ook vraagtekens geplaatst bij de mate waarin certificering kan helpen. Als een klant niet adequaat omgaat met de geleverde installaties of software, bijvoorbeeld door er een thuislaptop aan te koppelen, dan is de cybersecurity al gauw niet meer te garanderen. Verder moet men ook niet willen doorschieten in compliance. Een bedrijf kan 100% compliant zijn aan regels en certificering, maar nog steeds niet alle risico's uitgebannen hebben. Kan de tijd die wordt besteed aan het compliant worden dan niet beter besteed worden aan daadwerkelijke risicobeheersing?

3.2.2.3 Normkaders

Eén geïnterviewde noemt een derde thematiek die vanuit de publieke sector kan worden gestuurd namelijk normkaders. Een belangrijk aspect van een normkader is dat dit een dynamisch proces is. Er moet niet gedacht worden in eenmalig een concrete oplossing bij een probleem introduceren, maar het normkader moet continue worden gewijzigd en bijgesteld worden om veroudering te voorkomen te opzichte van maatschappelijke en technologische ontwikkelingen.
Als voorbeeld van de ontwikkeling van een normkader wordt de bankensector gegeven. Bij banken is het bewustzijn ontstaan dat ze naast markt- en krediet-risico's ook operationele-risico's lopen, dat wil zeggen dat als er fouten in het proces worden gemaakt, deze consequenties hebben. In 15 jaar tijd zou er een normkader zijn ontstaan omtrent het 'gij zult uw operationele risico inperken' waar banken zich aan houden.

Hierbij is het belangrijk dat een normkader specifiek voor de context van een bepaalde sector wordt opgesteld. Zie hiervoor ook sectie 3.2.1.2.

[22] http://isa99.isa.org/ISA99%20Wiki/Home.aspx
[23] http://www.iso55000.nl/

3.2.3 Private Sector

3.2.3.1 Onderling informatie delen

Geïnterviewden geven aan dat we eigenlijk nog bezig zijn met het in kaart brengen van het probleem rondom cybersecurity: we weten nog niet hoe groot de ijsberg is, omdat er geen meldplicht is over cyberincidenten. Cybersecurity is vaak geregeld op een need-to-know basis, incidenten worden vaak niet gedeeld in verband met privacy en mogelijke reputatieschade. Cybersituational awareness zou echter groeien als incidentinformatie zou worden gedeeld. Onderling zouden bedrijven hun eigen practice kunnen ranken met het doel om elkaar uit te dagen. Pas als men weet wat er mis kan gaan of is gegaan, kan daarvan geleerd worden.
Geïnterviewden geven aan dat hier een rol is weggelegd voor branches en werknemersorganisaties. Deze zouden kunnen helpen met het opstellen van 'proof of practice' en benchmarks waar bedrijven aan moeten voldoen en waarop ze onderling kunnen vergelijken. Ook worden Information Sharing and Analysis Centres (ISACs) als relevante partijen genoemd voor de vitale sectoren. Deze bestaan in Nederland voor twaalf sectoren. [24] Het is een vorm van institutionalisering van de uitwisseling van gegevens. Als hiermee het besef groeit dat iedereen dezelfde problemen heeft, verlaagt dit de drempel om informatie te delen. Het Nationaal Cyber Security Center (NCSC) coördineert deze ISAC's en zou kunnen sturen op domein overschrijdende samenwerking, bijvoorbeeld door ISACs op nationaal niveau te laten samen komen. De resulterende threat landscapes zouden dan van meer waarde zijn dan de huidige inzichten van ISACs individueel.

3.2.3.2 Opleiding, training en bijscholing

Geïnterviewden erkennen het feit dat de huidige generatie operators en medewerkers nieuwe skills nodig heeft. Operators zijn nu vaak geen bestuurders meer van arbeidsmiddelen maar supervisors, vaak op afstand, van het (geautomatiseerde) proces. Het belang van training en opleiding wordt dan ook vaak benoemd. Idealiter begint dit al op de basisschool met bewustwording van de nieuwe technologieën en hoe deze werken, maar dat zal nog jaren duren voordat er effect zichtbaar is op de werkvloer.
Bijscholing is dus ook van belang om een grote groep zittende vakmensen (bijvoorbeeld die van 40 jaar en ouder) met de nieuwe tools te laten werken. Ook voor deze groep zouden er 'Fieldlabs' moeten zijn die het mogelijk maken om in een industriële omgeving bij te leren met tutors en individuele begeleiding en voor het maken van leerplannen. Hier neemt op het moment niemand de verantwoordelijkheid voor. Het ministerie van OC&W legt volgens de geïnterviewden voornamelijk het accent op beginners op de arbeidsmarkt.

3.2.3.3 Onderhoud en beheer van software en hardware

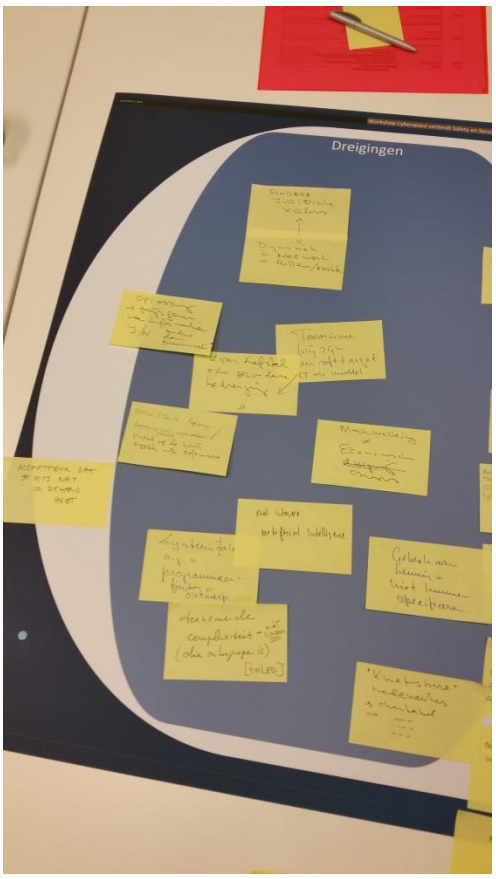
In de interviews wordt genoemd dat de bekende doctrine 'don't fix it if it ain't broken' niet opgaat voor cybersecurity. Constante updates zijn noodzakelijk om de beveiliging zo optimaal mogelijk te houden. Met andere woorden, meer nadruk op preventief onderhoud is daarbij nodig. Uit de interviews komt naar voren dat de verantwoordelijkheid hiervoor bij de gebruikers ligt. Op het moment is het zo dat installateurs en leveranciers een product zouden moeten leveren dat tot op dat

[24] https://www.ncsc.nl/samenwerking/publiek-private-samenwerking/isacs.html

moment voldoet aan alle cybersecurity eisen; het is daarna de verantwoordelijkheid van de gebruiker om dit zo te houden (zie ook sectie 3.1.1).

4 Workshop-resultaten

Tijdens de workshop konden deelnemers door middel van mind mapping ideeën op post-its schrijven en deze op aangegeven plaatsen plakken in een overzicht. In twee parallelsessies werd er enerzijds gekeken naar de dreigingen en het identificeren van kwetsbaarheden, en anderzijds naar mogelijke beheersmaatregelen op basis van de productlevenscyclus (sectie 2.1.2). Verder is er nog een lijst van actoren opgesteld waar bewustwording/informatieverstrekking belangrijk is of waar informatie verstrekking kan worden ondersteund. Figuur 2 geeft een voorbeeld van het resulterende overzicht. De resultaten hieronder zijn een directe weergave van de post-its zoals ze tijdens de sessies zijn gecreëerd.



