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 R10643

Opkomend risico voor arbeidsveiligheid door inzet van robots op de werkvloer

Datum	28 juli 2016
Auteurs	Wouter Steijn; Eric Luiijf; Dolf van der Beek (contactpersoon)
Exemplaarnummer	
Oplage	
Aantal pagina's	54
Aantal bijlagen	2
Opdrachtgever	Ministerie van Sociale Zaken en Werkgelegenheid
Projectnaam	Opkomend risico voor arbeidsveiligheid door inzet van robots op de werkvloer
Projectnummer	060.20710/01.06

Alle rechten voorbehouden.
Niets uit deze uitgave mag worden vermenigvuldigd en/of openbaar gemaakt door middel van druk, fotokopie, microfilm of op welke andere wijze dan ook, zonder voorafgaande toestemming van TNO.

Indien dit rapport in opdracht werd uitgebracht, wordt voor de rechten en verplichtingen van opdrachtgever en opdrachtnemer verwezen naar de Algemene Voorwaarden voor opdrachten aan TNO, dan wel de betreffende terzake tussen de partijen gesloten overeenkomst.
Het ter inzage geven van het TNO-rapport aan direct belanghebbenden is toegestaan.

© 2016 TNO

Inhoudsopgave

Lijst met afkortingen

AGV	Automated Guided Vehicle
CEN	European Committee for Standardization
CENELEC	European Committee for Electrotechnical Standardization
ICS (1)	Industriële Controle Systemen
ICS (2)	International Classification for Standards
ICT	Informatie- en Communicatie Technologie
IoT	Internet of Things
ISO	International Organization for Standardization
LoRa	Long Range
LPWAN	Low Power Wide Area Network
MANET	Mobile Ad hoc NETwork
NEN	Nederlands normalisatie-instituut
OSHA	Occupational Safety & Health Administration
PPE	Personal Protective Equipment
RAN	Robot Area Network
RUR	Rossums Universele Robots
SZW	Het Ministerie van Sociale Zaken en Werkgelegenheid
WiFi	Draadloos Internet

1 Inleiding

Al decennia lang spreken robots tot de verbeelding in toekomstvisioenen in films en boeken. Karel Čapek schreef al in 1920 een toneelstuk genaamd RUR (Rossums Universele Robots). De eerste echte robot 'Gargantuan' werd in de periode 1935 tot 1937 geconstrueerd. Deze was volledig opgebouwd uit Meccano® [1]. De huidige industriële robots lijken nog veel op de versie die in 1961 in de autoproductielijnen van General Motors zijn geïntroduceerd[2]. Robots zijn in de afgelopen vijftig jaar wel veel sneller en nauwkeuriger geworden, maar het blijven nu nog vaak locatie- of rail gebonden machines die automatisch een (enkele) taak uitvoeren binnen een vastgestelde gevarenzone of binnen een veiligheidskooi. In het kader op de volgende pagina worden enkele voorbeelden gegeven van de toepassing van hedendaagse industriële robots in verschillende sectoren. Deze robots staan nog ver weg van de intelligente en autonome robots zoals in sciencefiction boeken en films worden neergezet. Door deze verhalen is de beeldvorming van robots voor veel personen gericht op machines met een menselijke vorm, die zich zichzelf kunnen voortbewegen, met personen om kunnen gaan en op hun omgeving kunnen reageren.

1.1 Noodzaak van zicht op nieuwe risico's

Ondanks bovenstaande beperkingen introduceren de huidige industriële robots nieuwe risico's op de werkvloer ondanks de definiëring van veiligheidszones of kooien. Dit werd afgelopen jaar opnieuw benadrukt na een dodelijk ongeluk waarbij een werknemer door een robot werd doodgedrukt[3]. Aangezien industriële robots in toenemende mate in gebruik worden genomen in de land- en tuinbouw, maakindustrie en distributiemagazijnen kunnen dit soort arbeidsincidenten zich in de toekomst vaker gaan voordoen. Verder zal de programmering van industriële robots complexer worden naarmate ze meer of complexere taken gaan uitvoeren. Daarnaast staat de ontwikkeling van autonoom voortbewegende robots die zijn omgeving 'ziet' en daarop reageert niet stil[4]. Het is dus voorstelbaar dat in de nabije toekomst personen ook met autonome robots zullen gaan samenwerken in omgevingen die niet meer tot een vaste locatie of kooi beperkt zal zijn. Ook zullen personen en autonome robots zich samen door dezelfde ruimten bewegen. Ten gevolge zal het risico op letsel als direct gevolg van een botsing tussen mens en robot groter worden, maar ook indirecte arbeidsveiligheidsrisico's zullen toenemen als gevolg van de apparatuur die robots mogelijk meedragen die gevaarlijk zijn voor medewerkers in hun omgeving (bijv. lasers, stralingsbronnen, laselektroden, en mechanisch apparatuur).

---

[1] An Automatic Block-Setting Crane"(1938). *Meccano Magazine, 23*(3): 172. http://www.mecademic.com/references/MeccanoMagazine1938.pdf

[2] Martijn Wisse (2015). De robot de baas: De toekomst van werk in het tweede machinetijdperk. *Wetenschappelijke raad voor het regeringsbeleid. P 73.*

[3] http://www.automobielmanagement.nl/nieuws/overige/nid22164-robot-drukt-arbeider-dood-in-vw-fabriek.html

[4] Zo experimenteerde Schiphol onlangs met een robot die verdwaalde mensen kan begeleiden: http://www.telegraaf.nl/digitaal/24800958/__Robot_wijst_de_weg_op_Schiphol__.html

Het is belangrijk om bij deze trend vooruit te kijken en de machineveiligheid van morgen te definiëren zodat een robot al in het ontwerp en de ontwikkeling proactief intrinsiek veilig kan worden gemaakt. Denk bijvoorbeeld aan de drie wetten van Asimov[5] waar een robot zich aan zou moeten houden. De vraag is of naleving van die wetten voldoende is om de veiligheid van alle betrokkenen te garanderen? Maar ook morele dillema's kunnen in de toekomst een rol gaan spelen: moet een robot de voorkeur geven aan een handeling om de kans op een catastrofaal falen te minimaliseren boven de veiligheid van de individuele medewerker die toevallig in de buurt is?

Kader "Voorbeelden van toepassingen van hedendaagse robots op de werkvloer"

Assemblagelijnen

Lasrobot

Landbouwrobot

Zorgrobot

Bron plaatjes (beginnend linksboven met de klok mee). Gevonden d.d. 26-05-2016:

- https://www.mechatronicamachinebouw.nl/fileadmin/uploads_redactie_mm/images/2012/MM07/Rethink_Robotics_Baxter.jpg
- http://www.metalservices.nl/images/metalservices//afbeeldingen/constructietechniek/robot.jpg
- http://www.robots.nu/assets/Robot-categorie/_resampled/resizedimage475458-Zorgrobot-robot-voor-zorgtaken.jpg
- http://www.smartbot.eu/en/wp-content/themes/z-responsive/img/content/magazines/Agrobot_magazine.pdf

Om het risico van robotisering voor de arbeidsveiligheid op de werkplek te beheersen zullen adequate wet- en regelgeving en normen moeten worden opgesteld, die mogelijk geïnspireerd zijn op de wetten van Asimov. Daarnaast

[5] *Eerste wet*: een robot mag een mens geen letsel toebrengen of door niet te handelen toestaan dat een mens letsel oploopt. *Tweede wet:* een robot moet de bevelen uitvoeren die hem door mensen worden gegeven, behalve als die opdrachten in strijd zijn met de Eerste Wet. *Derde wet:* een robot moet zijn eigen bestaan beschermen, voor zover die bescherming niet in strijd is met de eerste of tweede wet.

moeten concrete aanbevelingen voor het bedrijfsleven worden geformuleerd om dit arbeidsrisico te beperken. Met dit doel voor ogen heeft het Ministerie van Sociale Zaken en Werkgelegenheid (SZW) de volgende kennisvraag aan TNO voorgelegd:

Wat zijn de risico's van robotisering op de werkplek en welke beheersmaatregelen zijn denkbaar om het genoemde risico te beheersen?

Deze kennisvraag is opgepakt in het TNO kennisinvesteringsproject "Emerging risks". Dit project onderzoekt de potentiële gevolgen van toenemende robotisering op de werkplek en de daaraan gerelateerde risico's voor de veiligheid en gezondheid van personen. Doel is een basis te bieden voor de veilige inzet van robots in de werkomgeving van personen.

In de huidige wet- en regelgeving is over robots strikt gesproken nog niets opgenomen, dan wel conflicteert de wet- en regelgeving voor machineveiligheid bij strikte toepassing met het gebruik van (proces)automatisering. Rapportages in 2015[6] en de in dit rapport opgenomen analyses, conclusies en aanbevelingen leveren inzichten op die kunnen fungeren als aanhaakpunten voor wijzigingen op nationaal en Europees niveau, in dit geval van de Arbowet, de Europese machinerichtlijn[7] en dergelijke. Duidelijk zal zijn dat robots in de werkomgeving van werknemers (en bezoekers) aan een aantal basisprincipes van arbeidsveiligheid moeten voldoen. Bijvoorbeeld naar gelang de arbeidshygiënische strategie in de vorm van bronmaatregelen (o.a., elimineren en isoleren van gevaar), collectieve maatregelen (o.a., afschermen van een groep van gevaar), individuele maatregelen, of persoonlijke beschermingsmiddelen.

Ook normalisatie-instituten zoals NEN, CEN/CENELEC en ISO voorzien de komende jaren een grote impact door robotisering op standaardisering activiteiten. Dit zal gevolgen hebben op de verschillende Europese richtlijnen (bijv. richtlijn machines en richtlijn arbeidsmiddelen) en de daaraan gelieerde geharmoniseerde Europese normen. Dit rapport dient mede ter ondersteuning van het Ministerie SZW in het inzicht krijgen in het thema Robotica en Arbeidsomstandigheden en kan een bijdrage leveren aan bijvoorbeeld normalisatie-instituten zoals het NEN bij het opzetten van een nationale en internationale normalisatieagenda op dit terrein.

In dit rapport heeft TNO niet alleen gekeken naar robots zoals die nu worden ingezet, maar ook naar de ontwikkeling en mogelijkheden van industriële robots in de nabije toekomst. Als industriële robots autonomer bewegen over de werkvloer waar zich ook personen bevinden zal het definiëren van veiligheidszones of het plaatsen van veiligheidskooien niet meer eenduidig kunnen. Maar ook andere kwetsbaarheden kunnen voortkomen uit de samenwerking van mens en robot. Industriële robots worden vaak ingezet bij zwaar en gevaarlijk werk en zijn daardoor vaak per definitie zelf ook zwaar en gevaarlijk. Dit bijvoorbeeld in contrast met zorgrobots die erop worden gebouwd om veilig te zijn voor de mensen waar ze voor zorgen[8]. Daarnaast kan een robot gevaarlijke apparatuur met zich mee dragen die gevaarlijk kan zijn voor de mens en zelfs bij uitval van de robot nog steeds gevaar

---

[6] Steijn, W., Luiijf, H., Gallis, R., Opkomende risico's voor arbeidsveiligheid als gevolg van IT-koppelingen van en tussen arbeidsmiddelen, TNO rapport 2016 R10096.

[7] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:157:0024:0086:nl:PDF

[8] Bijvoorbeeld, de RIBA til-robot is gebouwd met zachte materialen om de personen die hij moet optillen niet te bezeren: https://www.youtube.com/watch?v=wOzw71j4b78

op kan leveren omdat die apparatuur (bijvoorbeeld laser, laselektroden) niet spanningsvrij is.

TNO zal hieronder een eerste stap zetten in het beantwoorden van de bovenstaande kennisvraag van het Ministerie van SZW door middel van het uitvoeren van een inventarisatie van gevaren en bedreigingen en het in kaart brengen van mogelijke beschermingsmaatregelen ter voorkoming aan de bron of mitigatie van het risico. Hierbij richten wij vooral op het arbeidsveiligheidsrisico van verwonding of overlijden als gevolg van een incident met een of meer personen en een robot op de werkvloer. In aansluiting op bovenstaande kennisvraag wordt in dit rapport de volgende onderzoeksvraag uitgewerkt:

Welke beheersmaatregelen kunnen worden aangedragen om kwetsbaarheden te minimaliseren die zich nu en in de nabije toekomst voordoen als gevolg van de inzet van robots op de werkvloer?

1.2 Leeswijzer

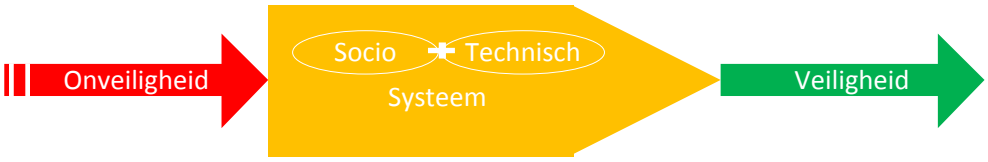
In dit rapport presenteren wij de gevolgde methodiek om deze onderzoeksvraag te beantwoorden en het resulterende overzicht van kwetsbaarheden en mogelijke beheersmaatregelen. In hoofdstuk 2 volgt uitleg over de gebruikte methodologie: een literatuur- en internetscan gevolgd door interviews en een workshop met experts vanuit verschillende domeinen. In hoofdstuk 3 definiëren wij de scope van dit rapport en definiëren wat wij in dit rapport onder robots verstaan. Hoofdstuk 4 presenteert de samenvatting van de resultaten van de gehouden interviews en de workshop. Hoofdstuk 5 geeft tot slot een overzicht van de uiteindelijke inventarisatie van kwetsbaarheden en mogelijke beheersmaatregelen voor bedrijven die robots bouwen en/of toepassen in de vorm van een kenniskaart.

2 Aanpak

Om de in hoofdstuk 1 gestelde 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 aan beheersmaatregelen om het risico voor arbeidsveiligheid als gevolg van toenemende robotisering op de werkvloer te minimaliseren. Met deze focus en de onderzoeksvraag in acht genomen is het volgende werkplan opgesteld:

1 Via een literatuur- en internetscan wordt de scope voor dit rapport afgebakend (zie hfst. 3) en een framework geselecteerd waarbinnen relevante gevaren en beheersmaatregelen kunnen worden beschreven.
2 Interviews worden gehouden met experts op gebied van veiligheid, robotontwikkeling en -gebruik. Een actoranalyse van relevante partijen voor deze interviews zal worden gedaan op basis van het framework dat in stap 1 is bepaald.
3 Een workshop wordt georganiseerd waarbij de resultaten uit de interviews worden teruggekoppeld aan de experts uit de praktijk om de resultaten verder aan te vullen en te verdiepen.
4 Eindrapportage in de vorm van een rapport en een kenniskaart.

Uitgangspunt in dit rapport is dat we het samenspel van mens en robot, gevaar en dreiging beschouwen als een socio-technisch systeem (zie figuur 1). We zullen dus beide aspecten benaderen en integreren in onze rapportage.



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

Verder gebruiken wij naast het traditionele *risico*begrip met betrekking tot de kans dat een potentieel gevaar tot een daadwerkelijk incident resulteert en de ernst van het letsel of de schade die dit tot gevolg heeft, ook de begrippen *dreiging* en *kwetsbaarheid*.

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 dat we gevaar door dreiging vervangen en kwetsbaarheden toevoegen als beïnvloeder van de kans dat een dreiging daadwerkelijk tot een incident leidt: 'de kans dat een potentiele dreiging resulteert in

[9] Adaptatie uit VROM (2008). *Handreiking Security Management*.

een daadwerkelijk incident geven de aanwezige kwetsbaarheden, en de ernst van het letsel of de schade die dit tot gevolg heeft.
Dreiging definiëren we hier in lijn met de definitie van de Belgische Privacy commissie[10] als "*elke onverwachte of onverhoopte gebeurtenis die aan een onderneming schade kan toebrengen*". Anders dan gevaar omvat het begrip dreiging ook het bewust toebrengen van schade en/of letsel. Denk hierbij bijvoorbeeld aan een hacker die bedrijfsprocessen ongeautoriseerd manipuleert, in vergelijking tot een onvoorziene softwarefout. Kwetsbaarheid kan in lijn daarmee worden gedefinieerd als "*een zwakte (binnen een organisatie of andere entiteit) die kan worden benut door een dreiging"* [11].