Figuur 2. Voorbeeld weergave van de resultaten uit de workshops.

4.1 Risico's, dreigingen en kwetsbaarheden

Accepteer dat je iets niet (compleet) in de hand hebt.

4.1.1 Dreigingen

- Ander juridisch kader van toepassing
- Dynamiek in netwerk en in de rollen/kracht
- Terrorisme

    - Wij (de industrie) zijn een soft target voor terroristen die met ICT als middel fysieke impact of angst willen bereiken.
- Bijvoorbeeld het koper diefstal: ook secundaire bedreiging (veiligheden vallen uit, of de controle of besturing valt uit)
- Online/remote toegang is bedreiging voor medewerkers.
    - Pistool op de borst
    - Lokaal fysieke toegang versus softwarematige toegang op afstand
- Marktwerking en economische crisis
- Niet-integere artificial intelligence
- Systeemfalen als gevolg van programmeerfout / ontwerp
- Toenemende complexiteit (niet lineair) die onbegrepen is (Taleb[25])
  Kwetsbare medewerkers
    - Bijv. chantabel.

4.1.2 Kwetsbaarheden

- Communicatie
    - Bestuurders en technici spreken andere taal
- Mede daardoor: een gebrek aan gevoel van urgentie bij RvB / directie
- Mede daardoor: Geen geld beschikbaar/voor over voor goede security (lage urgentie)
- Beveiliging van ICS en SCADA wordt niet meegenomen in verwervingsproces nieuwe functionaliteit
- Organisatie inrichting (koninkrijkjes: integrale benadering ontbreekt)
- Risicomanagement niet geïntegreerd in de business (verplicht nummer)
    - Geen business value
- Wereld meestal vanuit meerdere paradigma's
    - Conflict
- Paradigma shift nodig (grafiekje)
    - Out of the box denken
    - Oude paradigma's loslaten
- Gebrek aan integrale benadering (mens, processen, fysieke beveiliging, IT-beveiliging)
- Van gescheiden vakjes (ontwerp, ontwikkeling, fabricage, etc.)
    - naar één integraal verantwoordelijk team (of gescheiden maar goed verbonden met gemeenschappelijk doel/kennis)
- Systeemintegriteit (kennis van totale systeem)
- Renewable components. Nieuwe risico's voor zelfde component door nieuwe maar andere context. (reactie brandveiligheid vliegtuig versus brandveiligheid trein; moet getoetst worden naar norm van gebruik (wel of niet motor uitzetten))
- Bewustwording versus verantwoordelijkheid
    - Verantwoordelijkheid leid tot besluiten en acties
    - Bewustwording moet bij de top van bedrijven, politiek en ziekenhuizen gebeuren
    - Bewustwording door risicomanagement / BCM/ et cetera.

[25] Taleb is auteur van boeken als 'black swans' en 'anti-fragile' waarin hij een pleidooi houdt om meer aandacht te besteden aan de outlyers, dus verder dan de 10-6 bij de gauss kromme. Ook pleit hij (net als Snowden, met zijn Cynefyn model) voor meer aandacht voor het feit dat systemen niet lineair zijn.

- Onvoldoende kennis/kunde bij risicomanagement functionarissen om toegevoegde waarde voor business duidelijk te maken.
- Veiligheid en risico zijn ondeugdelijke begrippen voor niet-experts.
    - Onduidelijke terminologie
- Gebrek aan kennis. Onbewust onbekwaam over inhoud, processen, systemen en organisaties. Moeten naar onbewust bekwaam zie te komen.
- Leren leren over known, known unknown en unknown unknown
- Niet één veilige situatie maar meer; wordt door context bepaald (op basis van inhoud, processen, systemen en organisaties)
- Impact analyse uitvoeren over wat is belangrijk?
- Achterdeur via 'telewerken' geeft risico ongeautoriseerde manipulatie/ wijziging systeem.
- Niet-resilient managen.
    - In plaats van weg van statisch risicomanagement: anticiperend en adaptief vermogen
    - Leren zwakheden dreigers
- Toegankelijk voor drone (WiFi)
- Pleisters plakken i.p.v. fundamentele oplossingen
- Niet gebruiksvriendelijk ontwerp: nodigt slecht (i.e., onveilig) gedrag uit.
- Niet redundant uitvoeren van systemen.
- Ontbreken van lines of defences voor cyberrisico's (geen Layer of Protection Analysis; LOPA)
- Veel verschillende gebruikers
- Snel veranderende omgeving
- Zelfde informatie op diverse plaatsen opgeslagen / terecht gekomen.
    - Redundant (bijv. toegangsinformatie)
- Naïviteit bij gebruikers van gekoppelde arbeidsmiddelen of systemen
- Kennis op basis van need to know. Men moet telkens opnieuw het wiel uitvinden zonder dat je het weet.
- Fail to limit losses.
- Menselijke factoren
    - Denk aan toegangsprocedures / sleutels
- Niet voldoen aan gezamenlijke basisvoorwaarde, wel op één lijn gaan zitten.
- Oplossingen zoeken op basis van (achterhaalde) traditionele paradigma's voor risicomanagement.

4.2 Beheersmaatregelen

- Kennisontwikkeling over gedaante en impact van combinaties van nieuwe technologieën/risico's
- We begrijpen het niet, ICT gaat heel snel. Wat is de maatschappelijke verantwoordelijkheid.
- "Als het fout gaat hoor ik het wel (bestuurder)

Bij een opdracht

- Waar is de fase van behoefte definitie en opdracht formulering?
- Corporate Security Concept/ Corporate Security architecture

- Richtlijnen/ Terms of Reference bij bestellingen. Scope van Opdracht (Inclusief CyberSecurity)
- Architectuurontwikkeling integraal
- Classificatie risiconiveau
- Risico? Autorisatie? Verantwoordelijkheid! Borging!

Feedback loops zetten tussen de diverse stappen levenscycli

4.2.1 Ontwerp en engineering

- Gedragsregels cybersecurity
- Screening ontwerpers (kennis/kunde en kwaadwillend?)
- Cybersecurity ontwerp specificaties in opdracht, inclusief detectie en forensisch.
- Register ontwerpfase (units + interacties)
- Useability
- Ontwikkelproces structureren (o.a., taken verantwoordelijkheden en bevoegdheden). Vrijgave milestones en proplanning
- Ontwerp: Fabrikant moet gevaren inventariseren en ervoor zorgen dat deze zo veel mogelijk worden weggenomen. Voor restgevaar moet fabrikant aangeven hoe dit is te beheersen.
- Risico-inventarisatie
    - Toeganganalyse (internet)
    - Netwerk (alle niveaus)
    - Risico inventariseren
    - Hardware (draadje losnemen)
    - Software
    - Afschermen fysiek (kooi van Faraday)
    - White list (software/processen).

- PLC uitrusten met antivirus/malware beveiliging
- Ontwerp: intrinsiek veilig
    - Geen verbindingsmogelijkheden met de buitenwereld. Dus geen aansluitingen op internet. Geen mogelijkheden voor toegang via informatiedragers.
    - Naar integraal risicomanagement die de S verbinden: e.g. SafetySec HAZOP?
- Ontwerp: Moet rekening houden met de levenscyclus van product en onderdelen en grondstoffen.
- Meer system engineering toepassen.
- Nieuwe risicoscenario's introduceren
    - Cross domein leren
    - Analogieën: auto-machinesysteem "
- Betrek ICT specialisten bij risicosessies (safety cases, TRA's, RI&E's)

4.2.2 Productie/levering en installatie

- Ingangscontrole (specificaties)
- TVB's verdelen
- MoC
- Register 'realisatiefase'
- Programmaomgeving integer, zonder achterdeuren

- Testfase cybersecurity
- Project structureren (TVB's milestones: planning en vrijgave)
- Dat wat niet valt te regelen op niveau van een arbeidsmiddel. Dit vraagt om toepassing van technische of organisatorische maatregelen in de gebruiksfase.
- Trekt wissel op gedrag en cultuur
    - Gedrag van individuele personen
    - Cultuur van bedrijf of delen daarvan
- Vriendelijke hackers stresstest laten ontwikkelen gericht op machineveiligheid.
- Wie is verantwoordelijk voor geheel duidelijk maken.
    - Beheerder
    - Service supplier (i.e. onderhoudsdienst)
- Testprotocollen regressietesten.
- Juist leerprogramma
- Juiste clearance gebruiken
- Redundant uitvoeren systemen controleren die elkaar controleren.
- Productie richtlijnen en installatieboekjes uitbreiden met nieuwe risico's
    - Pagina 1: beveiligingsinstellingen (EMC-normen naar achteren)
    - Secure out-of-the-box
- MoC ook naar cyberrisico's laten kijken.
- Hoe arbeidsmiddel veilig moet worden geïnstalleerd geeft fabrikant aan. Hoe verder als er sprake is van samenbouw. Introduceert nieuwe risico's. Ook daar rol fabrikant.
- Systeemintegratoren
    - Maken complexe systemen van al dan niet 'veilige' componenten.
- Ook traditionele security laten meelopen met oog op machineveiligheid.

4.2.3 Gebruik

- Goede logging / audit-trail
- Gebruiker gecertificeerd en gescreend
- Geen koppeling met buitenwereld (standalone)
- TVB's
- Planning (updates/fysiek/softwarematig)
- Periodiek testen
- MoC
- Register levend houden
- Back-up
- Detectie en forensisch
- Tijdelijke wachtwoordgenerator
- Gedragsregels m.b.t. cybersecurity
- Toezicht/inspectie
- Voorkom dat personeel zelf software mag installeren (bijv. spelletjes) op ICS en andere interne systemen.
- Rolgebaseerde toegang en functiescheiding
- Integraal G&S management
    - …[26]

[26] Onleesbaar

    - Multidisciplinair incident management.
    - Integraal crisismanagement.
- Gebruik overeenkomstig de specificaties van de fabrikant.
- Procedures m.b.t. toegangscontrole en sleutel procedures.
- Gereguleerde overdracht/opleiding tussen installateur en gebruiker.
    - Beveiligingsstappen
    - Installateur op bezoek bij gebruiker

- Toegangsbeheer en wachtwoorden
- Opleiding/bijscholing vakmensen
- Loskoppelen arbeidsmiddel van externe netwerken zoals het internet
- Screening eigen personeel (antecedentenonderzoek)
- Nodig een groep hackers uit om je systeem aan te vallen (of minimaal de beveiligingslekken te identificeren).
- Protocol gebruik usb sticks, externe harde schijven en de cloud.
- Inplugmogelijkheden beperken
- Let op bezoekers en/of tijdelijke gebruikers zoals bv. stagairs.
- Breng barrières aan/schakels tussen gekoppelde (fysieke) systemen om cascade effecten te voorkomen elders in het systeem.
- Geef voorlichting over mogelijk cybersecurity risico's aan medewerkers en tijdelijke medewerkers, en aan third parties (uitbesteding)

4.2.4 Onderhoud

- Arbeidsmiddel gaat naar veilige modus bij storing
- Need to know! Onderhoud en gebruikers → bewust veilig
- Vernietiging data en wachtwoorden
- Lokaal onderhoud, niet op afstand
- Gecertificeerd personeel
- Goede logging / audit-trail
- Directe gebruikers actief betrekken
- SLA (service providers) inrichten op cybersecurity risico's
- Afspraken maken over resultaten op basis van gewenste/ongewenste effecten.
    - Relevantie van sturen op performance van uitvoering
- Onderhoudsrollen (logisch) gescheiden van gebruikersrollen
- Screening personeel installatie bureaus die softwareupdate uitvoeren aan procescontrole systemen dan wel arbeidsmiddelen
- Onderhoud (patching) op kleine (beheersbare) schaal (pilots)
- Tenminste op het veiligheidsniveau houden die de fabrikant heeft gespecificeerd.
- Updates veilig uitvoeren geen nieuwe gevaren introduceren
- Laat je systemen periodiek tijdens onderhoudsbeurt testen op beveiligingslekken.
- Back-up systemen automatiseren
- HRM personeelsregistratie systeem up to date houden. Let op toegang tot systemen door ex-medewerkers.

4.2.5 Vernieuwing

- Leren/feedbackloops bij elke stap
  - Verbetercyclus
- “Zie ontwerp en productie/levering”
- Referenties en verificatie
- Regelmatig op basis van contract
- Lokaal vernieuwen
- Geen systeem op afstand
- Ook reparatie? Reparatie is defecte delen vervangen door gelijkwaardige componenten.
- Aanpassen aan de stand van de wetenschap, techniek en technologie.

4.2.6 Afbreking/ontmantelen en afvoer

- Gebruik gecertificeerde partijen
- Door gespecialiseerde firma’s
- Controlemateriaal niet naar derde wereld gedumpt
- Aantoonbaar veilig ontmantelen
- Voor afvoer informatie dragers vernietigen
  - Inclusief informatie in embedded systemen, componenten en netwerkcomponenten
- Oude Pc’s, data definitief onbruikbaar maken.

4.2.7 Slotgedachten

- Waar is einde van systeem? I.e. Scope van de governance
- Tijdshorizon: verschuivende belangen
  - Kun je dit met een framework tackelen?
- Kijk naar totale beheersysteem
  - Monitoring door fabrikant als voorbeeld en online aanpassing Safety parameters
  - Information security problematiek qua componenten is veel omvattender dan componenten in machinerichtlijn

4.3 Actoren

Is governance wel of niet belangrijk?

4.3.1 Publieke sector

- Europese Platforms
- ISSA[27]/ ?/ Bilbao (EU agentschap voor V&G op het werk/ Focal Points
- NCSC (Nationaal Cyber Security Center)
- Rathenau Instituut
- SER (Sociaal Economische Raad)
- VVO/NCW
- WRN

[27] http://issa.int

4.3.2 Bedrijfsleven

- Universiteiten (e.g., Tilburg Institute for Law, Technology, & Society/ TU Delft/ Eindhoven/ Twente)
- Netwerk Pieter van Gelder
- WIB
    - Proces control
    - High end
- ISAC's (Information Sharing and Analysis Center)
    - i.e., er komt een nieuwe op het gebied van industrie
- FME
- NEN / Norm commissies (Cie's)
- COB (kenniscentrum voor ondergronds bouwen en ondergronds ruimtegebrek)
- VLR (De Nederlandse Vereniging voor Lift- en Roltraptechniek)
- Medische sector (systeem integratie IC techniek)
- Cyber Security Academy (CSA)
- Opleidingen
    - Vakopleidingen
- Vitale infrastructuur (zie EZ)
- DEVOPS teams (development and operation teams)
- VNCI (Vereniging van de Nederlandse Chemische Industrie)
- SmartIndustry.nl agenda
- Breed palet van productiebedrijven
- Fabrikant/ keuring/ certificering/ gebruik/ toezicht
- Beroeps vereniging
    - NVVK (Nederlandse Vereniging voor Veiligheidskunde)
    - SEC
- KPMG / accountant/ risk management (wet op jaarrekening stelt eis aan ondertekening m.b.t. de beveiliging van ICT-middelen, helaas ICS "te ver van het bed (en maatpakken)")
- DITCM
    - Ronde tafel bijeenkomsten (o.a. mobility)
- Beheersstichting / inspectiediensten
- Branche van softwareontwikkelaars
- Congres circuit (maar dan niet alleen over proces safety)
- Systemen van waterschappen (zie ook RAAK project HHS, TNO, Unie van Waterschappen, NCSC)

5 Discussie

Op basis van de resultaten uit de interviews en de workshop zijn in de reflectie op de resultaten door workshopdeelnemers, geïnterviewden en TNO deskundigen de volgende aanvullingen opgemerkt.