Het vaststellen van de definities voor deze begrippen is een dynamisch proces geweest tijdens dit project. Vandaar dat deze begrippen niet geheel eenduidig worden gebruikt bij de besproken interview- en workshopresultaten. Met dreiging wordt in dit kader vooral de gewilde onveiligheid benoemd als aanvulling op het concept arbeidsrisico dat vooral uitgaat van ongewilde onveiligheid.

2.1 Literatuur- en internetscan

Allereerst hebben wij een literatuur- en internetscan uitgevoerd. Het doel van deze scan was drieledig. Ten eerste wilden wij het onderwerp robotisering verkennen en het relevante gebied voor dit project afbakenen. Hiervan volgt een beschrijving in het volgende hoofdstuk. Ten tweede wilden wij de frameworks vinden op basis waarvan wij de dreigingen, kwetsbaarheden, en de beheersmaatregelen konden benaderen en betekenisvol categoriseren. Ten derde wilden wij een overzicht creëren van relevante partijen die interessant zouden zijn om te betrekken bij de interviews en workshop.

Hieronder lichten we kort de gekozen frameworks, de arbeidshygiënische strategie en de levenscyclus, toe en hoe wij met deze frameworks tot een actoranalyse zijn gekomen om relevante partijen te betrekken bij de interviews en de workshop.

2.1.1 Arbeidshygiënische strategie

De arbeidshygiënische strategie[12] maakt gebruik van de volgende hiërarchie aan mogelijke beheersmaatregelen zoals beschreven in de Arbowet[13]:

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

---

[10] Lexicon van de Belgische Commissie voor de bescherming van de persoonlijke levenssfeer (CBPL): https://www.privacycommission.be/nl/lexicon#letter_d

[11] 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

[12] Arboportaal: http://www.arboportaal.nl/onderwerpen/arbeidshygienische-strategie

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

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 en actoranalyse

In dit project hebben wij besloten om de nieuwe risicoaspecten te benaderen vanuit de levenscyclus van arbeidsmiddelen. Deze benadering houdt in dat we de toepassingen van arbeidsmiddelen benaderen van: a) ontwerp/engineering, b) productie/integrators/leverantie/installatie, c) gebruik, d) onderhoud, e) vernieuwing, tot en met f) afvoeren. Voor robots kunnen vergelijkbare fasen in de gehele levenscyclus van een robot worden onderkend. Naast deze fasen onderscheiden wij drie andere groepen aan partijen die een invloed hebben op ieder onderdeel van de bovenstaande levenscyclus:

1) Kennisontwikkelaars; bijv. universiteiten en andere kennisinstellingen.
2) Beleidsontwikkelaars, toezichthouders en normeringen; bijv. wet- en regelgevers, inspectiediensten of certificeerders, normalisatie-instituten.
3) Dienstverleners; bijv. verzekeraars of telecomproviders.

Om tot een overzicht van dreigingen en beheersmaatregelen te komen voor deze levensfasen moeten experts worden benaderd die in één of meer fases expertise hebben en of ontwikkelingen kunnen duiden. Tijdens de literatuurscan is een lijst opgesteld met potentiële interview- en workshopkandidaten voor ieder van de onderkende fasen.

2.2 Interviews

2.2.1 Interviewprotocol

De interviews waren semigestructureerd, dat wil zeggen dat er vooraf een protocol is opgesteld met vragen als handvat. Tijdens de interviews werd echter voornamelijk doorgevraagd naar datgene waar de geïnterviewde veel over kon vertellen. De interviews duurden ieder maximaal een half uur. In Appendix A staat het gehanteerde protocol. Vragen werden indien nodig aangepast aan de achtergrond van de geïnterviewde.

2.2.2 Deelnemers

Op basis van de literatuur- en internetscan is een actoranalyse gemaakt waarbij actoren uit de gehele productlevenscyclus zijn geselecteerd. Deze experts zijn vervolgens per mail uitgenodigd. Het doel was om tot maximaal tien deelnemers te komen. Een eerste reeks van 34 uitnodigen is verstuurd op 18 februari. Op 29 februari is een herinnering verstuurd en is een reeks uitnodigingen naar elf nieuwe experts gestuurd. In Tabel 1 is in een overzicht een anonieme beschrijving van de geïnterviewde deelnemers opgenomen.

Tabel 1. Achtergrond interviews

	Levenscyclus	Achtergrond/Type
1	Gebruiker	Levensmiddelenproducent
2	Gebruiker	Levensmiddelenproducent
3	Kennisinstituut	Interactieve robotica
4	Kennisinstituut	Agricultuur
5	Kennisinstituut	Exoskelet
6	Beleid	Ondernemersvereniging
7	Integrator	Logistiek
8	Beleid	Normontwikkeling
9	Leverancier	Industriële robots
10	Leverancier	Security robots

2.3 Workshop

Op 21 april 2016 is een workshop "*Mens-robot samenwerking: voorkom de botsing!; Wat is nodig om de arbeidsveiligheid van medewerkers te borgen*" gehouden. Experts zijn direct aan het eind van het interview uitgenodigd voor deze workshop, daarnaast is een uitnodiging verstuurd naar dezelfde actorenlijst die gebruikt is voor het samenstellen van de lijst met geïnterviewden.

Dit resulteerde uiteindelijk in zeven deelnemers naast drie TNO-projectleden. Helaas waren er een aantal personen verhinderd omdat er een conflicterend robot-event elders in Nederland plaatsvond en wij om logistieke redenen de workshop niet konden verplaatsen. Onder de zeven deelnemers waren vier eerder geïnterviewden. De deelnemers representeerde een groot deel van de robotlevenscyclus, van ontwerp tot gebruik en zowel kennis als beleid zoals uit tabel 2 blijkt.

Het doel van de workshop was om dieper in te gaan op de dreigingen, kwetsbaarheden en beheersmaatregelen. Hiervoor werden de deelnemers in twee groepen verdeeld die vervolgens in twee parallelle sessies van een half uur brainstormden over ofwel de risico's en kwetsbaarheden, ofwel de beheersmaatregelen aan de hand van de robotlevenscyclus. Na een veertigtal minuten wisselden de groepen van onderwerp voor een tweede ronde. Tijdens de sessies werden de deelnemers gevraagd om door middel van mind mapping ideeën op post-its schrijven en deze op aangegeven plaatsen te plakken in een overzicht. Afsluitend werd aan de deelnemers gevraagd om met stickers de belangrijkste ideeën te markeren. In Appendix B is een overzicht van de resulterende ideeën opgenomen.

Tabel 2. Workshopdeelnemers.

	Levenscyclus	Achtergrond/Type
1	Ontwerper	Industriële robots
2	Ontwerper	Industriële robots
3	Integrator	Industriële robots
4	Gebruiker	Technologie
5	Kennisinstituut	Exoskelet
6	Beleid	Normontwikkeling
7	Beleid	Beleidsontwikkeling

3 Robotica: afbakening van het rapport

De toepassing van robotica is zichtbaar in diverse industrieën en sectoren uiteenlopende van gezondheidszorg tot maakindustrie. Vanuit de Nederlandse Smart Industrie actieagenda[14] wordt sterk ingezet op de ontwikkeling van nieuwe productietechnologieën en de verdere integratie van informatie- en communicatie-technologie (ICT) in het hele proces van ontwerpen, fabriceren en distribueren in de industrie (i.c. verregaande digitalisering en verweving van apparaten, productiemiddelen en organisaties - het 'internet of things'). De inzet daarbij is primair het versterken van de Nederlandse industrie door maximaal gebruik te maken van de nieuwste ICT-ontwikkelingen zodat de industrie efficiënter, flexibeler, kwalitatief beter en preciezer op maat kan produceren. Daarnaast zijn er voorbeelden zoals in de gezondheidszorg, waar er wordt geïnvesteerd in de ontwikkeling van robots die een functie vervullen bij repetitieve precisiewerkzaamheden of bij het verlenen van zwaardere zorgtaken (bijvoorbeeld het op bed tillen) van ouderen en patiënten.

Bij deze ontwikkelingen gaat het primair om de robotfunctionaliteit. Veiligheids- en eventuele (cyber) security-risico's zijn daarmee niet de primaire drijver en veelal ook geen belangrijk aandachtspunt in de ontwikkeling van de robot.

Gezien het grote werkveld van robotica is het belangrijk om binnen dit rapport het speelveld goed af te bakenen. Hierbij baseren wij ons op de bevindingen van onze initiële literatuurscan. We zijn in dit rapport primair geïnteresseerd in robots in relatie tot arbeidsveiligheid. Wij beginnen met het geven van een algemene definitie van wat er onder de term robot wordt verstaan binnen de context van dit onderzoek. Omdat we ook geïnteresseerd zijn in mogelijke toekomstige ontwikkelingen die industriële robots ondergaan, kijken we ook breed naar wat de te verwachten mogelijkheden zijn binnen robotica. Daarom lichten we hieronder het concept industriële robot verder toe. Welke ontwikkelingen kunnen er binnen de robotica worden verwacht? Wat zou dat voor de industriële robot in relatie tot arbeidsveiligheid kunnen betekenen? Op basis van deze informatie, in combinatie met de opgestelde definitie, zijn uitgangspunten en vragen geformuleerd voor de gehouden telefonische interviews met de robotica-experts.

Tot slot benoemen we enkele belangrijke aspecten die we in de literatuur zijn tegengekomen. Deze aspecten zullen later in dit rapport worden besproken naar gelang hun directe of indirecte effect die ze kunnen hebben op arbeidsveiligheid.

3.1 Definitie robot

Het concept robots omvat tegenwoordig niet alleen fysieke robots, maar ook 'slimme' sensornetwerken, analysesoftware, ofwel kunstmatige intelligentie in het

[14] http://www.smartindustry.nl/wp-content/uploads/2014/11/Smart-Industry-actieagenda-LR.pdf

algemeen[15]. Een fysieke robot kan worden beschouwd als een machine met software, waardoor de mogelijkheden groter zijn dan een standaardmachine.

In dit rapport richten wij ons voornamelijk op de fysieke machine die als industriële robot wordt ingezet. Hierbij beschouwen we de software als een onderdeel van deze robot. Puur softwarematige robots worden echter buiten beschouwing gelaten. Zelfs voor de fysieke industriële robot, zijn er meer definities mogelijk. Hieronder een greep uit de definities die wij tegenkwamen:

> *A robot is an automatic and programmable machine, able to perform certain operations autonomously. A robot can substitute a human in certain tasks, expecially dangerous, repetitive or heavy tasks. A robot can be equipped with sensors to perceive its surroundings and adapt to new situations.*[16].
>
> *Een robot is een apparaat met (a) sensoren om (iets van) de omgeving waar te nemen, (b) computeralgoritmen om beslissingen te nemen aan de hand van de sensorgegevens, en (c) motoren om iets mechanisch in beweging te zetten*[17]*.*
>
> *A robot is a mechanical or virtual artificial agent, usually an electro-mechanical machine that is guided by a computer program or electronic circuitry*[18]*.*
>
> *[An industrial robot is] automatically controlled, reprogrammable, multipurpose manipulator, programmable in three or more axes which can be either fixed in place or mobile for use in industrial automation applications* [19]*.*

Aan de hand van deze definities kunnen we stellen dat:

> Een robot een machine is die kan worden ge*programmeerd, sensoren* heeft, en een bepaalde gradatie van *mobiliteit* heeft waardoor de robot *autonoom* een taak kan uitvoeren.

Deze definitie is puur bedoeld om binnen de context van dit rapport duidelijk te maken wat wij met het begrip ‘robot’ bedoelen. Het sleutelwoord in deze definitie is de autonomie van de robot die wordt bepaald door hoe deze geprogrammeerd is, wat voor sensoren de robot heeft, en hoe mobiel (of niet) de robot is. Deze factoren kunnen een rol spelen in het maken van onderscheid in verschillende type robots. Hieronder lichten wij de verschillende gradaties van deze factoren verder toe in relatie tot het doel van dit onderzoek.

3.1.1 Programmeerbaar

Robots worden nu nog vaak geprogrammeerd om één of enkele taken uit te kunnen voeren (zie het kader voor een voorbeeld voor de programmering van een simpele taak). Bij uitzonderingen die buiten de ingestelde programmering vallen komt de

---

[15] van Est, R., & Kool, L. (2015). *Werken aan de robotsamenleving: Visies en inzichten uit de wetenschap over de relatie technologie en werkgelegenheid.* Rathenau Instituut: Den Haag.

[16] IGI Global. Lesson 1. Humanoid robots. https://www.youtube.com/watch?v=3FXRw2CWACg&feature=youtu.be

[17] Martijn Wisse (2015). De robot de baas: De toekomst van werk in het tweede machinetijdperk. *Wetenschappelijke raad voor het regeringsbeleid. P 73.*

[18] https://en.wikipedia.org/wiki/Robot

[19] ISO 8373:2012, Robots and robotic devices — Vocabulary

robot in de problemen. Robotontwikkelaars werken hard aan multipurpose robots, dat wil zeggen robots die meer dan één taak kunnen uitvoeren. Deze robots zijn echter nog niet op het niveau van snelheid en nauwkeurigheid als robots die voor één specifieke taak zijn ontwikkeld[20]. Wel komen deze multipurpose robots al dichter in de buurt van robots met echte kunstmatige intelligentie die op hun omgeving kunnen reageren en daarmee kunnen interacteren. Het toevoegen van 'emoties' en beloning- en strafsystemen aan robots is een ander onderzoeksgebied om de kloof tussen mens en de robot als machine te verkleinen. [21]

3.1.2 Sensoren

Zelfs robots met een relatief simpele taak moeten herkennen of ze een product hebben vastgepakt. Herkennen hoe groot of in welke hoek een schroef ligt die moet worden opgepakt, tot het scannen van de omgeving om te bepalen waar veilig naar toe kan worden bewogen zonder ergens tegen aan te stoten.

Alternatief is het actief scannen van de omgeving om zo een model van de omgeving te creëren op basis waarvan de robot kan onderkennen hoe deze zich conflictenvrij door zijn omgeving kan bewegen en daarin kan handelen. Deze techniek wordt ook toegepast bij autonome rijdende auto's.

3.1.3 Mobiliteit

Bij geen of nauwelijks mobiliteit is sprake van een vaste locatie van waaruit de robot handelt. Verder kan de robot op een rails zitten of een vastgesteld pad herkennen (dat bijvoorbeeld rood geschilderd is of met ingefreesde magneten is aangegeven).

Binnen de mobiele robotica speelt bij mobiliteit ook de vorm een grote rol, uiteenlopend van wielen en rupsbanden via twee- of meerbenig tot zuignappen[22]. In dit rapport speelt dit onderscheid minder.

Wat wel van belang is of een robot op zijn vaste plek blijft of een duidelijke vaste route heeft, dan wel autonoom rond beweegt waarbij er sprake is van een dynamisch wijzigende route.

Met betrekking tot autonome voertuigen in open teelten is het rapport Veiligheid van autonome voertuigen in open teelten[23] interessant omdat het ingaat op de veiligheid van autonoom werkende machines in de precisielandbouw. Vigerende wet- en regelgeving waaronder de EU trekkerrichtlijn (2003/37/EG) en de EU machinerichtlijn (2006/42/EG) worden besproken in de context van de verdergaande 'robotisering' van de landbouw.