5.1 Integraal risico management

5.1.1 Risico management

De basis is dat het aspect cybersecurity verbonden wordt aan veiligheidsmanagement en de risico-evaluatie niet alleen in termen van financiële of als imago-impact wordt uitgevoerd. Ook een strikte compliance aanpak is geen garantie dat integrale veiligheid wordt bereikt.
Regelmatig is benadrukt dat de ICT- en security-afdeling partijen zich bewuster moeten worden van de arbeidsveiligheidsproblematiek. Bijvoorbeeld tijdens crisismanagement worden al vaak knopen doorgehakt, maar is het de vraag of zij het gehele proces wel kunnen overzien. Ook bij crisismanagement is het dus van belang dat deze partijen bij elkaar worden gebracht.
Veiligheidsmanagement zal zich moeten uitstrekken over de hele levenscyclus. Het doel moet zijn om de problematiek waar mogelijk bij alle actoren in de (product)levenscyclus te internaliseren en van onbewust onwetend, naar bewust wetend te komen.
In het kader van risico management kan nagegaan worden welke standaard methoden en technieken zich laten uitbreiden naar cybersecurity of zelfs integrale analyse methoden worden ontwikkeld. Gedacht kan worden het expliciet meenemen in HAZOPS van de rol van programmatuur en de rol van de mens. Doel hoeft daarbij niet per definitie te zijn om de mens “weg te ontwerpen” maar juist ook zijn rol in het veerkrachtig opvangen van dreigingen en verstoringen te versterken.

5.1.2 Scholing

Scholing is één van de manieren om betrokken deskundigen en vaklieden die zich met de arbeidsveiligheid dan wel cybersecurity bezighouden bewust te maken en bij te scholen. Ook deskundigen in betrokken staven zullen door bijscholing hun kennis en inzicht dienen te vergroten. Zo verstopt ICS zich in (genetwerkte) functionaliteit en is de proceseigenaar zich niet bewust van het cyberrisico. [28] Hij/zij is er niet voor opgeleid en onderkent de uitdagingen niet.
De scholingsnoodzaak gaat op voor diverse typen organisaties: Onderhoud/service, Productie, Leverancier. Branches kunnen zowel bij bedrijven als in hun netwerk en keten bewustwording entameren.

5.1.3 Technologie

Een belangrijk aandachtspunt is de gewenning aan vertrouwde levenscycli: bijvoorbeeld je PC/laptop elke 3 jaar vervangen, de vaste telefoon was elke 15 jaar (wellicht nooit meer), en liften elke 30 jaar. Bij machines met een lange levensduur kunnen tijdens onderhoud of storingsoplossing wel nieuwe vervangende module met ICT-functionaliteit embedded worden geplaatst. Daarbij kan over het hoofd worden gezien dat veilige basisinstellingen moeten worden aangepast, er geen

[28] Luiijf, E., & te Paske, B.J. (2015). *Cyber Security of Industrial Control Systems*: https://www.tno.nl/ics-security/

overdracht aan de ‘eigenaar’ plaats vindt, of overleg plaatsvindt met de ICT-afdeling! Denk bijvoorbeeld aan de consequentie van een data-abonnement voor een mobiel waarmee bijv. de lift met de buitenwereld communiceert. Ook kan een traditioneel werktuigkundig georiënteerde afdeling bestaande functionaliteiten binnen te brengen of vernieuwen (waaronder arbeidsmiddelen) zonder zich te realiseren dat de vernieuwing ICT-gebaseerd is. Voor de eigen bedrijfs-ICT-afdeling gebeurt dat ongemerkt en ‘achter hun rug’ om. Veelal geschiedt de installatie door een externe firma die zorgt dat alles werkt. Het “cyber secure” aspect van de installatie valt veelal buiten scope met als consequentie dat er bijvoorbeeld geen cyber security instructie gegeven wordt of bedrijfsprocedures hierop worden aangepast.
Ook voor inkoop is het van belang om cyber security bij verwerving mee te nemen. Vaak wordt dit aspect onterecht als ballast ervaren.
Al met al gaat het dus niet alleen om de ICT-techniek maar ook over de methode van werken en de inrichting van de organisatie. Daarbij begint het bij de design specificaties en gaat het bijvoorbeeld ook om alertheid op ‘function creep’. Over een periode van vele jaren kan een systeem groeien en complexer worden zonder dat iemand in de gaten heeft dat het kritiek wordt vanuit cybersecurity. Dit is niet alleen het geval met losse arbeidsmiddelen maar ook met systeemintegratoren die geen veilig product en functionaliteit afleveren. Zowel product als proces moeten cybersecure worden geleverd.

5.2 Complexiteit

De toenemende koppeling van systemen in netwerken onderling maakt cybersecurity problematiek nog ingewikkelder. Wij weten gewoonweg niet hoe software interacteert met andere software. Denk bijvoorbeeld aan gebouwbeheerssystemen. Een ander voorbeeld zijn auto’s. Daar werken meer dan 50 PLCs van diverse fabrikanten samen. Het resultaat: een (elektronische) handrem trekt zichzelf aan op de snelweg. Engineering kan dat niet allemaal meer oplossen. Het omgekeerde vraagt ook aandacht namelijk het ontbreken van stabiele connectiviteit. Als er wordt gekozen voor een bepaald communicatieplatform (bijvoorbeeld internet of 4G) dat wordt verstoord zonder dat dit te maken heeft met kwaadwillendheid of het arbeidsmiddel zelf. Dit kan vervolgens er voor zorgen dat het mis gaat met de werking van dat arbeidsmiddel. De arbeidsveiligheid kan dan in gevaar komen zonder dat hier een bewuste (kwaadwillende) actor achter zit.

5.3 Lerende organisatie

Duidelijk komt uit de interviews naar voren dat de kennis over bronnen waar informatie te vinden is, beperkt is. Bronnen als ICSCERT in de versus, de scadasec mailing list, de SCADA/ICS factsheets van het Nationaal Cyber Security Centrum [29], de trendanalyses in bijvoorbeeld het jaarlijks verschijnende Cyber Security Beeld Nederland (CSBN) en de (vitale) sector-gerichte Information Sharing and Analysis Centres (ISACS)[30] kunnen meer in voetlicht te worden gebracht.