3.2 Industriële robot: nu

De grootste voordelen van robots zijn dat ze niet moe worden, zich niet vervelen, niet klagen, sterk en precies zijn. Deze eigenschappen maken ze ideaal voor

---

[20] Zie bijvoorbeeld: https://www.youtube.com/watch?v=8P9geWwi9e0

[21] Zie M. Seijlhouwer, Meelevende machines, De Ingenieur, 2016, jaargang 128, no 4, pg 12-19.

[22] Bijv. een ramenwasrobot

[23] S. Heijting, C. Kempenaar en A. Nieuwenhuizen, Veiligheid van autonome voertuigen in open teelten, PPL project 79/ZGLE.11.0108 (2013).

gevaarlijk, zwaar en repetitief werk[24]. Robots worden momenteel dus ingezet bij het verplaatsen van (zwaar) materiaal binnen een gebouw of naar een vrachtwagen; lassen, spuiten en assembleren (bijvoorbeeld auto's); en plukken van bijna rijpe groenten en fruit in kassen.

In het kader "Toepassingen van hedendaagse robots op de werkvloer" waren voorbeelden te zien van toepassingen van industriële robots in assemblagelijnen en lasrobots.

Over het algemeen geldt nu nog voor industriële robots die wijdverspreid in gebruik zijn binnen fabrieken dat ze[25]:

- vaak in een gecontroleerde omgeving staan,
- een repetitief en voorgeprogrammeerde taak hebben,
- nog geen directe interactie met personen (incl. derden, bezoekers) om zich heen hebben,
- zich nog niet zelf kunnen aanpassen aan nieuwe situaties.

Voorbeelden van parameters waarbinnen robots worden gedefinieerd en kunnen worden verbeterd zijn[26]:

- de hoeveelheid assen ('vrijheidsgraden') waarop de robot kan bewegen,
- de maximale reiklengte van de robot,
- het aantal gewrichten van de robot (beweegbare delen),
- de snelheid van bewegen, de acceleratie van beweging,
- de nauwkeurigheid in een taak,
- de nauwkeurigheid bij herhaling van een taak.

Nu is het vaak nog dat robots alleen maar goed zijn voor de specifieke taak waarvoor ze worden ingezet, al neemt de flexibiliteit waarmee robots kunnen worden geprogrammeerd voor een nieuwe taak toe. Dit blijven echter soortgelijke taken waarbij bijvoorbeeld enkele coördinaten moeten worden bijgesteld of een andere tooling op dezelfde plaats wordt ingezet (schroevendraaier in plaats van boor). De huidige staat van robots die meer verschillende soorten handelingen kunnen uitvoeren zijn nog lang niet zo efficiënt als industriële robots die voor de uitvoering van één taak gebouwd zijn (zie bijvoorbeeld de DARPA Robotics Challenge[27]).

3.3 Industriële robot: toekomst

In sciencefiction films en boeken worden robots vaak als handige kompanen neergezet: het zijn robots die volledig autonoom zijn, zich aan iedere situatie kunnen aanpassen en zelden zonder energie komen te staan. Om tot dit soort robots te kunnen komen zijn nog veel ontwikkelingen nodig op het gebied van visuele en auditieve perceptie, spraak (luisteren en spreken), manipulatie,

[24] http://www.nrc.nl/next/2015/10/31/robot-wordt-eerder-arts-of-advocaat-dan-kapper-1551807
[25] IGI Global. Lesson 1. Humanoid robots. https://www.youtube.com/watch?v=3FXRw2CWACg&feature=youtu.be
[26] https://en.wikipedia.org/wiki/Industrial_robot
[27] https://www.youtube.com/watch?v=8P9geWwi9e0

redeneervermogen, adaptievermogen, lerend vermogen, emoties[28], en begrijpen van sociale conventies. Er wordt binnen robotica dan ook hoog ingezet op het ontwikkelen van robots die zich autonoom kunnen voortbewegen, hun omgeving kunnen 'zien' en hierop anticiperen, kunnen samenwerken met personen, en geschikt zijn voor meer dan één taak. Dit betreft de zogenaamde 'general purpose robots'.

Elementen hiervan zie je al sporadisch worden toegepast in de maatschappij:

- In het ALIZ-E project waarin een interactierobot wordt ontwikkeld die kinderen helpt meer over hun diabetes te leren[29].
- Project SPENCER is gericht op de ontwikkeling van robots met slimme interactiesystemen (bijv. een robot die verdwaalde reizigers op Schiphol begeleidt (2015))[30].
- Zorgrobot LEA die is ontwikkeld om ouderen te ondersteunen om zelfstandig te blijven functioneren[31].
- Robots die dienen als vermakers, koks en serveerders in een restaurant in China (2014)[32].
- De Bigdog robot en de LS3 Legged Squad Support System die als een soort van rennende "lastdieren" zware spullen voor uitgestegen infanteristen kunnen vervoeren door ruw terrein[33].
- In 2015 waren de finales van de DARPA Robotics Challenge om een robot te ontwikkelen die meerdere taken autonoom kan uitvoeren (i.e., deur openen, traplopen, schakelaar aanzetten en een schroef kan aandraaien)[34].
- De bewakingsrobot SAM[35].
- In het project 'Titan the robot' wordt er gefocust op robots als vermaak[36].

Deze projecten laten zien aan dat er naar een zekere mate van menselijkheid of mensomgeving in robots wordt nagestreefd. Daarbij moet worden vermeld dat de interactie met deze robots nog verre van gelijkwaardig is wanneer vergeleken met menselijke interactie. Ook komen ze nog niet in de buurt van de snelheid en efficiëntie waarmee huidige industriële robots hun taak uitvoeren. Het is echter goed mogelijk dat deze problemen in de toekomst zullen worden opgelost. Ook zijn er elementen in de ontwikkeling van deze robots te zien die ook relevant kunnen zijn binnen een industriële omgeving.

Industriële robots van de toekomst zullen op termijn autonomer en adaptiever in de dynamische omgeving van een werkvloer worden. In deze omgeving zullen ze zich moeten aanpassen aan dynamische veranderingen van de omgeving (een container meer of minder, een tijdelijk geblokkeerde doorgang, enzovoorts), samen moeten werken met personen en deze dynamisch moeten ontwijken bij het uitvoeren van hun eigen taken. Verder zouden ze eventueel kunnen switchen

---

28 Zie M. Seijlhouwer, Meelevende machines, De Ingenieur, 2016, jaargang 128, no 4, pg 12-19,
29 http://www.aliz-e.org
30 http://www.spencer.eu/
31 http://www.robotcaresystems.com/wat-is-het/
32 http://www.chinadaily.com.cn/m/jiangsu/kunshan/2014-08/08/content_18274963.htm
33 http://www.bostondynamics.com/robot_bigdog.html
34 https://www.youtube.com/watch?v=8P9geWwi9e0 - te zien is dat dit type robots nog relatief beperkt zijn qua efficiëntie.
35 http://www.robots.nu/nederlandse-sam-robot-beveiligt-je-pand/
36 https://www.youtube.com/watch?v=cjfPFr9SswA

tussen taken om met producten die variëren in grootte, gewicht, kwetsbaarheid en positie te kunnen werken.[37]

Een belangrijk aspect is wat deze ontwikkelingen voor de veiligheid betekenen van personen die hun werkomgeving delen met dergelijke robots. Een groot verschil tussen industriële robots en sociale of zorgrobots is dat waar de laatstgenoemde typen robots specifiek worden ontwikkeld om met personen om te gaan, industriële robots daarentegen voornamelijk zullen worden ingezet om zwaar, gevaarlijk en repetitief werk uit te voeren. Ze zullen dus per definitie direct of indirect risicovoller zijn voor de veiligheid van de mens.

Elke robot bevat of is gekoppeld met één of meer veelal met de buitenwereld interacterende computersystemen en bevat industriële procescontrolesystemen (ICS) die de motoren voor armen en voortbeweging sturen. Deze ICS en communicatie brengen een aan veiligheid gerelateerd cyberrisico in de cyber-fysieke wereld, in dit geval robots, met zich mee. Meer informatie met betrekking tot dit specifieke risico en de aangrijpingspunten is respectievelijk te vinden in een recent TNO rapport[38] en in paragraaf 3.5 hieronder.

Belangrijke drijfveren vanuit de industrie voor verdergaande robotisering zullen de functionaliteit en bruikbaarheid van de robots zijn. Vooralsnog kunnen autonome of ‘general purpose’ robots echter nog niet concurreren met de huidige industriële robots op het gebied van snelheid en efficiëntie. Wanneer complete industrieën zich inzetten op de ontwikkeling en grootschalige inzet van robots zal dit verschil waarschijnlijk snel verdwijnen. Een dergelijke ontwikkeling zou vergelijkbaar zijn met de ontwikkeling van de zelfrijdende auto’s die sneller is verlopen dan veel experts vooraf vermoedden.[39]

In de context van de gestelde definitie zijn de volgende ontwikkelingen te verwachten met betrekking tot industriële robots die wijdverspreid in gebruik zijn:

- **Programmeerbaar en flexibel qua taken**: Robots die meer dan één taak kunnen uitvoeren. Het programmeren zal hierdoor wel mogelijk complexer worden voor de industrie zelf.
- **Mobiliteit**: Robots die zich autonoom over de werkvloer verplaatsen zonder vooraf gedefinieerde paden om materialen en producten te vervoeren of om taken op verschillende locaties uit te voeren. Dit gebeurt in zekere mate al met zelfrijdend containertransport op bijvoorbeeld de APM containerterminal in Rotterdam, maar zou in de toekomst ook kunnen gebeuren op locaties waar zich meer personen bevinden.
- **Sensoren**: Naarmate robots mobieler worden en meer taken gaan uitvoeren zal het van belang zijn dat zij hun omgeving goed ‘zien’ en hier goed op kunnen anticiperen. Ook zullen sensoren steeds slimmer worden: nieuwe ontwikkelingen zijn het meten van de door de robot uitgeoefende kracht. Bij

[37] Bijvoorbeeld het pakken van een onderdeel uit een bak waar de producten schots en scheef in liggen. Martijn Wisse (2015). De robot de baas: De toekomst van werk in het tweede machinetijdperk. *Wetenschappelijke raad voor het regeringsbeleid. P 73.*

[38] Steijn, W., Luiijf, H., Gallis, R., Opkomende risico's voor arbeidsveiligheid als gevolg van IT-koppelingen van en tussen arbeidsmiddelen, TNO rapport 2016 R10096.

[39] http://www.nrc.nl/next/2015/10/31/robot-wordt-eerder-arts-of-advocaat-dan-kapper-1551807

onverwachte weerstand op bijvoorbeeld de armbeweging kan de uitgeoefende kracht verminderen dan wel stil worden gezet.

3.4 Type scenario's toepassing robots

Naar verwachting zal de wereldpopulatie aan mensen ruim negen miljard zijn in 2050[40]. Met deze toenemende populatie en toenemende vergrijzing in de 'westerse wereld' groeit de vraag naar producten, diensten en zorg. De verwachting is dat robots in toenemende mate zullen worden ingezet in allerlei sectoren als aanvulling op de beschikbare arbeid omdat ze nauwkeurig werken en omdat ze nieuwe vormen van productie toe laten.

Ter illustratie van de diversiteit in toepassingen van robots geven we hier enkele voorbeelden van type robots waarbij arbeidsveiligheid een rol kan gaan spelen: lasrobot[41], assemblagerobot[42], baliewerker[43], transportrobots (bijv. robots in containerterminal[44], agrobot[45] en ziekenhuis logistiek[46]), sociale robots (bijv. Nao[47] en Alica[48]), zorgrobots (bijv. RIBA II[49]), bedieningsrobots (bijv. Infinium Serve[50]), militaire robots (bijv. BigDog[51]), en veiligheidsrobots (bijv. blusrobot[52] en bewakingsrobot[53]). Deze voorbeelden laten tevens zien dat toepassingen van robots in veel verschillende sectoren of settingen kunnen worden verwacht zoals in de zorg, horeca, landbouw, productie, industrie, recreatie (bijv. in pretparken), transport (bijv. op vliegvelden), defensie, hulpverlening, en inspectiediensten en Rijkswaterstaat.

3.5 Cyber-fysieke veiligheid

Robots worden bestuurd met programmatuur. Daarnaast gebruiken ze in toenemende mate mobiele en vaste telecommunicatienetwerken voor hun situationele 'bewustzijn' zoals een kaart van de omgeving waarin ze opereren of een indicatie of geautoriseerde personen zich in die omgeving ophouden, het verkrijgen van nieuwe opdrachten en de interactie met andere robots. Via die netwerken kunnen robots op directe of indirecte wijze gekoppeld zijn aan publieke netwerken, waaronder het internet.

---

40 https://nl.wikipedia.org/wiki/Wereldbevolking
41 https://www.youtube.com/watch?v=kbi2Jd4-mu8
42 https://www.youtube.com/watch?v=JIC0SIkmbjk
43 Hotelrobotisering van baliewerk en bagageafhandeling. Een extreem voorbeeld is het Henn-na Hotel in Japan (http://www.theguardian.com/travel/2015/aug/14/japan-henn-na-hotel-staffed-by-robots). Ook in Nederland en België worden de eerste robots in dit segment te vinden (http://customerfirst.nl/nieuws/2015/06/servicerobot-marriot-hotel-in-gent-herkent-gasten/index.xml)
44 https://www.youtube.com/watch?v=22SvOhI47Tw
45 https://www.youtube.com/watch?v=LFfod3EYdqc
46 https://www.youtube.com/watch?v=Q0gNDFXy8YI
47 https://www.youtube.com/watch?v=aLMmGCwNfNk
48 https://www.youtube.com/watch?v=vlh73k4ybeo
49 https://www.youtube.com/watch?v=wOzw71j4b78
50 https://www.youtube.com/watch?v=cLY56vefkFE
51 https://www.youtube.com/watch?v=afeBlgRF-4g
52 https://www.youtube.com/watch?v=e3Z7kXLQRu0
53 http://www.robots.nu/nederlandse-sam-robot-beveiligt-je-pand/

Computers, sensoren, kunstmatige intelligentieprogrammatuur en netwerken geven robots een grote potentie. Tegelijkertijd kan het een achilleshiel zijn. Door malware, hacking, technische en menselijke fouten kunnen robots zich anders in de fysieke omgeving gedragen dan verwacht, waardoor er mogelijk voor de mens onveilige situaties ontstaan. Dit kan zowel direct waarbij een robot in botsing komt met een mens dan wel indirect waarbij bijvoorbeeld een robot uit de koers een stelling met opgeslagen chemicaliën omver rijdt of indien de robot apparatuur met zich meedraagt die op zich gevaar voor de mens kan opleveren (bijv. lasers, stralingsbron, laselektroden, mechanische apparatuur).