[29] https://www.ncsc.nl/actueel/dossiers/ics-scada.html
[30] Zie o.a. www.ncsc.nl

Veel onderzoek in andere domeinen, bijvoorbeeld over motieven van hackers, is ook bruikbaar voor het beoordelen van risico's van cybersecurity voor arbeidsveiligheid.
Cross domain leren levert belangrijke informatie op. Op dit moment wordt er nog vaak gezegd '*maar hier gebeurt niks'*. Echter, als je wacht tot er iets gebeurt ben je meer kwijt (geld, imago, tijd) dan wanneer je nu gestructureerd en integraal over risico's gaat denken. Een dergelijke opstelling zorgt er ook voor dat incidenten 'onder de mat geschoven worden' en pas aan het licht komen als er ernstige incidenten optreden. In de safety-gerelateerde wereld betreft dit zwaar risico voor 'lijf en leden'.
Een ander voorbeeld is. Je kan wel leren uit andere 'fouten' bijv. de storing bij Vodafone of T-Mobile waar een brandje in één apparaat het hele landelijke netwerk platlegde. Omdat er geen overeenkomst was met andere providers om op hun netwerk te mogen meeliften heeft dit veel tijd, geld en imagoschade gekost.

5.4 Cultuur en gedrag

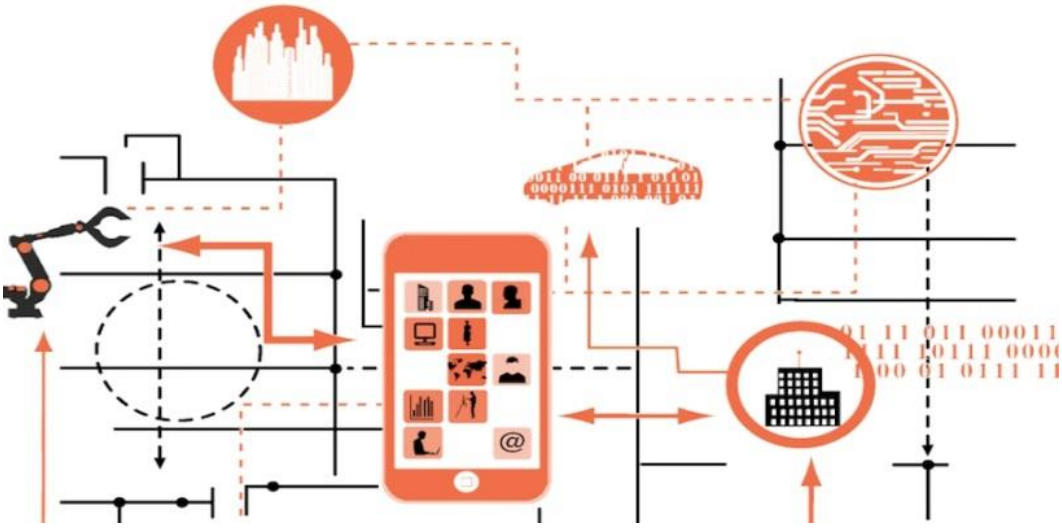
Naast de invalshoek structuur en leren is tot slot de invalshoek cultuur aan de orde. De gewenste organisatiecultuur zal mede belicht moeten worden vanuit de invalshoek cybersecurity en arbeidsveiligheid tezamen. Met name de uiting daarvan in gedrag is het bewijs van een safe en secure cultuur.
De toenemende verbondenheid van arbeidsmiddelen met het internet brengt nieuw gedrag met zich mee wat bewust en onbewust tot risico's kan leiden:

- Het toepassen van "Bring Your Own Device" in de bedrijfsomgeving leidt tot nieuwe kwetsbaarheden
- Via de privé en bedrijfssfeer zijn naast phishing, verschillende andere aanvalsvectoren te onderkennen. [31]
- Niet nieuw maar door toegenomen connectiviteit hebben "ontevreden" medewerkers nieuwe mogelijkheden om grote schade aan te richten.

[31] Zie Luiijf, H.A.M., & te Paske, B.J. (2015). Cyber Security of Industrial Control Systems: https://www.tno.nl/ics-security/ voor een overzicht.

6 Synthese en aanbevelingen

In dit project kwam duidelijk naar voren dat hoewel dit een belangrijk onderwerp is, er nog niet veel structureel aan gewerkt wordt, noch nationaal, noch internationaal. In dit oogpunt is dit rapport een eerste in zijn soort. Juist nu is echter wel een belangrijke window of opportunity. The internet of things (IoT) golf is nu aan het ontstaan. Dat is dus nog een ontwikkeling die beïnvloed kan worden. Wij zijn frontrunners, komt uit veel interviews naar voren. Wordt nog weinig mee gedaan, nog niet veel over nagedacht. Hieronder geven wij onze synthese van de gegevens die we binnen dit project hebben verzameld samen met onze aanbeveling naar organisaties toe.
Het is niet te ontkennen dat de introductie van nieuwe ICT en koppeling van en tussen arbeidsmiddelen via het internet of telecommunicatie heeft de industrie grote stappen kunnen zetten in termen van efficiëntie. Toch is uit de interviews en workshop gebleken dat deze ontwikkelingen ook veel nieuwe dreigingen en kwetsbaarheden met zich meebrengen. Wij stellen het volgende als generieke definitie voor: *de mogelijkheid dat een of meerdere individuen ongeautoriseerde toegang krijgen tot bedrijfssystemen in de arbeidsomgeving en deze dusdanig verstoren dat er (potentieel) een arbeidsonveilige situatie optreedt.* Deze definitie is alomvattend: het kan zowel toegang betekenen van kwaadwillende hackers of malware, alsmede onbedoelde acties van een onderhoudsmonteur.



Figuur 3.The internet of Things zorgt voor een complexe verbondenheid tussen systemen en processen.[32]

Een belangrijke onderliggende factor die bijdraagt aan dit risico is de toenemende complexiteit als gevolg van IoT: dat wil zeggen, dat alles via netwerken met elkaar verbonden wordt (figuur 1). De schaal waar dit op gebeurt wordt, niet altijd beseft, omdat de achterliggende ICS niet altijd zichtbaar zijn. Het wordt gepresenteerd in termen van functies en mogelijkheden, zonder het directe besef dat dit ook achter

[32] Bloem, van Doorn, Duivestein, van Manen, van Ommeren (2013). Things: Internet of Business Opportunities. *VINT research report 1 of 4. http://www.fr.sogeti.com/globalassets/global/downloads/reports/vint-research-1-things-internet-of-business-opportunities.pdf*

deuren voor externe partijen (hackers) creëert[33]. Systeemprocessen kunnen opeens benaderd worden op een schaal Hieronder presenteren wij de belangrijkste risico's, kwetsbaarheden, en beheersmaatregelen die uit het project naar voren komen, de belangrijkste (actoren en) informatiebronnen voor bedrijven die aan preventie willen werken, en enkele concrete stappen om het risico aan te pakken vanuit bedrijfsperspectief. In appendix A is deze informatie samengevat in een kenniskaart.

6.1 Risico's

- Procesverstoringen bedreigen business continuity en beheerste productie.
- Medewerkers met letsel of dood ten gevolge van een arbeidsonveilige situatie door onbedoelde cyberverstoring of door hacking, malware of signaalverstoring, en daarbij komende financiële schade (e.g., ziektekosten en verzuim).
- Via chantage kan toegang tot proces en machines worden afgedwongen (e.g., fysieke bedreiging medewerkers of creëren van access point via 'phishing').
- Imago schade ten gevolge van voor publiek zichtbare incidenten (e.g., waarbij slachtoffers te betreuren zijn).

6.2 Kwetsbaarheden

Tabel 6. Overzicht kwetsbaarheden met toelichting.

Kwetsbaarheden	Toelichting
Communicatie	Bestuurders en technici spreken een andere taal. Hierdoor is het gedeelde inzicht en onderlinge communicatie tussen (ICT) security en operationeel personeel of veiligheidskundige over (cyber)technische risicoaspecten voor arbeidsveiligheid, als die er al is, vaak beperkt.
Kosten cybersecurity	De huidige concurrentiemarkt zorgt er voor dat met name het MKB nauwelijks investeert in cybersecurity in relatie tot arbeidsveiligheid en in plaats daarvan focust op functionaliteit (i.e., men wil een kraan die een container van A naar B kan verplaatsen, de cybersecurity is van ondergeschikt belang). Hetzelfde geldt voor fabrikanten en systeemintegratoren. Onderliggende factor is dat er nog maar weinig (publiekelijk breed bekende) incidenten zijn geweest met impact op de veiligheid van medewerkers en personen die de urgentie van investeringen in cybersecurity vergroten.
Snelle ontwikkelingen	Snelle technologische ontwikkelingen zorgen er voor dat programmatuur en cybersecurity de veiligheid van arbeidsmiddelen snel veroudert. Daarnaast neemt de complexiteit toe van ICT-gecontroleerde en bestuurde (24/7) processen.

[33] http://link.springer.com/chapter/10.1007%2F978-3-319-24255-2_2

Kwetsbaarheden	Toelichting
Achterhaald risicomanagement[34]	Ondanks de toenemende verbondenheid van systemen en processen, wordt nog te vaak geprobeerd om vanuit gescheiden invalshoeken naar risicofactoren te kijken (e.g., onderhoud versus uitvoering, safety versus security, of staf versus management). Dit is echter een verouderd paradigma. Een integraal risicomanagement is noodzakelijk. Ook ontbreekt vaak een bewustzijn en overzicht van de samenhang van de technische systemen alsook de actoren die bij het bedreigen/zorgen voor veilige oplossingen een rol spelen.
Ontbreken cyber-situational awareness	De cyber-situational awareness is nog betrekkelijk laag bij de meeste organisaties. Daarnaast is er schroom incidenten te delen met anderen om ervan te kunnen leren. Per 1 januari 2016 gaat een wetsvoorstel in die bedrijven verplicht stelt om datalekken te melden.
Onbewust onbekwaam	Onbewust onbekwame medewerkers die onbewust invloed uitoefenen op machine programmatuur en daarmee geïmplementeerde beheersmaatregelen teniet doen. Huidige risicoanalyses nemen deze factor vaak niet mee en gaan uit van de juiste intentie in handelen van hun medewerkers.

Beheersmaatregelenwaar tot nu toe nog nooit rekening mee is gehouden, en waarvan het besef nog maar beperkt aanwezig lijkt te zijn[35].
De complexiteit van de toenemende verbondenheid van systemen, processen, en bijvoorbeeld het internet, maakt het ook moeilijker voor medewerkers die hiermee moeten werken om het overzicht te houden. De als resultaat onbewust onbekwame acties kunnen verschillende onveilige situaties creëren. Bijvoorbeeld door achterdeuren te openen voor hackers via malware, of direct door onbewust een systeemverstoring te creëren omdat niet alle consequenties van een handeling overzien worden op het gehele netwerk.

Voor alle actoren in de levenscyclus worden taken onderkend. Vanuit preventief oogpunt voor een veilig toepassing van arbeidsmiddelen ligt daarbij een belangrijke rol bij de producenten. Al in het onderwerp maar ook in de productie en installatiefase is het van belang met de in dit rapport onderkende dreigingen en kwetsbaarheden rekening te houden. Waar dit niet in de techniek van het arbeidsmiddel te realiseren valt is het van belang dat de eigenaar, beheerder en gebruiker van het arbeidsmiddel over de onderkende kwetsbaarheden wordt geïnformeerd en hoe die beheersbaar zijn. Hiertoe kunnen, in analogie met

[34] Ook in andere domeinen wordt deze conclusie getrokken: "Gap 7: Lack of advanced risk assessment tools Risk assessment methodologies that can deal with multiple networked stakeholders working in collaboration need to be developed. This requires a different mind-set for existing risk management approaches, which often begin by scoping a system (i.e. defining its borders) prior to a risk assessment based on the individual elements. However, in interconnected systems this clear border does not exist. To address this gap we need to redesign risk management systems/approaches so that they operate from a stakeholder perspective rather than border perspective."
https://www.enisa.europa.eu/activities/Resilience-and-CIIP/smart-infrastructures/intelligent-public-transport/good-practices-recommendations

[35] Een relatief onschuldig voorbeeld, dat wel tekenend is voor de schaal waarop systemen met het internet worden verbonden, is dat er nu zelfs Barbecues zijn die gehackt kunnen worden: http://news.softpedia.com/news/barbeques-are-now-hackable-thanks-to-ever-evolving-technology-497418.shtml

traditionele noodscenario's, ook worden gerekend what if scenario's en het beheersen daarvan

- Fail safe/safe fail
- Damage tolerant
- Anticiperende en snelle response bij vermoeden van dreiging.

Waar mogelijk zou daartoe al in het ontwerp rekening kunnen worden gehouden.

6.3

Tabel 7. Maatregelen om het risico te minimaliseren

Levenscylus	Beheersmaatregel
Ontwerp	✓ Intrinsiek veilig ontwerp (gestuurd door technische standaarden). ✓ Integrale veiligheidsrisico -inventarisatie en -evaluatie over de gehele levenscyclus van het arbeidsmiddel. ✓ Ontwerpen gericht op fail safe/safe fail en damage control bij blootstelling aan cybercrime.
Productie, leverantie en installatie	✓ Leveranciers en dienstverleners (bijvoorbeeld voor onderhoud)leveren secure-out-of-the-box producten. ✓ Systeemintegratoren en installateurs leveren Industrial Control Systems (ICS) integraal veilig op. ✓ Cybersecurity is integraal deel van het verwervingsproces en de testfase van producten en diensten. ✓ De beveiliging van (informatie-) systemen of componenten contractueel vastleggen met (toe)leveranciers.
Gebruik	✓ Integraal en multidisciplinair risicomanagement. ✓ Veiligheidsmanagement en veiligheidscultuur mede richten op cybersecurity ✓ Arbeidsveiligheidsgedragsregels/protocollen omtrent omgang met ICS en andere interne systemen met cybersecurity aspecten aanvullen ✓ Cybersecurity procedures om ICS en netwerken veilig te houden. ✓ Hardening van ICS en minimalisatie koppelvlakken. ✓ Voorlichting risico's en gewenst gedrag onder (tijdelijke) medewerkers en leveranciers/contractors ✓ (Bij)scholing eigen personeel voor omgang met ICS. ✓ Toezicht op ICT-netwerkanomalieën (bijv. auditing). ✓ Ontwikkel beleid voor het intern en extern delen van cybersecurity-gerelateerde informatie. ✓ Periodiek uitvoeren penetratietesten met betrekking tot cybersecurity van arbeidsmiddelen (bijv. door white hackers). ✓ Arbeidsveiligheidsgedragsregels/protocollen omtrent omgang met ICS en andere interne systemen met cybersecurity aspecten aanvullen ✓ Screening eigen personeel ✓ Integrale aanpak incidentmanagement (safety en security). ✓ Bedrijfs(nood)organisatie ook inrichten op anticiperende en snelle response bij reële cybercrime dreiging
Onderhoud	✓ Onderhoud(services) mede inrichten op beheersing vanuit integrale veiligheid ✓ Malware detectiebeleid en -uitvoering: zorgen voor tijdige actuele malware-detectie. ✓ Signaleren van pogingen tot inbraak in systemen tijdens onderhoud. ✓ Patchbeleid en -uitvoering: tijdig patchen. (bijv. updates op beheersbare schaal uitvoeren) ✓ Controle op toegang en werkzaamheden eigen medewerkers en derde partijen bij onderhoud. ✓ Testen / voorkomen nieuwe beveiligingslekken door installatie nieuwe componenten.
Vernieuwing	✓ Zorgen voor een management of change proces gebaseerd op integrale veiligheid. ✓ Zorgen voor toekomstige oplossingen: research en ontwikkeling stimuleren t.b.v. vernieuwing van de huidige stand van wetenschap en techniek op het gebied van cybersecurity. ✓ Testen / voorkomen nieuwe beveiligingslekken door binnenbrengen nieuwe (functionaliteiten van) arbeidsmiddelen.
Afvoeren	✓ Verwijderen gevoelige (configuratie)informatie en inschakelen betrouwbare partijen. ✓ Verouderde of niet meer geschikte installaties en systemen onbruikbaar maken