Hieronder een korte schets van mogelijke risicofactoren en tevens een korte uitleg en mogelijke mitigerende maatregelen voor ieder van de genoemde risicofactoren:

1 Verkeerde sensorinformatie.
Verwacht wordt dat de werkomgeving steeds meer sensoren gaat bevatten die een robot situationele ‘bewustzijn’ kunnen geven. Sensoren kunnen echter andere informatie geven dan de ‘werkelijkheid’ door bewuste manipulatie (malware, hacker), door technisch falen of door menselijk falen (bijv. configuratiefout).
Tegenmaatregelen zijn een self-protected node waardoor onverwachte afwijkingen niet worden geaccepteerd en het correleren van meer informatiebronnen.
2 Verstoorde communicatie tussen sensor(en) en de robot.
Communicatie tussen robot en sensoren gebeurt meestal via draadloze communicatietechnieken. Denk aan WiFi, Zigbee, Bluetooth of in de nabije toekomst LoRa, een LPWAN techniek.[54]
3 Een communicatiekanaal kan worden/zijn geblokkeerd (jamming van frequenties, denial-of-service aanval/overbelasting van kanaal) of verkeerde informatie geven, bijvoorbeeld door signaalmanipulatie.
Tegenmaatregelen zijn onder andere robuuste communicatie, sterke versleuteling en anti-stoormaatregelen (industriële communicatie).
4 Verstoorde communicatie tussen robot en de “thuisbasis”.
Via dit communicatiekanaal kan een robot instructies voor volgende werkzaamheden of gewijzigde prioriteiten ontvangen en tevens de momentane status doorgeven aan een centrale bedien- c.q. controlepost. Communicatie zal op dezelfde wijze plaatsvinden als onder het vorige punt, dan wel via vaste communicatie zodra een mobiele robot zich koppelt aan een ‘oplaadstation’.
Tegenmaatregelen zijn onder andere robuuste communicatie, sterke versleuteling en anti-stoormaatregelen (industriële communicatie).
5 Verstoorde communicatie tussen robots onderling.
Verwacht mag worden dat autonome robots onderling informatie uitwisselen via hun “robot area network” (RAN) om samen de meest optimale en efficiënte taakuitvoering te bereiken. RANs kunnen gebaseerd zijn op technieken als WiFi, maar ook op Mobile Ad hoc NETwork (MANETs). Het kunstmatige intelligentiedomein heeft in de laatste decennia volop gewerkt aan intelligent

[54] LoRA staat voor Long Range en is, een techniek volgens de LPWAN (Low Power Wide Area Network) specificatie die bedoeld is voor de (massieve) koppeling van draadloze “things” op batterijen. Dit is met name een techniek die zal gaan worden ingezet voor intelligente sensoren. LoRa van KPN zal in het tweede kwartaal van 2016 in heel Nederland beschikbaar zijn.

agents die samenwerken om een klus te klaren (o.a. swarming, dat is het tegelijkertijd als een gecoördineerde zwerm optreden van een groter aantal losse eenheden. Dat is te vergelijken met een groep mieren die een groot insect naar hun hol transporteren.).
Opzettelijke inbreuken op de onderlinge communicatie kan leiden tot verkeerde instructies en onderling situationeel 'inzicht' waardoor gevaar kan ontstaan voor de mens die dezelfde fysieke ruimte deelt.
Tegenmaatregelen zijn onder andere robuuste communicatie, self-protecting node maatregelen, sterke versleuteling en anti-stoormaatregelen (industriële communicatie).

6 Gemanipuleerde programmatuur of instructies.
Tijdens herprogrammering, bijvoorbeeld via een laptop of een overdraagbaar medium als USB, kan onverwachts malware in een robot terechtkomen.
Tegenmaatregelen zijn onder andere anti-malware, intrusion detection, gelaagd gescheiden netwerken.

7 Onbetrouwbare centrale bedien- c.q. controlepost.
Malware, inbraken en menselijke fouten op de centrale bedien- c.q. controlepost kunnen leiden tot foutieve instructies aan de robots op de werkvloer. Door de robots bijvoorbeeld overdag op nachtstand te zetten of door tijdens gepland onderhoud over te schakelen op 'normaal' kan betekenen dat de robots zich onbedoeld bevinden in gebieden waar personen werkzaam zijn.
Tegenmaatregelen zijn onder andere anti-malware, gescheiden netwerken, intrusion detection en sterke programmatische maatregelen om overgangen naar een onveiligere operationele modus alleen toe te staan onder sterke controle (bijv. akkoord twee personen).

3.6 De rol van wet- en regelgeving

Op het moment wordt de veiligheid betreffende immobiele industriële robots vaak grotendeels gewaarborgd door er een veiligheidskooi omheen te plaatsen, of door op een andere manier een veiligheidszone te creëren waardoor medewerkers op veilige afstand van de robot kunnen blijven[55]. Echter, naarmate robots intelligenter (of in andere woorden complexer) en mobieler zullen worden op de werkvloer zullen de maatregelen om de veiligheid te waarborgen ook complexer worden.

Hierbij is het belangrijk om een inventarisatie te maken van wat de verwachte toepassingen worden en welke nieuwe dreigingen op het gebied van arbeidsveiligheid daarbij meekomen. Op deze manier kan men proberen te anticiperen op situaties die zich in de nabije toekomst kunnen gaan voordoen. Daarnaast dient de literatuur ook als inspiratiebron. Zo worden de drie wetten van Asimov vaak genoemd als mogelijk startpunt voor robots met hoge kunstmatige intelligentie:

- Eerste Wet: Een robot mag een mens geen letsel toebrengen of door niet te handelen toestaan dat een mens letsel oploopt.

[55] De beperkingen van deze aanpak blijkt ook uit het aan het begin gegeven voorbeeld waarbij de onderhoudsmedewerker zicht ten tijde van het ongeluk noodzakelijkerwijs in de veiligheidskooi bevond.

- Tweede Wet: Een robot moet de bevelen uitvoeren die hem door mensen worden gegeven, behalve als die opdrachten in strijd zijn met de Eerste Wet.
- Derde Wet: Een robot moet zijn eigen bestaan beschermen, voor zover die bescherming niet in strijd is met de Eerste of Tweede Wet.

Murphy en Woods hebben deze drie wetten in 2009 geherformuleerd om on de praktijk toepasbaar te zijn[56]:

- Een mens mag geen robot inzetten wanneer dat dit werk met de robot niet voldoet aan de hoogste wettelijke en professionele normen van veiligheid en ethiek.
- Een robot moet afhankelijk van zijn functie mensen voldoende kunnen beantwoorden.
- Een robot moet worden begiftigd met genoeg toereikende autonomie om zijn eigen bestaan te kunnen beschermen zolang hij hierdoor gemakkelijk te bedienen blijft en zijn autonomie niet in strijd is met de Eerste en de Tweede Wet.

Verder zal wet- en regelgeving mogelijk een rol gaan spelen in het sturen van het maatschappelijke debat rondom robots dat naast de veiligheid ook tal van andere aspecten kent. Hieronder benoemen wij enkele van die aspecten:

- *Aansprakelijkheid en verantwoordelijkheid*
  Bij de toepassing van de robot zijn meerdere partijen betrokken: de ontwerper en bouwer van de robot, de installateur en integrator die hem plaatst, en de uiteindelijke gebruiker. Wie is er verantwoordelijk (en dus aansprakelijk) als er iets mis is met de robot of wanneer er een ongeluk gebeurt?
- *Acceptatie door de maatschappij*
  Acceptatie van robots in de maatschappij is van meerdere aspecten afhankelijk die eerst moeten worden geadresseerd. Zo gaat robotisering gepaard met een angst op minder banen en daardoor toenemende werkeloosheid. Met robotisering kunnen echter ook nieuwe arbeidskansen worden gecreëerd door cognitieve ondersteuning te bieden aan personen met een cognitieve beperking.
  Daarnaast is er de vraag of een zorgrobot de zorg die een mens biedt kan overnemen. Verder kan men zich afvragen hoe de maatschappij zal reageren op ongelukken die met robots gebeuren, bijvoorbeeld wanneer een bezorgingsdrone een pakje op iemand laat vallen, of tegen iemand aan botst. Alleen al de term ‘robots’ zorgt er voor dat we anders reageren dan wanneer we het over een machine hebben[57]. Of dit nu op straat of op de werkvloer is. Ook hoe robots worden gepresenteerd aan de maatschappij speelt hier een rol. Wanneer robots als beter en preciezer dan de mens worden gepresenteerd zal dit tot meer acceptatie leiden bij managers, maar zouden werknemers zich bedreigd kunnen voelen.
- *Privacy*
  Robots zijn – net zoals mensen - afhankelijk van sensorische informatie om op hun omgeving te kunnen reageren. Bij robots kan deze informatie echter

[56] Murphy, R.R., & Woods, D.D. (2009). Beyond Asimov: The three laws of responsible robotics. *IEEE Intelligent Systems, 24*(4), 14-20.
[57] http://jalopnik.com/the-way-were-reacting-to-the-vw-worker-killed-by-a-robo-1715462359

makkelijker worden opgeslagen. Hierdoor zijn robots in potentie een risico voor de privacy. Voorbeelden hiervan zijn een sociale robot waar intieme geheimen mee worden gedeeld, of een zorgrobot waarmee ook een camera in huis wordt gehaald. Ook de privacy van personen op de werkvloer zal in acht moeten worden genomen naarmate meer camera's en sensoren op de werkplek komen.

- *Moraliteit*

  Naarmate robots met personen gaan samenwerken en autonomere beslissingen kunnen nemen, zal de vraag of een robot moraliteit moet hebben belangrijker worden. Moeten robots ethische beslissingen kunnen nemen, en zo ja, waar moeten die beslissingen op gebaseerd zijn. Moet een automatisch rijdende auto kiezen om tegen een muur uit te wijken om een kind te ontwijken, of zou het behoud van de inzittenden voorrang moeten krijgen[58]? Moet een robot een enkele werknemer in gevaar brengen, om de algehele veiligheid van de installatie te behouden? Vaak weten we niet eens hoe de mens zou reageren in deze situaties, kan dit dan wel voor een robot worden voorgeprogrammeerd?[59]
- *Rechten van een robot*

  Naarmate robots autonomer en intelligenter worden - met andere woorden, naarmate de robot meer op een mens gaan lijken – kan ook de vraag worden gesteld of een robot dan soortgelijke rechten verdient. Denk bijvoorbeeld aan het recht om te worden onderhouden, of het recht om niet uit te worden gezet.

Sommige van deze aspecten lijken nog ver weg te staan van de huidige toepassing van industriële robots. Maar naarmate de robotisering van de maatschappij zal toenemen, zullen deze aspecten moeten worden opgelost en zullen ze mogelijk ook een indirect effect hebben op de industriële robots en de manier waarop ze worden ingezet.

[58] Zie bijvoorbeeld ook: http://jalopnik.com/what-should-robot-cars-ethical-rules-be-1579407463

[59] Een ander alternatief is dat de robot dit zichzelf aanleert doormiddel van leerstrategieën met beloning- en strafsystemen. Zie hiervoor, M. Seijlhouwer, Meelevende machines, De Ingenieur, 2016, jaargang 128, no 4, pg 12-19.

4 Interview- en workshopresultaten

In dit hoofdstuk wordt een samenvatting gegeven van de meningen en suggesties die uit de interviews en workshop naar voren kwamen.

4.1 Definitie robots

Experts werden gevraagd om een definitie te geven van een robot. Hieruit kwam naar voren dat de term robot als een containerbegrip kan worden beschouwd waar veel machines onder vallen. Hieronder geven we enkele definities of roboteigenschappen zoals ze in de interviews naar voren kwamen:

- **Apparaten die geprogrammeerd worden voor een bepaald doel**.
  Deze hoef je zelf niet te besturen, ze zijn geprogrammeerd met een begin en een einde. De termen robotisering en automatisering zijn niet uitwisselbaar, maar er is ook geen principieel verschil. Een robot kan zelfstandig een complexe handeling verrichten. Een robot heeft echter geen eigen wil, het zal altijd op basis van geprogrammeerde regels blijven.
- **Alle fysieke robots of ICT-systemen die taken van mens overnemen**.
  Belangrijke elementen zijn de sensoren, een cognitief proces (informatie verwerkingsproces) en uitvoering. Hier vallen ook exoskeletten onder: deze moeten waarnemen wat een mens wil doen, de informatie verwerken, om vervolgens met de juiste timing en kracht de motoren aan te sturen.
- **Robots kunnen zelfstandig bewegen**.
- **Robots wijken pas van machines af als ze zelfdenkend/zelflerend zijn**.
  Robots worden geprogrammeerd om iets te doen, pas als de machine buiten de programmatuur kan treden is het een robot.
- **Robots zijn machines die taken van mensen gedeeltelijk of volledig overnemen**.
  Het beschrijven van een robot kan men doen aan de hand van een onderverdeling tussen mobiliteit en de handeling die wordt uitgevoerd. Software robots zijn een aparte categorie.
- **Robotisering gaat vooral over logistieke functies**.

Ter herinnering, nogmaals de definitie die wij voorafgaand aan dit onderzoek hebben gesteld:

Een robot een machine is die kan worden geprogrammeerd, sensoren heeft, en met een bepaalde gradatie van mobiliteit heeft waardoor de robot autonoom een taak kan uitvoeren,

Tot slot kwam in de interviews naar voren dat autonomie als term niet duidelijk is. Bij autonomie denkt men snel aan een robot die volledig zelfstandig kan handelen. In onze definitie leggen wij echter de nadruk op dat de robot alleen de taak waar hij voor bedoeld is autonoom kan uitvoeren. Binnen een ‘collaborative workplace’ staan dus ook autonome robots, ook al werken deze per definitie samen met de mens.

4.2 Voordelen van robotisering

Volgens de experts zijn de voordelen van robotisering te vinden in de mogelijkheid voor bedrijven om hogere productiviteit tegen minder kosten en van betere kwaliteit (hogere precisie) te bereiken. Verder kunnen robots fysiek belastende, repetitieve, of gevaarlijk werk overnemen van de mens.

4.3 Verwachte ontwikkelingen in nabije toekomst

Experts vonden het over het algemeen moeilijk om een inschatting te maken van de ontwikkelingen in de nabije toekomst. Er was dan ook niet altijd overeenstemming in geschatte tijdspaden van de ontwikkelingen tussen de experts. Wel was men het er over eens dat de ontwikkelingen nu in een hoog tempo gaan.

Waar een groot deel van de experts op een lijn zat, is dat er een verschuiving wordt verwacht van een klassieke robot op een vaste werkplek naar 'collaborative workplaces' waar robots en personen samenwerken. Dit geldt niet alleen voor zwaar of gevaarlijk werk. De experts verwachten ook een trend waarbij robots een functie krijgen voor kleinere taken: breng dit, beantwoordt dat, breng mij daarheen. Anderzijds zorgt deze samenwerking er ook voor dat er altijd een mens in de buurt is om de robot te assisteren. Bijvoorbeeld wanneer deze een pallet niet kan pakken omdat deze scheef ligt, al kunnen robots hier dankzij sensorontwikkelingen steeds beter mee omgaan. Vanuit de landbouwtechniek werden drie rollen geïdentificeerd die personen nog moeten uitvoeren bij de samenwerking met robots:

1 De aansturing;
  Deze rol zal echter snel verdwijnen aangezien autonome robots al op de markt komen. [60]
2 De veiligheid waarborgen;
  Met lasers en sensoren kan al een hoop, maar afhankelijk van de voorspelbaarheid van de omgeving moet er nu nog vaak een mens bij zijn.
3 Controle van de werkzaamheden;
  Dit lijkt iets wat robots voorlopig nog niet zelf kunnen.

Met betrekking tot de verschuiving naar collaboratieve werkplekken, maken de experts wel een specifiek onderscheid tussen werkvloeren met een focus op massaproductie en die met een focus op maatwerk. Waar de focus op massaproductie ligt, zal deze verschuiving minder snel gaan omdat robots het werk zelf snel en efficiënt kunnen uitvoeren. Echter, wanneer de klantwens variabel kan zijn, bijvoorbeeld in de auto-industrie[61], is de mens nog noodzakelijk voor de afwerking en zal de focus meer op samenwerking tussen mens en robot liggen.

Echte interactie tussen mens en machine wordt nog niet snel verwacht. Scenario's waarin er sprake zou zijn van menselijke interactie vanuit een robot (bijv. een robotdocent) zijn zeer veeleisend. Daarvoor moet de interactie tussen mens en machine eerst beter worden onderzocht. Voordat robots tegen een betaalbare (en

[60] http://www.precisionmakers.com/nl/
[61] http://www.theregister.co.uk/2016/02/25/mercedes_deautomates_production_lines/?mt=1456477368984

vermarktbare) prijs over de basisvaardigheden van de mens beschikt, zoals goed kunnen voelen wat het vastpakt en de omgeving goed kunnen zien, moeten we volgens een aantal experts nog tien tot vijftien jaar wachten.

Verder worden er ontwikkelingen verwacht naar typen robots die meer taken kunnen uitvoeren, onafhankelijk van formaat kunnen opereren, en die vrij door de ruimte kunnen bewegen. Hieronder staan enkele specifieke verwachtingen die genoemd zijn met betrekking tot ontwikkelingen op het gebied van programmering, sensoren, en mobiliteit.

- De vooruitgang in robotica de komende jaren wordt vooral verwacht op het gebied van softwareontwikkeling. Men kijkt heel erg naar wat grote partijen als Google doen. Onlangs heeft Google bijv. haar kunstmatige intelligentie (AI) software open source gemaakt en beschikbaar gesteld aan anderen[62].

- Op korte termijn lijkt men echter voornamelijk naar simpelere programmering te willen gaan die minder tijd kost. Nu kunnen robots vaak nog voor één taak tegelijk worden ingezet. De robot kan wel opnieuw worden geprogrammeerd voor een andere taak, maar dit kost nog relatief veel moeite.

- De ontwikkelingen in programmering gaan hand in hand met de ontwikkelingen op het gebied van sensoren. Er bestaan nu robots met camera's die aangeleerde producten kunnen herkennen, maar men wil naar een robot die ook automatisch nieuwe producten kan herkennen en aanleren. Door betere herkenning van producten, die bijvoorbeeld scheef liggen, zullen robots minder afhankelijk zijn van het ingrijpen door een mens.

- Ontwikkelingen in sensoren zijn ook noodzakelijk voor betere mobiliteit. Men verwacht dat binnen vijf tot tien jaar de eerste zelf voortbewegende robots op de markt komen die op de omgeving kunnen reageren. Deze voorspelling is natuurlijk afhankelijk van de omgeving waar de robot moet gaan worden ingezet: binnen een magazijn zal dit eerder gebeuren dan in een ongestructureerde omgeving. Zoals eerder aangegeven zijn er echter al robots op de markt die binnen[63] en buiten zelf voortbewegen[64].

4.4 Dreigingen en kwetsbaarheden

In de introductie noemden wij het risico van een botsing tussen mens en robot als focusgebied van dit rapport. Hierbij denken wij aan risico's zoals letsel als direct gevolg van het contact tussen mens en robot, maar ook aan indirecte risico's als gevolg van gevaarlijk apparatuur dat de robot meedraagt (bijv. lasers, stralingsbronnen, laselektroden, en mechanisch apparatuur). Dit risico is extra relevant gezien de verwachte verschuiving van de immobiele en geïsoleerde robot naar een situatie met toenemende interactie en samenwerking van mens en robots.

---

62 http://www.nu.nl/internet/4161514/google-maakt-zelflerende-software-beschikbaar-iedereen.html
63 http://www.robots.nu/nederlandse-sam-robot-beveiligt-je-pand/
64 http://www.precisionmakers.com/nl/

De focus in dit rapport ligt op het risico op een botsing tussen mens (romp, hoofd en ledematen) en robot en het daaraan verbonden directe en indirecte arbeidsrisico. In de interviews waren wij benieuwd naar mogelijke kwetsbaarheden die de kans op dit risico verder vergroten. In Tabel 3 zijn specifieke kwetsbaarheden die tijdens de literatuurscan, de interviews, en de workshop naar voren zijn gekomen onderverdeeld in zeven thema's.

Tabel 3. Overzicht van de kwetsbaarheden die in de interviews genoemd zijn. Met een samenvatting van belangrijkste elementen die uit de interviews naar voren kwamen.

Kwetsbaarheden en dreigingen	**Samenvatting**
Taakverandering	Door de inzet van robots vindt er een verandering plaats van de taak die personen hebben. Als gevolg van deze verandering kunnen vaardigheden vervagen omdat deze alleen in noodsituaties moeten worden toegepast, kan cognitieve onder- of overbelasting plaatsvinden waardoor de kans op fouten wordt vergroot, of fysieke overbelasting optreden omdat de taken die overblijven zeer repetitief zijn waarbij de robot het tempo bepaald.
Onvoorziene situaties	Bij het ontwerp van een robot probeert men met alle mogelijke scenario's rekening te houden. Dit is vaak echter onmogelijk omdat dit afhankelijk kan zijn van het uiteindelijke (foutieve) gebruik van de robot, het spontaan onvoorzien handelen van de mens, zich onverwacht andere situaties voordoen, de software op onverwachte manier interacteert met andere software, of omdat er simpelweg niet aan gedacht is.
Vertrouwen in de machine	Personen hebben over het algemeen een groot vertrouwen in de capaciteiten en het functioneren van machines en technologie. Deze machines en de software die hen bestuurt, worden echter door personen gemaakt en kunnen dus fouten bevatten. Maakt een robot altijd betere keuzes en wie bepaalt waar deze keuzes op gebaseerd zijn?
Gedeelde verantwoordelijkheid	Bij de inzet van een robot zijn meer partijen betrokken: de ontwikkelaar van de robot, de systeemintegrator, de installateur, en de uiteindelijke gebruiker. Onduidelijkheid in waar verantwoordelijkheden voor veilig gebruik liggen kan ertoe leiden dat niemand deze op zich neemt.
Regulatory gaps	Technologische ontwikkelingen gaan snel en laten zich niet altijd goed voorspellen, waardoor het moeilijk is om wet- en regelgeving up-to-date te houden. Zo zijn er bijvoorbeeld nog geen richtlijnen voor zelfstandig rijdende machines, terwijl deze al wel op de markt zijn. Een achterhaald normenkader kan de ontwikkeling van grotere veiligheid tegenwerken.
Non-compliance	Tot nu toe lijken de meeste ongelukken met robots gerelateerd te zijn aan het negeren van veiligheidszones of het overtreden van veiligheidsinstructies. Inefficiënte procedures of veiligheidsfuncties kunnen hierbij een rol spelen, omdat de gebruiker op zoek gaat naar manieren om de veiligheidsmaatregelen te omzeilen.
Cybersecurity	Potentieel zwakke ICT-beveiliging is een duidelijke kwetsbaarheid waardoor de dreiging van hackers of overname van de besturing actueler wordt. Met name grote robots kunnen gevaar opleveren zodra de besturing niet meer werkt of wordt overgenomen.

4.4.1 Taakverandering (belasting/ vervaging vaardigheden)

Robots vervangen niet altijd personen op de werkvloer, maar waar robots worden toegepast vindt er wel een verandering plaats voor de taak van de mens. Op dit

moment zijn robots vaak afhankelijk van de mens om te kunnen functioneren, bijvoorbeeld voor het toeleveren van halfproducten en materialen en om controle uit te voeren op het proces. Deze taken die voor de mens overblijven, worden vaak als saai en oninteressant werk gezien en brengen meerdere implicaties met zich mee zoals het verliezen van vaardigheden en onder- of overbelasting.

Omdat een robot veel taken op zich neemt kunnen bepaalde vaardigheden van de medewerkers vervagen. Wanneer zich een niet-normale situatie voordoet is het dan nog de vraag of mensen tijdig en goed kunnen reageren. Dit is bijvoorbeeld het geval bij zelfrijdende auto's waar je als chauffeur moet kunnen ingrijpen in een bepaalde noodsituatie. Echter, ook met industriële robots moeten medewerkers nog wel kunnen handelen wanneer de robot uitvalt of kapot gaat.

Door de uitholling van de taken voor de mens wordt zijn werk minder attractief en is er een grotere kans op concentratieverlies met als gevolg het maken van fouten. Hierdoor kunnen gevaarlijke interacties ontstaan met de robot. Dit wordt ook wel als cognitieve onderbelasting gezien.

Cognitieve overbelasting kan plaatsvinden wanneer mensen een monitortaak moeten uitvoeren die meer robots tegelijk betreft. Hierbij kan het gebeuren dat bepaalde meldingen niet of te laat worden gezien waardoor een onveilige situatie ontstaat.

Tot slot is er het gevaar van fysieke overbelasting. Denk hierbij bijvoorbeeld aan repetitief en eenzijdig werk waarbij de robot het tempo bepaalt. De industrie wil vaak robots die zo snel mogelijk werken. De fysieke capaciteit van de mens kan dan een ondergeschikte rol spelen als ondersteuner van de robot.

4.4.2 Onvoorziene situaties

Een robot die excelleert in zijn functie kan een gevaar voor de mens worden als de robot wordt ingezet in een context waar die niet voor bedoeld is. Bijvoorbeeld een bewakingsrobot die bedoeld is voor het rondrijden op een lege bedrijfsvloer en wordt gebruikt wanneer het bedrijf in werking is met personen op de werkvloer. Anderzijds kan de robot ook terecht komen in een situatie waar in de programmering geen rekening mee gehouden is. Neem bijvoorbeeld autonome landbouwrobots die in principe op mensvrije locaties werken. Deze machines hebben vaak geen sensoren om personen te 'zien'. Toch kunnen onbevoegden zich op de akkers bevinden waar robots actief zijn.

Bij het ontwerp van een robot alle mogelijke scenario's voorzien die zich mogelijk kunnen afspelen, is vaak een onmogelijke taak. De mens is ten slotte behoorlijk onvoorspelbaar. Toch is het belangrijk om bij het ontwerp van iedere robot bij onvoorziene situaties stil te staan. Robots die een zware last moeten verplaatsen kunnen direct of indirect[65] gevaar opleveren voor eventuele personen in de buurt, maar ook een veilige assemblagerobot kan onveilig worden als deze een mes moet hanteren voor zijn functie. Het hoeft dus niet de robot te zijn die per se onveilig is, maar de uiteindelijke toepassing.

[65] Een zware last kan van een robot vallen, maar de robot kan ook tegen een opslagstelling aanrijden waardoor opgeslagen materiaal op een mens op enige afstand van de robot kan vallen.

Verder is ‘management of change’ belangrijk bij het upgraden en integreren van bestaande en nieuwe systemen. Ondanks dat alle machines/apparaten individueel CE gemarkeerd zijn, kunnen door het samenknopen van systemen en daarmee de toenemende complexiteit nieuwe, complexe interacties ontstaan. Bijvoorbeeld een noodstop die niet meer werkt omdat er nieuwe verbindingen in het systeem zijn aangebracht waar de noodstop geen invloed op heeft.

Gelukkig zijn er ook situaties die wel kunnen worden voorzien, maar waar niet altijd aan wordt gedacht. Bijvoorbeeld onveilige situaties tijdens onderhoud, omdat hier tijdens het ontwerp geen rekening mee gehouden is. Een simpel voorbeeld dat genoemd werd is een hoge robot waarbij een monteur op onveilige hoogte onderhoud moet plegen. Het delen van veiligheids-gerelateerde informatie heeft op sectorniveau nog ruimte voor verbetering, bijvoorbeeld door het delen van ‘best practices’.

4.4.3 Vertrouwen in de machine

Volgens een expert hebben mensen over het algemeen teveel vertrouwen in het functioneren van machines en technologie. Als voorbeeld wordt het internet aangedragen: mensen nemen vaak informatie die ze online vinden voor waar aan (ongeacht de bron). Toch is alle technologie door mensen gemaakt. Zo ook de software die een robot bestuurt; ook in deze software kunnen fouten zitten wat tot onverwacht gedrag van de robot kan leiden. Robotsoftware moet getest, maar ook goed worden onderhouden.

Verder kan men zich afvragen wie moet bepalen wat voor keuzes een robot maakt. Stel dat de robot in een situatie komt waar een ongeval onvermijdelijk is. Kiest de robot dan voor een beperkt ongeval (met mogelijk dodelijke afloop voor een persoon) of kiest de robot voor een potentiele onveiligheid van meer personen? Kunnen dit soort keuzes rationeel worden geprogrammeerd? Klopt de assumptie dat een robot altijd betere keuzes maakt, of moet de mens altijd in staat zijn deze te kunnen overrulen?

4.4.4 Gedeelde verantwoordelijkheid

Het samenstellen, configureren, installeren en programmeren van robots worden vaak uitbesteed. Als gevolg daarvan kunnen er situaties ontstaan waarbij de uiteindelijke gebruiker van de robot weinig tot niets weet over de exacte instructies van de robot en zijn functioneren. Daardoor kan een werknemer worden geraakt door een onverwachte beweging, of waarin de gebruiker niet weet wat hij of zij moet doen bij een storing. Waar liggen de verantwoordelijkheden om dit soort situaties te voorkomen, bij de ontwikkelaar(s) van de robot, de installateur, of bij de uiteindelijke gebruiker? Een andere situatie is wanneer een ZZP’er een robot inzet bij een ander bedrijf, wie is er dan verantwoordelijk voor de veiligheid? Een expert uitte zijn zorg dat onduidelijkheid in deze verantwoordelijkheden ertoe kan leiden dat niemand deze op zich neemt.

4.4.5 Regulatory gaps

Een grote kwetsbaarheid die naar voren kwam tijdens de interviews betrof de invloed van wet en regelgeving. Omdat de technologische ontwikkelingen zo snel

gaan, lopen wet- en regelgeving, waarbij aanpassingen vaak via een traag proces worden doorgevoerd, al snel achter.

Een voorbeeld dat genoemd werd is het feit dat er nog geen richtlijnen bestaan voor zelfstandig rijdende machines. Toch zijn er al meerdere voorbeelden bekend van dergelijke robots op de markt[66]. Zo weidt bijvoorbeeld OSHA wel een hoofdstuk uit aan industriële robots en veiligheid, maar heeft dit hoofdstuk voornamelijk betrekking op niet mobiele robots[67]. Naarmate meer partijen met autonoom voortbewegende robots aan de slag gaan, wordt de kans groter dan er ondeugdelijke ontwerpen op de markt komen en daarmee onveilige situaties ontstaan. Verder kan het gebruik van een oud normenkader de ontwikkeling van betere veiligheid tegenwerken wanneer die wordt toegepast op nieuwe technologieën.

4.4.6 Non-compliance

De meeste ongelukken met robots lijken gerelateerd te zijn aan het overtreden van veiligheidszones of instructies. Met andere woorden, de gebruikers houden zich niet altijd aan de veiligheidsrichtlijnen. De kans hierop wordt vele malen groter wanneer de opgestelde procedures inefficiënt of onzinnig lijken te zijn of wanneer een veiligheidsfunctie te vaak foutieve alarmen afgeeft (bijvoorbeeld wanneer een machine stopt als er een vogel langs vliegt). Experts geven aan dat in deze situaties irritaties ontstaan bij de gebruikers en de kans groter is dat deze gaan kijken naar manieren om deze veiligheidsmaatregelen te negeren, omzeilen of zelfs om aanpassingen te maken aan de robot. Tijd is namelijk geld en mensen willen niet geïrriteerd raken door ‘nutteloze’ tijdverspilling tijdens hun werk. Zeker voor kleine bedrijven of zelfstandigen kan dit een rol gaan spelen.

4.4.7 Cybersecurity

Indien er sprake is van zwakke ICT beveiliging vormt dit een kwetsbaarheid waardoor de dreiging van hackers of overname van de besturing reëler wordt. Experts herkennen het risico dat ontstaat als een robot wordt gehackt. Zeker zelf voortbewegende robots kunnen potentiele wapens worden. Cybersecurity staat op de agenda bij leveranciers, echter het is moeilijk 100% veiligheid te garanderen gezien de snelheid waarmee de industrie zich ontwikkelt. Een voorbeeld van hoe deze kwetsbaarheid kan ontstaan is de toegang tot het netwerk voor leveranciers die op afstand onderhoud aan robots willen kunnen plegen.

4.5 Beheersmaatregelen

In deze paragraaf geven wij een overzicht van de verschillende beheersmaatregelen die uit de interviews naar voren zijn gekomen. De beheersmaatregelen zijn onderverdeeld naar de levenscyclus van robots. De experts leken vooral veel winst te zien tijdens de ontwerpfase van een robot. Bij het veilig ontwerpen van een robot kunnen veel risico’s worden verminderd.