6.4 Sleutelspelers in kennisdeling en bewustwording

- De uitvoerenden betrokkenen bij cybersecurity en veiligheid in de levenscyclus van arbeidsmiddelen
- Kennisinstituten en kennispunten (bijv. ncsc.nl)
- Verzekeraars
- Brancheverenigingen (informatie delen, kennis ontwikkelen, richtlijnen ontwikkelen)
- Overheden en normalisatie-instituten ((inter)nationale regelgeving, normkaders)

6.5 Aanbevelingen voor bedrijven en organisaties

- Zorg voor coördinatie van integrale veiligheid en cybersecurity op boardroomniveau in één portefeuille bijvoorbeeld op topniveau bij een Chief Information Officer of CEO.
- Zorg voor een multidisciplinair team dat het cybersecurity-gerelateerde risico voor arbeidsveiligheid integraal evalueert en daarin de human factors nadrukkelijk meeneemt, incidenten waarneemt en zo nodig noodmaatregelen kan treffen.
- Analyseer waar in het hier en nu netwerk koppelingen tussen arbeidsmiddelen en “risicovolle” interne omgevingen en buitenwerelden zijn.
- Zorg voor het delen van kennis, wissel good practices uit en waarschuw elkaar over incidenten en dreigingen.[36]
- Anticipeer op veranderingen van arbeidsmiddelen en de koppeling van arbeidsmiddelen met ICS en (publieke) netwerken, door middel van integrale veiligheidsanalyses en producteisen.
- Neem veiligheid en cybersecurity mee in ontwerp, systeemintegratie en levering of het geven van opdrachten hiertoe zoals het uitvoeren van onderhoud. Neem daarbij de onderlinge samenhang (bijvoorbeeld systeemarchitectuur of relevante actoren) in acht.
- Zorg voor bewustwording bij alle betrokkenen van het belang van een integrale behandeling van arbeidsveiligheid en cybersecurity. School mensen (in management, staf en uitvoering) zo nodig bij.[37]

[36] Per 01-01-2016 is de meldplicht Datalekken ingegaan. Zie voor meer informatie o.a.: http://www.cip-overheid.nl/wp-content/uploads/2015/11/20151130_Meldplicht_v2_0_def01.11.pdf

[37] Zie een ander TNO rapport voor meer informatie over kwalificatie veroudering. Dit rapport is hier te vinden: https://www.tno.nl/media/1305/kwalificatieveroudering_in_nederland_tno_r13017.pdf

7 Ondertekening

Utrecht, 18 februari 2016

TNO

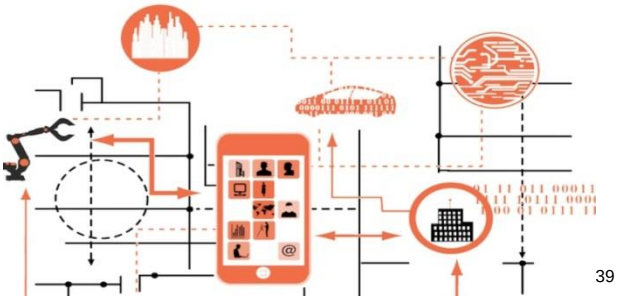
Drs. H.C. Borst
Researchmanager

Ir J.K.J. van der Vorm
Projectleider

A Kenniskaart

Opzet veiligheidskaart Veilige Arbeidsmiddelen en Cybersecurity[38]

"De werkgever zorgt voor de veiligheid en de gezondheid van de werknemers inzake alle met de arbeid verbonden aspecten. Heeft u uw cybersecurity ook geregeld voor computergestuurde arbeidsmiddelen?"



39

Dankzij de introductie van ICT-systemen ingebed in de besturing van arbeidsmiddelen via lokale netwerken en publieke netwerken zoals het internet hebben bedrijven en organisaties grote stappen kunnen zetten in termen van efficiëntie. Deze ontwikkelingen brengen echter ook nieuwe dreigingen en kwetsbaarheden. Vooral de mogelijkheid dat individuen of malware ook ongeautoriseerd toegang krijgen tot bedrijfssystemen en netwerken in de arbeidsomgeving en deze dusdanig ongeautoriseerd verstoren dat er een arbeidsonveilige situatie optreedt. Ook wordt de complexiteit vaak onderschat en wordt er daardoor onvoldoende geanticipeerd op mogelijke onverwachte storingen als gevolg van die complexiteit. Toch wordt er in veel bedrijven en organisaties dit risico nog niet onderkend. Gezien de snelle technologische ontwikkelingen en de toenemende verbondenheid van systemen en processen is het echter een kwestie van wachten tot het een keer goed fout gaat. Voorkomen is beter dan genezen. U, als een van de actoren in de levenscyclus van arbeidsmiddelen, bent aan zet!

Wat zijn de risico's voor bedrijven en organisaties?

- Procesverstoringen bedreigen business continuity en beheerste productie.
- Medewerkers met letsel of dood ten gevolge van een arbeidsonveilige situatie door onbedoelde cyberverstoring of door hacking, malware of signaalverstoring, en daarbij komende financiële schade (e.g., ziektekosten en verzuim).
- Via chantage kan toegang tot proces en machines worden afgedwongen (e.g., fysieke bedreiging medewerkers of creëren van access point via 'phishing').
- Imago schade ten gevolge van voor publiek zichtbare incidenten (e.g., waarbij slachtoffers te betreuren zijn).

[38] Deze kenniskaart wordt separaat en in eigen opmaak gepubliceerd

[39] Bron Plaatje: Bloem, van Doorn, Duivestein, van Manen, van Ommeren (2013). Things: Internet of Business Opportunities. *VINT research report 1 of 4. http://www.fr.sogeti.com/globalassets/global/downloads/reports/vint-research-1-things-internet-of-business-opportunities.pdf*

Tabel 1. Wat zijn kwetsbaarheden die de kans op het risico vergroten?