---

[66] Bijvoorbeeld autonome grasmaaiers (http://www.precisionmakers.com/) en bewakingsrobots (http://www.robots.nu/nederlandse-sam-robot-beveiligt-je-pand/)

[67] https://www.osha.gov/dts/osta/otm/otm_iv/otm_iv_4.html

Tabel 4 geeft een overzicht van de beheersmaatregelen per fase van de levenscyclus en onderverdeeld in de categorieën van de arbeidshygiënische strategie. Dit is een ruwe onderverdeling omdat er natuurlijk ook overlap kan bestaan waarbij beheersmaatregelen niet exact in één van de categorieën past. Verder zijn binnen elke categorie de beheersmaatregelen geordend op basis van het belang dat ze werd toegewezen tijdens de werkgroep (aangegeven met '*'). De focus van de experts lag op bron-aanpakken en collectieve of individuele maatregelen; er zijn geen persoonlijke beschermingsmiddelen genoemd tijdens de workshop.

De tabel geeft eveneens een indicatie van welke bedreigingen of kwetsbaarheden de beheersmaatregelen kan verkleinen. De meeste beheersmaatregelen lijken gericht op het voorkomen van non-compliance of onvoorziene situaties.

Vervolgens geven wij een toelichting per fase met betrekking tot de belangrijkste benoemde beheersmaatregelen.

Tabel 4. Overzicht van de beheersmaatregelen die in de interviews en tijdens de workshop zijn genoemd. Onderverdeeld naar fase van de levenscyclus.

Levenscyclus	Beheersmaatregelen		Voorbeeld aangepakte kwetsbaarheid en/of dreiging
Ontwerp/ Engineering			
Bron aanpak	✓	Bij ontwerp rekening houden met de functie van de robot, bijvoorbeeld door het uitvoeren van een risicoanalyse voor elke denkbare toekomstige toepassing (******)	Onvoorziene situaties
	✓	Het betrekken van de uiteindelijke gebruikers (de medewerkers die met de robot moeten werken) bij het ontwerp, voor het benutten van kennistaken en het creëren van een draagvlak voor acceptatie (***)	Onvoorziene situaties
	✓	Implementeren van de drie wetten van Asimov (**)	Regulatory gaps
	✓	Rekening houden met gebruiks- en onderhoudsergonomie bij het ontwerp van de robot (**)	Onvoorziene situaties
	✓	Software wordt virtueel getest (*)	Gedeelde verantwoordelijkheid
	✓	Bij ontwerp rekening houden met onderhoudswerkzaamheden die aan de robot moeten worden gepleegd, bijvoorbeeld door de periferie van de robot mee te nemen in ontwerp	Taakverandering
Collectieve maatregelen	✓	Implementeren van een goed bereikbare noodstopfunctionaliteit in het ontwerp. Waarbij de robot veilig tot stilstand komt (safe modus) (*)	Onvoorziene situaties
	✓	Het delen van ‘best practices’ sector breed en tussen sectoren	Non-compliance
	✓	Ontwikkel gestandaardiseerde of geharmoniseerde symbolen ter ondersteun van instructies voor het werken met robots	Non-compliance
	✓	Transparantie omtrent bevoegdheden en competenties rondom het ontwerp, samenbouw, onderhoud en ontmanteling van de robot	Non-compliance
	✓	Gebruik maken van de best beschikbare technologie en software in het ontwerp	Onvoorziene situaties/ cybersecurity
	✓	Gebruik waar mogelijk gecertificeerde onderdelen	Onvoorziene situaties
Individuele maatregelen		*Tijdens de workshop niet aangedragen.*	
Persoonlijke beschermingsmiddelen		*Tijdens de workshop niet aangedragen.*	
productie tot configuratie			
Bron aanpak	✓	Borging veilig gedrag, veiligheidscultuur en -kennis bij het personeel dat de robot moet configureren (*****)	Non-compliance
	✓	Het verzorgen van een intrinsiek veilige arbeidsomgeving voor installatie, samenbouw en onderhoud, door onnodige risico’s – op basis van een risico analyse- te voorkomen (*)	Non-compliance
Collectieve maatregelen	✓	Communicatie met- en tussen onder andere de veiligheidskundige, klant en leverancier over veilig gebruik van de robot	Onvoorziene situaties
	✓	Aanvullende instructies voor de robot leveren in verband met de integratie van verschillende componenten	Onvoorziene situaties
Individuele maatregelen	✓	De interfaces om robots te programmeren en bedienen standaardiseren	Non-compliance
Persoonlijke beschermingsmiddelen		*Tijdens de workshop niet aangedragen.*	

Levenscyclus		Beheersmaatregelen	Voorbeeld aangepakte kwetsbaarheid en/of dreiging
Gebruik			
Bronaanpak	✓	Veiligheid mens is prioritair, dan pas zelfbehoud van het product of robot (= Asimov)	Vertrouwen in de machine
	✓	Het werkproces inrichten vanuit de mens ondersteund door de robot, en niet andersom	Taakverandering
	✓	Het uitvoeren van een Taak-Risico analyse	Onvoorziene situaties
Collectieve maatregelen	✓	Het delen van 'best practices' sector breed en tussen sectoren (**)	Onvoorziene situaties
	✓	Implementeren van good housekeeping en zorgen voor onder andere een schone werkvloer	Non-compliance
	✓	Richten op gebruiksgemak en gemakkelijk programmeren en configureren (*)	Non-compliance
	✓	Intern periodieke en systematische controle of veiligheidssystemen nog goed werken uitvoeren (*)	Gedeelde verantwoordelijkheid
	✓	Intern periodieke en systematische conformiteitsbeoordeling aan veiligheidseisen uitvoeren (*)	Onvoorziene situaties
	✓	Training effectief volgen die door de leverancier wordt verzorgd en zorgen voor interne opvolging van noodzakelijke trainingen en opleidingen (*)	Gedeelde verantwoordelijkheid
	✓	Geven van geschrevenen mondelinge voorlichting en instructies aan medewerkers die met de robot gaan werken en zorgen dat deze begrepen zijn	Non-compliance
	✓	Uitvoeren van een risicoanalyse, en het opstellen van een plan van aanpak omtrent het gebruik van robots (hulpmiddelen online, digitale vragenlijst)	Onvoorziene situaties
	✓	Monitoren en registreren van ervaringen (en het terugkoppelen van deze informatie aan de leverancier)	Onvoorziene situaties
	✓	Het op orde hebben van de cybersecurity met betrekking tot de datacommunicatiestromen van en naar de robot	Cybersecurity
	✓	Opstellen van voorschriften en gedragsregels met betrekking tot de omgang met robots op de werkvloer	Non-compliance
	✓	Gebruik maken van verbeterloops om continue verbetering na te streven voor de inzet van robots	Non-compliance
	✓	Monitoren op afwijkingen in programmatuur en tijdig bijstellen	Onvoorziene situaties
Individuele maatregelen	✓	Het geven van feedback aan medewerkers bij overtreding van veiligheidsregels (*)	Non-compliance
	✓	Aanspreekgedrag stimuleren op de werkvloer zowel op onveilig werken met robots als op gewenst gedrag	Non-compliance
Persoonlijke beschermingsmiddelen		*Tijdens de workshop niet aangedragen.*	
Onderhoud			
Bron aanpak		*Tijdens de workshop niet aangedragen.*	
Collectieve maatregelen	✓	Lock-out (LoTo) procedures die garanderen dat de robot onder controle staat van de onderhoudsmedewerker (***)	Vertrouwen in de machine
	✓	Het uitvoeren van een Taak-Risico analyse (**)	Onvoorziene situaties
	✓	Opstellen van onderhoud regimes	Non-compliance
	✓	Registeren van gevaarlijke situaties en hier terugkoppeling op geven	Gedeelde verantwoordelijkheid
Individuele maatregelen	✓	Goede communicatie tussen gebruiker en leverancier vooraf aan onderhoudswerkzaamheden (over eventuele noodzakelijke veiligheidsmaatregelen) en het opstellen van een plan van aanpak (***)	Onvoorziene situaties
	✓	Gebruik maken van een Last Minute Risk Analysis (LMRA)	Onvoorziene situaties
	✓	Het invoeren of verplichten van een werkvergunning voor het plegen van onderhoud	Non-compliance
Persoonlijke beschermingsmiddelen		*Tijdens de workshop niet aangedragen.*	

Levenscyclus		**Beheersmaatregelen**	**Voorbeeld aangepakte kwetsbaarheid en/of dreiging**
Vernieuwing			
Bronaanpak	✓	Zorg dat robots aan te passen zijn naar nieuwe wet en regelgeving of nieuwe hard- of software (om veroudering te voorkomen) (*****)	Regulatory gaps
Collectieve maatregelen	✓	Toezien dat eventueel hergebruik van oude componenten in nieuwe installaties verantwoord gebeurt (*)	Onvoorziene situaties
	✓	Richtlijnenregimes ter bevordering van tijdige hernieuwing invoeren	Onvoorziene situaties
Individuele maatregelen		*Tijdens de workshop niet aangedragen.*	
Persoonlijke beschermingsmiddelen		*Tijdens de workshop niet aangedragen.*	
Afvoeren			
Bron aanpak	✓	Op veilige wijze vernietigen van software en configuratiegegevens (overschrijven of componenten vernietigen) (*)	Cybersecurity
	✓	Voorkomen dat afgevoerde oude (onveilige) robots kunnen worden gebruikt	Non-compliance
Collectieve maatregelen	✓	Kennis verkrijgen van wat de gevaren zijn tijdens het ontmantelen van de robot (*****)	Gedeelde verantwoordelijkheid
	✓	Het scheiden van zeldzame (aard)metalen en kunststoffen omwille van de: toxiciteit van dit soort ‘afval’ (***)	Gedeelde verantwoordelijkheid
	✓	Transparantie over de milieubelasting van de overgebleven componenten	Gedeelde verantwoordelijkheid
Individuele maatregelen		*Tijdens de workshop niet aangedragen.*	
Persoonlijke beschermingsmiddelen		*Tijdens de workshop niet aangedragen.*	

4.5.1 Ontwerp en Engineering

In de workshop werd duidelijk dat de experts geloven dat de belangrijkste beheersmaatregelen al tijdens de ontwerpfase gebeuren. Een belangrijke maatregel is dat er al bij het ontwerp van een robot goed wordt nagedacht over de uiteindelijke functie die de robot moet verrichten en het onderhoud dat aan de robot moet worden uitgevoerd. Zo moet, conform de Europese Machinerichtlijn 2006/42/EG, er bij het ontwerpen van een nieuwe robot (lees machine) een risicoanalyse plaatsvinden op basis van de geplande toepassing. Zo zou het bijvoorbeeld kunnen dat de verfdampen die bij een verfrobot ontstaan een gevaar voor de mens opleveren. Bij een andere robot kan een verhit oppervlakte tot verbranding leiden. Een goede voorkomende aanpak zou zijn om de uiteindelijke gebruikers te betrekken bij deze fase om hun kennis te benutten.

Bovenstaande is in aansluiting op de Europese Machinerichtlijn 2006/42/EG die stelt dat risico analyses moeten worden uitgevoerd om de machine (in dit geval betreft het dan een robot) zodanig te ontwerpen dat op basis van de verwachte toepassing, maar ook mogelijk misbruik, van de robot de geïdentificeerde gevaren - die in de gehele levenscyclus kunnen plaatsvinden- zoveel mogelijk worden weggenomen. Voor robots die veel met personen moeten samenwerken kan bijvoorbeeld worden gedacht aan het implementeren van stootkussens of aan het lichter of minder sterk maken van de robot. Op deze manier zal er geen (of minder) schade optreden mocht er toch een botsing met een mens (direct risico) of met een voor de mens gevaarlijk object (indirect risico) plaatsvinden. Aangezien robots op dit moment nog niet worden genoemd in de Europese Machinerichtlijn 2006/42/EG (bijlage 4), moet de fabrikant zelf aantonen of de robot voldoet aan de essentiële veiligheidseisen (bijlage 1), zonder hierbij een onafhankelijke partij te hoeven betrekken. Verder schrijft de richtlijn voor dat eventueel restrisico moet worden beschreven bij de instructies (bijlage 1, lid 1.7.4.2, onderdeel l).

Een ander voorbeeld is een vrij rond bewegende robot die ‘by design’ langzamer en zichtbaarder is gemaakt als reactie op de klantwens om de robot zich ook tussen personen te laten voortbewegen. Ook kan het gedrag van een robot voorspelbaarder worden gemaakt met behulp van verkeersregels voor tijdens normale werkuren in plaats van het berekenen van de kortste route.

Verder is het van belang dat tijdens het ontwerp van een robot ook rekening wordt gehouden met de ergonomie. Door tijdens de ontwerpfase al rekening te houden met de personen die uiteindelijk met de robot moeten gaan werken of in hun werkgebied kunnen komen kunnen veel gevaren, zowel die tijdens normaal gebruik als tijdens onderhoud, al in het ontwerp van de robot worden weggenomen. Zo kan fysieke overbelasting bij gebruik van een exoskelet worden voorkomen door vooraf te kijken naar de limieten van de mens en waarvoor het skelet precies zal worden gebruikt. De snelheid en versnellingen van de bewegingen kunnen daar op worden aangepast.

Zelfs in een zogenaamde ‘lights-out’ fabriek waar geen mensen meer betrokken zijn bij het primaire proces, zal de human factor ook een rol spelen. In een dergelijke fabriek zullen personen nodig zijn voor het monitoren van de robots en voor onder andere het plegen van onderhoud, reparaties of foutdiagnoses. Met betrekking tot

de monitoringstaak zal het een uitdaging zijn om cognitieve onder of overbelasting te voorkomen door zodanig ondersteuning te bieden dat het werk interessant en uitdagend blijft (ook kan de focus liggen op specifiek inrichten van een werkplek voor medewerkers met een beperking of bijzonder talent). Hiervoor moet het operator systeem worden geoptimaliseerd door te kijken waar de cruciale fouten die niet mogen worden gemaakt liggen en daar ondersteuning te bieden. Hierdoor zal wel een bepaald kennisniveau noodzakelijk zijn om met het operatorsysteem te mogen werken. Met betrekking tot de onderhoudstaak zal het van belang zijn dat de robot zodanig is ontworpen of geplaatst dat hier veilig onderhoud aan kan worden gepleegd (denk bijvoorbeeld aan werken op hoogte).

Adaptieve automatisering is het concept waarbij software de mens die met de robot werkt monitort en zo de snelheid van het proces kan aanpassen om overbelasting te voorkomen. Hierdoor blijft de mens in controle van het werkproces en zal de acceptatie van de robot op de werkvloer groter zijn.

Twee specifieke technologische aspecten waar tijdens de ontwerpfase van een robot over moet worden nagedacht, kwamen uit de interviews naar voren: de sensoren en een noodstopfunctie.

Historisch gezien, wordt er vanuit veiligheidsoptiek gebruik gemaakt van een fysieke barrière tussen mens en robot. Tegenwoordig hoeven robots niet meer volledig te worden afgeschermd omdat ze sensoren hebben. De robot kan met deze sensoren de aanwezigheid van personen detecteren en gaat langzamer draaien of stilstaan als een persoon in reikwijdte van de robot komt. Het voordeel van deze sensoren is dat ze personen ook veilig houden op die momenten dat de robots moeten worden benaderd, bijvoorbeeld tijdens onderhoud. Als de intrinsieke veiligheid van componenten niet kan worden aangetoond zou men toch moeten terugvallen op het plaatsen van een fysieke barrière als extra veiligheidsmaatregel.

Naast het voorkomen van botsingen kunnen sensoren ook worden gebruikt om vast te stellen of aan alle randvoorwaarden voor veiligheid wordt voldaan. Bijvoorbeeld om te bepalen of iemand op de besturingsstoel zit bij een ‘driver-assisted vehicle’. Dit kan bijvoorbeeld helpen in de landbouwsector waar het heel verleidelijk is voor de boeren om in- en uit te stappen van de langzaam rijdende semiautonome trekker.

De fysieke noodstopknop waarmee een robot direct kan worden stilgelegd is een voor de hand liggende beheersmaatregel. Idealiter kan deze noodknop ook op afstand worden bediend. Op deze manier kan direct worden ingegrepen wanneer een gevaarlijke situatie dreigt te ontstaan. Zo krijgt bijvoorbeeld bij tests met landbouwrobots altijd één persoon de taak om met de noodknop in de buurt van de robot te lopen. Dit moet op dat moment ook de enige taak van die persoon zijn. Hierbij ontstaat natuurlijk wel het risico van een potentieel geestdodende taak waarbij de kans op afleiding en fouten groter wordt.

Tot slot zal het van belang zijn om robots en de veiligheidsfuncties continu door te ontwikkelen en op de hoogte te blijven van de meest recente technologische mogelijkheden. Stootbumpers en lasers om een robot te laten stoppen als de robot ergens tegen aan dreigt te rijden zijn de eerste stappen richting meer veiligheid. Nieuwe ontwikkelingen, waaronder intuïtieve programmatuur (bijv. fuzzy logic),

bewegen zich echter richting slimmere robots die kunnen voorspellen wat bewegende objecten zoals een mens gaan doen in de ruimtelijke interactie met de robot. Andersom kan dan met het gedrag van de robot de mens om zich heen worden gestuurd als de robot duidelijk zijn doel en richting kenbaar maakt. Zo zouden omstanders eerder opzij stappen voor de robot als deze met een constante snelheid recht vooruit beweegt dan wanneer de robot weifelend tussen omstanders door probeert te manoeuvreren.

In een gestructureerde omgeving is dit makkelijker te bewerkstelligen dan bijvoorbeeld buiten. Buiten moeten robots personen ook kunnen onderscheiden van bijvoorbeeld bewegende voorwerpen als takken of een opwaaiend stuk papier en kunnen schaduwbeelden leiden tot een onnodige stop. Een ander voorbeeld is het kunnen bepalen dat er niet volledig hoeft te worden geremd als er een vogel op het pad zit; als er snelheid terug wordt genomen zal het probleem zichzelf waarschijnlijk oplossen.

Deze ontwikkelingen zullen uiteindelijk leiden tot minder ‘false alarms’ als gevolg van veiligheidsfuncties en daarmee wordt de robot mensvriendelijker en veiliger voor de mens. Hiermee wordt de kans verkleind dat er irritaties bij de gebruiker optreden alsmede een vermindering van non-compliance met de veiligheidsvoorschriften. Echter, naarmate de robot slimmer wordt, neemt de noodzaak toe om bepaalde regels, zoals de drie wetten van Asimov, in de robot te programmeren. Dit lijkt echter nog niet noodzakelijk te zijn in de nabije toekomst.

4.5.2 Productie, levering, samenstellen, installatie en configuratie

In de interacties met robots wordt de deskundigheid van medewerkers die zich met de robot bezig houden in alle fasen van de levensduur belangrijk. Het geven van heldere en juiste instructies zijn daar een onderdeel van en vallen onder de verantwoordelijkheid van werkgevers en/ of fabrikanten. Een uitdaging die in de workshop naar voren kwam is dat er vaak meerdere fabrikanten bij een robot betrokken zijn: Zo kunnen er verschillende fabrikanten betrokken zijn voor de robot zelf, het besturingssysteem, en de software separaat. Uiteindelijk zal de robot in de handel moeten worden gebracht onder de verantwoordelijkheid van een fabrikant. Deze verantwoordelijkheden staan in de machinerichtlijn 2006/42/EG benoemd en bestaan er onder andere uit dat de robot moet voldoen aan de essentiële veiligheids- en gezondheidseisen (bijlage 1) en moet de robot voorzien zijn van een gebruiksaanwijzing (artikel 5).

In de workshop kwam verder de borging van veilig gedrag, veiligheidscultuur en -kennis bij het personeel dat de veiligheid van een robot configureert en implementeert als belangrijkste beheersmaatregel naar voren in deze fase. Met andere woorden, het is van belang dat een robot correct wordt samengesteld, geconfigureerd en geplaatst bij een bedrijf. Eén manier om dat te bewerkstelligen is om te garanderen dat hier vakbekwame personen mee aan de slag gaan.

Verder werd het trainen van de gebruiker in veilig gebruik van de robot benoemd als belangrijke beheersmaatregel. Naast het testen of de robot goed geplaatst is en werkt, moeten leveranciers, in samenwerking met systeemintegratoren en installateurs, instructies meegeven over hoe de robot moet worden gebruikt. De verantwoordelijkheid voor het volgen van deze instructies ligt zowel bij de opdrachtgever (de uiteindelijke gebruiker van de robot) en de opdrachtnemer

(leverancier/installateur). De opdrachtnemer moet de instructie geven en de opdrachtgever moet zeker zijn van het feit dat de medewerkers voldoende weten over de robot. Dit impliceert een bepaald kennisniveau bij de opdrachtgever. Zeker nu er in toenemende mate minder met fysieke afscheidingen gaat worden gewerkt, is de voorlichting en communicatie belangrijk.

Een voorbeeld hiervan is verkeersregels die worden opgesteld om botsingen met autonoom voortbewegende robots te voorkomen. De regels worden opgesteld in overleg met de ontwerper, maar de verantwoordelijkheid dat alle medewerkers (en derden zoals bezoekers) deze regels kennen ligt bij de organisatie waar de robot wordt gebruikt.

Leveranciers leiden klanten vaak ook op om met de geleverde robots om te kunnen gaan en deze te programmeren.

Verder zou het delen van ‘best practices’ vaker moeten gebeuren tussen integrators en installateurs.

4.5.3 Gebruik

Ook tijdens de gebruiksfase kwam het delen van ‘best practices’ naar voren als belangrijke beheersmaatregel. Verder hadden de experts geen voorkeur voor bepaalde beheersmaatregelen maar werden verschillende beheersmaatregelen als van belang benoemd. Dit waren onder andere het belang van housekeeping (asset management) rondom de robot of het gemak waarmee een robot kan worden gebruikt of ingesteld.

Verder kwam de training in het gebruik van de robot naar voren. Het is belangrijk dat diegene die met een robot moet werken weet hoe de robot werkt en wat die doet. Hij of zij moet voor zichzelf de vraag kunnen beantwoorden: “Welke bewegingen kan de robot maken en wat betekent dit voor mij?”. Medewerkers moeten de robot volledig begrijpen, weten hoe ze met een storing moeten omgaan en weten hoe ze het risico voor zichzelf kunnen minimaliseren. Hierbij zijn training, voorlichting en interne opvolging van essentieel belang.

Robotisering heeft echter ook gevolgen voor de vraag naar schoolopleidingen. Met toenemende robotisering zal de samenstelling van het personeelsbestand van organisaties gaan veranderen door veranderingen in de taakeisen. Er zal meer vraag zijn naar technisch gekwalificeerde personen aan de fabricage/proceslijn die complexe(re) taken uitvoeren en storingen (preventief) kunnen oplossen.

Qua werkbelasting zijn er twee stromen te onderscheiden:

1. Het fysiek zware en monotone werk zal met de tijd worden geëlimineerd en monitoringstaken zullen toenemen. Het gevraagde opleidingsniveau zal daarmee hoger worden bij organisaties waar met robots wordt gewerkt. Hierbij is het belangrijk dat technologische en digitale componenten snel een grotere rol krijgen in opleidingen. Het algemene kennisniveau zal zich dus moeten aanpassen aan de (technologische) ontwikkelingen in de maatschappij.
2. Het werk wordt saai en eentonig indien de mens een assistent van de robot wordt die saaie taken moet uitvoeren om de robot te laten functioneren (bijv. een kratje recht zetten dat niet door de robot wordt herkend). Het is dus van belang om de taken van mens en machine goed te definiëren zodat het ook

duidelijk is wanneer en hoe de mens moet ingrijpen. Nu wordt vaak het werkproces ontworpen vanuit wat technisch mogelijk is. Beter is het om het werkproces in te richten vanuit het oogpunt van de werknemer die wordt geassisteerd door robots.

Verder geldt momenteel voor de meeste robots dat zij de omgeving beter kunnen 'begrijpen' als de omgeving gestructureerd is. Waar mogelijk zouden personen dus moeten worden weggehouden van de plekken waar robots werken.

Als organisatie kun je een risico-inventarisatie en –evaluatie gericht op robots uitvoeren. Op basis van de uitkomst kan vervolgens de werkplek en het proces veiliger worden ingericht en een bijbehorend plan van aanpak worden opgesteld.

Tot slot kunnen interne procedures een belangrijke beheersmaatregel zijn tijdens het gebruik van een robot. Denk hierbij aan 'life saving rules'[68], aanspreekgedrag, feedback bij overtreding van veiligheidsregels, periodieke controle of veiligheidssystemen nog werken en een periodieke conformiteitsbeoordeling (aan veiligheidsvoorschriften).

Tot slot kunnen verbeterloops helpen om proces breed continu naar een hoger niveau te streven. Hierbij kijk je tijdens het gehele proces naar onvolkomenheden en hoe deze te verbeteren.

Het wordt steeds moeilijker om een concrete handleiding te schrijven waar een gebruiker zich aan moet houden om veilig gebruik te maken van een robot of daarmee samen te werken. Dit omdat in tegenstelling tot een magnetron, de functie en de context waarin gebruik wordt gemaakt van robots zich steeds moeilijker eenduidig laat definiëren. Dit maakt het ook lastiger om te bepalen waar de taken om bepaalde risicofactoren te beheersen, moeten worden neergelegd.

4.5.4 Onderhoud

Een belangrijke beheersmaatregel voor onderhoud betreft de communicatie met de klant, of dit nu vooraf is over eventueel noodzakelijke veiligheidsmaatregelen, het opstellen van een formeel job safety plan of het aanvragen van een werkvergunning. Op deze manier kan men uitsluiten dat de onderhoudsmedewerker onnodig risico loopt.

Daarnaast is het belangrijk dat de onderhoudsmedewerker te allen tijde de robot kan uitschakelen of overrulen. Een goede aanpak is bijvoorbeeld het principe van LTT[69]:

- Lock out: het uitzetten en daarna op slot zetten van een machine,
- Tag out: het plaatsen van een tag waarom en wie de machine heeft uitgezet,
- Try out: toetsen of de machine echt uitstaat.

Verder houden leveranciers ook eigen statistieken bij met betrekking tot gevaarlijke situaties. Dit zijn vaak meldingen door personen die in aanraking komen met

[68] Zie bijvoorbeeld de Life Saving Rules van Shell: http://www.shell.nl/sustainability/veiligheid.html
[69] http://www.hamer.net/algemeen/lock-tag of http://www.verbondpk.nl/Arbocatalogus/LTT

verlaagde functionele veiligheid als gevolg van veroudering of omdat de toegang tot de robot niet goed is. Hier worden klanten dan voor gewaarschuwd.

Daarnaast gaan de huidige mobiele robots regelmatig terug naar een synchronisatiepositie. Hier kunnen afwijkingen worden gedetecteerd op basis waarvan de robot kan worden uitgeschakeld of worden 'bijgesteld'.

Ook zullen door de organisatie safety- en (cyber)securityeisen moeten worden gesteld aan medewerkers en diensten van derden zoals onderhoud, al dan niet op afstand, van de robot(s).

4.5.5 Vernieuwing

Voor de vernieuwingsfase werd door de experts over het algemeen gesteld dat het niet heel anders is als wat voor de installatiefase geldt. Wel kwam naar voren dat het belangrijk is om flexibel te blijven richting toekomstige ontwikkelingen. Bijvoorbeeld wanneer wet- en regelgeving zodanig verandert dat een bepaalde toepassing van een robot niet meer mag of juist mogelijk wordt als de randvoorwaarden gunstig veranderen. Of wanneer een beter onderdeel op de markt komt, niet de gehele robot hoeft te worden vervangen.

4.5.6 Afbreken/ontmantelen en afvoer

Voor de laatste fase, afbreken/ontmantelen en afvoer, kwamen twee beheersmaatregelen naar voren als belangrijk. Ten eerste moeten er duidelijke instructies zijn over wat de specifieke gevaren kunnen zijn tijdens de fysieke ontmanteling van een robot. De tweede beheersmaatregel betrof de toxiciteit van het resulterende 'afval' van een robot: de zeldzamen (aard)metalen en kunststoffen moeten goed worden gescheiden.

Verder moet worden voorkomen dat configuratiegegevens zoals digitale certificaten, netwerkadressen en wachtwoorden op straat komen te liggen waardoor onbevoegden zich toegang tot de bedrijfsprocessen en de (andere) robots daarin kunnen verwerven.[70]

[70] https://www.security.nl/posting/13460/Hardeschijven+energiebedrijf+op+eBay+beland

5 Discussie

Dit project draagt bij aan de bewustwording van het aan robotisering verbonden risico voor personen bij de arbeidsplaatsen in de diverse industrieën waar wordt ingezet op (verdere) robotisering van het productieproces. Met dit rapport reageren wij op de kennisvraag zoals gesteld door SZW:

Wat zijn de risico's van robotisering op de werkplek en welke beheersmaatregelen zijn denkbaar om het genoemde risico te beheersen?

De ontwikkelingen op het gebied van robotica gaan snel, wat ook blijkt uit de toenemende nationale en internationale aandacht voor robots, robotisering, industrie 2.0 en smart industrie. Dit is te zien in publicaties als De Ingenieur[71], de Lichtkogel[72] en Control Design[73], maar ook in de rapporten van bijvoorbeeld het Rathenau-instituut[74]. Daarnaast vinden er steeds meer lezingen en bijeenkomsten plaats over robotisering[75]. Dit onderzoek vindt plaats aan de voorkant van de voorziene ontwikkelingen van de functionaliteit van diverse meer potente robottypen. De uitkomsten van het onderzoek kunnen goed worden meegenomen in de ontwikkeling van nieuwe robots.

Bij de experts waren er weinig tot geen ongevallen bekend tussen robots en personen. Dit komt overeen met een recent rapport van Control Systems waarin werd aangegeven dat er sinds 1 januari 1997 slechts 25 ernstige robot gerelateerde arbeidsincidenten in de VS hebben plaatsgevonden waarvan minder dan 20 met dodelijke afloop (in verhouding tot 4.679 werk gerelateerde incidenten met een dodelijke afloop in 2014)[76]. Wel werd duidelijk dat incidenten ook (of juist) buiten het normale gebruik van de robot om gebeuren. Bijvoorbeeld tijdens het plaatsen, testen, of onderhouden van de robot[77]. Dit benadrukt het belang om naar de gehele levenscyclus van de robot te kijken.

Naarmate robots meer gaan worden ingezet is de kans echter groot dat dit aantal zal toenemen. Naast botsing kan men ook nog denken aan indirecte risico's zoals het raken door een robot van bijv. een stelling of stapels opgeslagen goederen waardoor op indirecte wijze een onveilige situatie ontstaat (gescheurd vat chemicaliën, zware goederen die omvallen). Of door verminderde concentratie door

---

71 M. Seijlhouwer, Meelevende machines, De Ingenieur, 2016, jaargang 128, no 4, pg 12-19,

72 Robots in de openbare Ruimte, Lichtkogel nr 1, 2016. https://staticresources.rijkswaterstaat.nl/binaries/Lichtkogel%202016%20nr1%20Robots%20in%20de%20openbare%20ruimte_tcm21-80156.pdf

73 Collaborative Robots in Control Design for Machine Builders (2016).

74 L. Royakkers, F. Daemen, R. van Est (2012), Overal robots: Automatisering van de liefde tot de dood, Rathenau instituut en
R. van Est , L. Kool (2015) Werken aan de robotsamenleving, Rathenau instituut. https://www.rathenau.nl/nl/publicatie/werken-aan-de-robotsamenleving.

75 Bijv. een bijeenkomst over de inzet van robots door hulpdiensten bij calamiteiten.

76 Bacidore, M. (2016). The new world of collaborative robots. *Control Design for Machine Builders. Special report: Collaborative robots*.