Kwetsbaarheden	Toelichting
Communicatie	Bestuurders en technici spreken een andere taal. Hierdoor is het gedeelde inzicht en onderlinge communicatie tussen (ICT) security en operationeel personeel of veiligheidskundige over (cyber)technische risicoaspecten voor arbeidsveiligheid, als die er al is, vaak beperkt.
Kosten cybersecurity	De huidige concurrentiemarkt zorgt er voor dat met name het MKB nauwelijks investeert in cybersecurity in relatie tot arbeidsveiligheid en in plaats daarvan focust op functionaliteit (i.e., men wil een kraan die een container van A naar B kan verplaatsen, de cybersecurity is van ondergeschikt belang). Hetzelfde geldt voor fabrikanten en systeemintegratoren. Onderliggende factor is dat er nog maar weinig (publiekelijk breed bekende) incidenten zijn geweest met impact op de veiligheid van medewerkers en personen die de urgentie van investeringen in cybersecurity vergroten.
Snelle ontwikkelingen	Snelle technologische ontwikkelingen zorgen er voor dat programmatuur en cybersecurity de veiligheid van arbeidsmiddelen snel veroudert. Daarnaast neemt de complexiteit toe van ICT-gecontroleerde en bestuurde (24/7) processen.
Achterhaald risicomanagement	Ondanks de toenemende verbondenheid van systemen en processen, wordt nog te vaak geprobeerd om vanuit gescheiden invalshoeken naar risicofactoren te kijken (e.g., onderhoud versus uitvoering, safety versus security, of staf versus management). Dit is echter een verouderd paradigma. Een integraal risicomanagement is noodzakelijk. Ook ontbreekt vaak een bewustzijn en overzicht van de samenhang van de technische systemen alsook de actoren die bij het bedreigen/zorgen voor veilige oplossingen een rol spelen.
Ontbreken cyber-situational awareness	De cyber-situational awareness is nog betrekkelijk laag bij de meeste organisaties. Daarnaast is er schroom incidenten te delen met anderen om ervan te kunnen leren. Per 1 januari 2016 gaat een wetsvoorstel in die bedrijven verplicht stelt om datalekken te melden.
Onbewust onbekwaam	Onbewust onbekwame medewerkers die onbewust invloed uitoefenen op machine programmatuur en daarmee geïmplementeerde beheersmaatregelen teniet doen. Huidige risicoanalyses nemen deze factor vaak niet mee en gaan uit van de juiste intentie in handelen van hun medewerkers.

Tabel 3. Maatregelen om het risico te minimaliseren

Levenscylus	Beheersmaatregel
Ontwerp	✓ Intrinsiek veilig ontwerp (gestuurd door technische standaarden). ✓ Integrale veiligheidsrisico -inventarisatie en -evaluatie over de gehele levenscyclus van het arbeidsmiddel. ✓ Ontwerpen gericht op fail safe/safe fail en damage control bij blootstelling aan cybercrime.
Productie, leverantie en installatie	✓ Leveranciers en dienstverleners (bijvoorbeeld voor onderhoud)leveren secure-out-of-the-box producten. ✓ Systeemintegratoren en installateurs leveren Industrial Control Systems (ICS) integraal veilig op. ✓ Cybersecurity is integraal deel van het verwervingsproces en de testfase van producten en diensten. ✓ De beveiliging van (informatie-) systemen of componenten contractueel vastleggen met (toe)leveranciers.
Gebruik	✓ Integraal en multidisciplinair risicomanagement.

Levenscylus	Beheersmaatregel
Gebruik	✓ Ontwikkel beleid voor het intern en extern delen van cybersecurity-gerelateerde informatie. ✓ Arbeidsveiligheidsgedragsregels/protocollen omtrent omgang met ICS en andere interne systemen met cybersecurity aspecten aanvullen ✓ Screening eigen personeel ✓ Integrale aanpak incidentmanagement (safety en security) ✓ Bedrijfs(nood)organisatie ook inrichten op anticiperende en snelle response bij cybercrime dreigingen.
Onderhoud	✓ Onderhoud(services) mede inrichten op beheersing vanuit integrale veiligheid ✓ Malware detectiebeleid en -uitvoering: zorgen voor tijdige actuele malware-detectie. ✓ Signaleren van pogingen tot inbraak in systemen tijdens onderhoud. ✓ Patchbeleid en -uitvoering: tijdig patchen. (bijv. updates op beheersbare schaal uitvoeren) ✓ Controle op toegang en werkzaamheden eigen medewerkers en derde partijen bij onderhoud. ✓ Testen / voorkomen nieuwe beveiligingslekken door installatie nieuwe componenten.

Levenscylus	Beheersmaatregel
	✓ Veiligheidsmanagement en veiligheidscultuur mede richten op cybersecurity ✓ Arbeidsveiligheidsgedragsregels/protocollen omtrent omgang met ICS en andere interne systemen met cybersecurity aspecten aanvullen ✓ Cybersecurity procedures om ICS en netwerken veilig te houden. ✓ Hardening van ICS en minimalisatie koppelvlakken. ✓ Voorlichting risico's en gewenst gedrag onder (tijdelijke) medewerkers en leveranciers/contractors ✓ (Bij)scholing personeel voor omgang met ICS. ✓ Toezicht op ICT-netwerkanomalieën (bijv. auditing).

Levenscylus	Beheersmaatregel
Vernieuwing	✓ Zorgen voor een management of change proces gebaseerd op integrale veiligheid. ✓ Zorgen voor toekomstige oplossingen: research en ontwikkeling stimuleren t.b.v. vernieuwing van de huidige stand van wetenschap en techniek op het gebied van cybersecurity. ✓ Testen / voorkomen nieuwe beveiligingslekken door binnenbrengen nieuwe (functionaliteiten van) arbeidsmiddelen.
Afvoeren	✓ Verwijderen gevoelige (configuratie)informatie en inschakelen betrouwbare partijen. ✓ Verouderde of niet meer geschikte installaties of systemen onbruikbaar maken

Belangrijke (actoren en) informatiebronnen voor preventie

- De uitvoerenden betrokkenen bij cybersecurity en veiligheid in de levenscyclus van arbeidsmiddelen
- Kennisinstituten en kennispunten (bijv. ncsc.nl)
- Verzekeraars
- Brancheverenigingen (informatie delen, kennis ontwikkelen, richtlijnen ontwikkelen)
- Overheden en normalisatie-instituten ((inter)nationale regelgeving, normkaders)

Stappen om het risico aan te pakken vanuit bedrijfsperspectief

- Zorg voor coördinatie van integrale veiligheid en cybersecurity op boardroomniveau in één portefeuille bijvoorbeeld op topniveau bij een Chief Information Officer of CEO.
- Zorg voor een multidisciplinair team dat het cybersecurity-gerelateerde risico voor arbeidsveiligheid integraal evalueert en daarin de human factors nadrukkelijk meeneemt, incidenten waarneemt en zo nodig noodmaatregelen kan treffen.
- Analyseer waar in het hier en nu netwerk koppelingen tussen arbeidsmiddelen en "risicovolle" interne omgevingen en buitenwerelden zijn.
- Zorg voor het delen van kennis, wissel good practices uit en waarschuw elkaar over incidenten en dreigingen.
- Anticipeer op veranderingen van arbeidsmiddelen en de koppeling van arbeidsmiddelen met ICS en (publieke) netwerken, door middel van integrale veiligheidsanalyses en producteisen.
- Neem veiligheid en cybersecurity mee in ontwerp, systeemintegratie en levering of het geven van opdrachten hiertoe zoals het uitvoeren van onderhoud. Neem daarbij de onderlinge samenhang (bijvoorbeeld systeemarchitectuur of relevante actoren) in acht.
- Zorg voor bewustwording bij alle betrokkenen van het belang van een integrale behandeling van arbeidsveiligheid en cybersecurity. School mensen (in management, staf en uitvoering) zo nodig bij.