77 Zie ook de OSHA technical Manual Sectie 4, hoofdstuk 4: https://www.osha.gov/dts/osta/otm/otm_iv/otm_iv_4.html

bijvoorbeeld cognitieve onder belasting. Er is nog maar weinig bekend over de psychosociale gevolgen van het werken met robots (e.g. motivatie, verlies van kwaliteit van werk).

Dit rapport heeft een inventarisatie van dreigingen en kwetsbaarheden opgesteld en van beheersmaatregelen die hiertegen kunnen worden genomen in verschillende levensfases van de robot. In dit hoofdstuk bespreken we de belangrijkste bevinden en enkele implicaties van de resultaten uit dit rapport.

5.1 Robotica als containerbegrip

Eén van de eerste dingen die opviel tijdens de interviews met de experts, is dat robots en robotica een problematisch begrip zijn. Wat wordt er precies bedoeld met robots, over welk type robot hebben we het? Hierover moest eerst overeenstemming ontstaan voordat het gesprek kon plaatsvinden.

Robotica is een containerbegrip waar veel verschillende toepassingen onder vallen. Zelfs met de door ons gehanteerde definitie, een robot is een machine die kan worden geprogrammeerd, sensoren heeft, en een bepaalde gradatie van mobiliteit heeft waardoor de robot autonoom een taak kan uitvoeren, kan men nog steeds zowel intelligente robots zoals te zien in films (e.g. I robot) scharen, maar ook een simpele wasdroger. De laatste is immers een machine die kan worden geprogrammeerd om autonoom de was te drogen en gebruikt hierbij sensoren om het programma te verkorten als het om minder was of vervuiling gaat.

Vervolgens kwamen we interessante tegenstellingen tegen in de gehanteerde definities van de experts. Zo benoemde één expert dat zolang een machine niet buiten zijn programmatuur treedt, het geen robot is. Terwijl een andere expert stelde dat zelfs de meest geavanceerde robot uiteindelijk niets anders dan een verzameling aan geprogrammeerde regels zal zijn.

Een afgeleide kwestie is vervolgens wat de uiteindelijke mogelijkheden zijn op het gebied van robotica en wat we hiervan kunnen verwachten op de korte termijn. Dit lijkt heel afhankelijk van de expert die je spreekt. Binnen de industrie lijkt men vooralsnog pragmatisch te kijken naar de robots die ze nodig hebben/willen. Het proces moet sneller, preciezer, gemakkelijker en goedkoper, maar natuurlijk ook veilig verlopen. In sectie 5.6 gaan we verder in over de verwachte toekomst voor de industriële robot.

Wat voor nu van belang is, is dat de term robot niet onderscheidend genoeg is als werkdefinitie. Zelfs binnen de ‘industriële robot’ is grote variatie te vinden in type robot die afhankelijk is van hun toepassingsvorm.

5.2 Veilig ontwerp

De experts waren het over het algemeen eens dat het ontwerp van de robot het belangrijkste moment is om de meeste onveiligheden uit het systeem te krijgen. Dit staat gelijk aan het principe van de bronaanpak uit de arbeidshygiënische strategie.

Tot specifieke aanbevelingen kwam het echter niet, de reden hiervoor is simpel: een universeel veilig robotontwerp bestaat niet. Welke aspecten noodzakelijk zijn hangt grotendeels af van de functie waar de robot voor gaat worden ingezet. Een lichter frame voor robots die veel met personen samenwerken kan de schade van een botsing minimaliseren, maar bij een robot die zware lasten moet tillen en verplaatsen zal een lichter frame tot een te lage structurele integriteit leiden waardoor geheel andere onveilige situaties ontstaan (laten vallen van de last bijvoorbeeld).

Het algemene advies is dan ook dat het belangrijk is om van te voren risicoanalyses uit te voeren op de beoogde toepassing (of toekomstige toepassingen) en deze mee te nemen in het ontwerp en de meest geschikte technologieën gebruiken.

Een robot bestaat over het algemeen uit twee delen. De machine of armen die het werk doen en het controlesysteem. Bij het analyseren van de risicoaspecten moet men niet alleen naar het uitvoerende deel van de robot kijken, maar juist ook naar het controlesysteem. Is dit goed beveiligd tegen ongeautoriseerde invloeden van buitenaf (e.g., hackers), zitten er geen programmeerfouten in, is het up to date, wie heeft er allemaal toegang? De integriteit van de besturingssoftware bepaalt voor een groot gedeelte of de robot veilig kan worden gebruikt evenals in hoeverre de robot is afgeschermd voor ongewenste invloeden van buitenaf. Hetzelfde geldt voor de aansturing van gevaarlijke elementen die de robot bij zich heeft, zoals laser, stralingsbron, en machinerie.

Een ander algemeen advies dat naar voren is gekomen, is dat er zou moeten worden gestreefd naar een optimalisering van de samenwerking tussen mens en robot. Robots zijn zeer precies, snel, sterk en goed in repetitief werk. Mensen zijn creatief, goed in beslissingen nemen, flexibel en adaptief. Wanneer het beste wordt genomen van beide kanten kan er optimaal worden geprofiteerd van een samenwerking tussen mens en robot. Als dit wordt nagelaten en medewerkers afhankelijk worden van de robot of indien de werkuitdaging voor personen wordt weggenomen, bestaat het risico dat in abnormale situaties niet meer adequaat kan worden gereageerd, of dat de overgebleven taken niet meer uitdagend genoeg zijn waardoor de kans op fouten toeneemt.

Verder waren de experts unanimiteit over het feit dat een robot altijd vergezeld moet zijn van een noodstopfunctionaliteit. Dat wil zeggen, de mens moet te allen tijde de robot op een veilige wijze kunnen uitschakelen of overrulen. Hiermee blijft de mens in controle (en verantwoordelijk) voor het gehele proces.

Ook de rol van sensoren is belangrijk. Zeker nu fysieke afscheidingen verdwijnen, zal het vertrouwen op sensoren steeds groter worden. Sensoren hebben de ontwikkelingen in de functionaliteit van robots kunnen bijhouden[78]. Het is van belang dat sensoren steeds beter worden en de achterliggende software steeds ‘slimmer’. Denk bijvoorbeeld aan 3d-scanners die herkennen wanneer een menselijke voet in een bepaalde radius stapt[79]. Deze sensoren worden bijvoorbeeld

[78] Bacidore, M. (2016). The new world of collaborative robots. *Control Design for Machine Builders. Special report: Collaborative robots*.

[79] Voorbeeld van product op de markt: https://www.sick.com/media/dox/9/79/879/Industry_guide_Building_Safety_and_Security_en_IM0036879.PDF

ook voor de bewaking van gebouwen ingezet. Maar er kan ook ‘out of the box’ worden gedacht door bijvoorbeeld een ‘veiligheidsschild’ rondom de mens te creëren waar robots op reageren door stil te gaan staan zodra dit schild in de buurt komt [80].

5.3 De human factor

Al moet de voorkeur liggen bij het ontwerpen van een inherent veilig ontworpen robot om zo de bron van het risico aan te pakken, zal ook de menselijke factor in beschouwing moeten worden genomen. Een belangrijke verantwoordelijkheid ligt hierbij bij de organisatie die de robots inzet. Dit kan binnen organisaties door de richtlijnen die bij een robot worden gegeven te volgen, eventuele trainingen te volgen die noodzakelijk zijn en deze regelmatig updaten. Het gebruiken van ter zake kundig personeel of organisaties voor samenstellen, installatie en configuratie, onderhoud en verwijdering.

Ook voor organisaties is het belangrijk om de robots mee te nemen in risico-inventarisaties en -evaluaties. Organisaties kunnen hierin worden geholpen door methoden als een elektronische vragenlijst of checklist. Een gecodificeerde vragenlijst helpt bij de risico-inventarisatie en –evaluatie en kan tevens helpen bij het aantonen van de compliance met vigerende wet- en regelgevingsaspecten. Tevens kunnen ‘best practices’ worden aangereikt.

We moeten waken voor een te groot vertrouwen in de robot waar dit nog niet terecht is. De programmering en de onderliggende software waarop een robot handelt, is ten slotte mensenwerk. De correctheid hiervan moet worden gecontroleerd om fouten te voorkomen en er voor te zorgen dat deze goed blijft werken. Wie bepaalt of controleert straks op basis van welke argumenten een robot (morele) keuzes gaat maken?

Een risico dat wordt genoemd is dat robotisering met zich meebrengt dat de programmatuur van robots dadelijk bepalend is voor wat wel en niet mogelijk is. Neem bijvoorbeeld een administratieve robot. Deze heeft veel moeite om uitzonderlijke situaties te behandelen waar mensen weinig problemen mee hebben omdat deze buiten ‘zijn programmatuur’ treedt.

Tegelijkertijd kan een organisatie al gauw verleren hoe het proces kan plaatsvinden zonder de inzet van een robot. Een voorbeeld dat gegeven werd is hoe het overstappen op een manueel proces moeizaam verliep nadat het automatische check-in systeem uitviel op een vliegveld.

Naarmate robots meer taken op zich nemen, kunnen we potentieel meer afhankelijk worden van de robot. Enerzijds omdat de programmering bepalend kan worden, anderzijds omdat de menselijke vaardigheden vervallen. Zelfrijdende auto’s vallen echter nog terug op de chauffeur in bepaalde situaties en zelfs in een ‘lights out’ fabriek (waar alleen maar robots op de werkvloer staan) zijn personen nodig om de

[80] http://www.engineersonline.nl/producten/elektrotechniek/veiligheid/id25604-veilige-werkplek.html

robots te monitoren en het proces te controleren. Waardoor er op die plekken werkgelegenheid ontstaat.

Met andere woorden, voorlopig lijkt de robot nog afhankelijk te zijn van de mens. Het lijkt van belang om de menselijke factor goed te integreren in het ontwerp van de robot en het uiteindelijke werkproces, om de robot optimaal te benutten.

5.4 Wet- en regelgeving

5.4.1 Wet- en regelgeving algemene robottoepassingen

Voor de mechanische kant van de huidige robots lijkt de bestaande wet- en regelgeving alsmede normeringen grotendeels voldoende te zijn. Vanuit normalisatie worden huidige robots niet als nieuw gezien maar als machines[81] met een elektrotechnisch onderdeel (bijv. het praten en communiceren van robots) en niet-elektrotechnische delen. Echter omdat er sprake is van een samenstel dat deels valt buiten de huidige normeringen, is de bestaande wet- en regelgeving niet toereikend. Zo valt programmatuur en het risico voor onveiligheid daarvan nu buiten de machinerichtlijn. Wel zijn er ontwikkelingen waarbij zowel ICS- (International Classification for Standards) als ISO- (International Organization for Standardization) normen voor robots uitbrengen. Zo gaan de standaarden ISO 10218-1:2011, ISO 10218-2:2011, en de ISO 13482:2014 specifiek over de veiligheidsvoorschriften voor industriële en zorgrobots.

In de praktijk groeien normen en standaarden mee met ontwikkelingen in de maatschappij. Voorlopig zal dit goed gaan omdat veel technologische ontwikkelingen nog niet rijp zijn voor de markt. Neem bijvoorbeeld de zelfrijdende auto: er zijn nu wel al veel testpilots, maar het zal voorlopig nog even duren voordat iedereen een zelfrijdende auto heeft[82]. Enerzijds geeft dit nog de tijd om de wet- en regelgeving hieromtrent op orde te krijgen, anderzijds is er nog geen relevante jurisprudentie die richting kan geven aan de wet- en regelgeving. Het is zaak om belangrijke ‘regulatory gaps’ te identificeren en deze tijdig op te vullen.

Het ontbreken van wet- en regelgeving rondom autonome onderwater-, vaar- en voertuigen kan vanuit robotica gezien worden als een belangrijke ‘regulatory gap’. Dit omdat er verschillende type autonoom voortbewegende robots op de markt zijn waar nog geen regulering voor bestaat. Ook in het buitenland bestaat hier nog geen regulering voor. Ook experimenten met robots kunnen in conflict komen met de huidige wet- en regelgeving die niet voorziet in autonome(re) robots in de buitenruimte. Autonome voertuigen zijn een duidelijk voorbeeld waarbij de markt voorloopt op wet- en regelgeving, de robots worden namelijk al door verschillende partijen verkocht[83]. Het ontwerp van dit soort robots gebeurt dan op eigen initiatief en gezond verstand waarbij de klantvraag leidend kan zijn in wat de robot uiteindelijk mag en moet kunnen. Vaak vult de markt dit soort gaps op. Wanneer

---

[81] Ook OSHA bestempeld robots als machines: https://www.osha.gov/Publications/Mach_SafeGuard/chapt6.html

[82] Zo heeft de huidige generatie van zelfrijdende auto’s nog moeite met slechte weersomstandigheden. Zie bijvoorbeeld: https://static.googleusercontent.com/media/www.google.com/en//selfdrivingcar/files/reports/report-1215.pdf.

[83] Zie bijvoorbeeld http://www.precisionmakers.com/nl/; en http://robotsecuritysystems.com/

meer bedrijven met dezelfde innovatie bezig zijn gaan deze samen, soms ook met overheden, om de tafel zitten om hierover na te denken. Dit hoeft niet direct een probleem te zijn, maar kan wel tot onveilige situaties leiden naarmate meer partijen zich zonder afspraken en standaarden op dit gebied wagen.

5.4.2 Wet- en regelgeving specifiek binnen de landbouwsector

Ook in de landbouwsector speelt dit probleem. Zij hebben een rapport[84] opgesteld betreffende de wet- en regelgeving en aanbevelingen rondom de toepassing van autonome trekkers. In dat rapport wordt de conclusie getrokken om voorlopig semiautonome voertuigen in te zetten conform richtlijn 2009/127/EG (Richtlijn machines voor de toediening van pesticiden) waarin wordt vereist dat er sprake moet zijn van het monitoren en de mogelijkheid om in te grijpen. Er wordt teruggegrepen op deze richtlijn omdat autonome trekkers soms ook spuitmachines voorttrekken, en omdat de Trekker- (2003/37/EG[85]) en de Machinerichtlijn (2006/42/EG) nog geen uitsluitsel geven.

De complexiteit hier is dat de trekker een voertuig is en onder die wet- en regelgeving valt en de voortgetrokken machinerie, als mechanisatie wordt beschouwd. Met de ontwikkelingen van bijvoorbeeld een door een automatisch voertuig voortgetrokken plukrobot zal de scheidslijn tussen de trekker-richtlijn en de machinerichtlijn worden overschreden.

Ook kan de autonomie van een landbouwrobot qua ruimte en afstand worden beperkt door bijvoorbeeld stringentere wet- en regelgeving zoals die voor drones in de maak is. Legitieme ontwikkelingen voor robots kunnen daardoor onbedoeld worden afgesneden, tenzij er een vergunningsoptie in de wet- en regelgeving in wordt gebouwd.

Mogelijk is hier een grotere rol voor vakbonden weggelegd. Als voorbeeld geldt CEMA, een Europese vakbond ontwikkelaars van landbouwmachines, die zich hard maakt voor gebalanceerde wet- en regelgeving binnen de EU, onder andere om het mogelijk te maken om slimme technologieën toe te passen.

5.4.3 Noodzaak van tijdige governance

Het is belangrijk voor de ontwikkeling van nieuwe robots dat het wettelijk kader er gereed voor is. Bij het ontwikkelen van robots en nieuwe toepassingen moet al in een vroeg stadium worden gedacht aan wetgeving. Anders kan de wetgeving in een later stadium in de weg zitten omdat het product niet aantoonbaar veilig is. Dit concept heet ‘Lock in’ en kan producten doen falen. Voor startups is het belangrijk om te weten aan welke wet- en regelgeving moet worden voldaan afhankelijk van wat je wilt ontwikkelen. Zo zal bijvoorbeeld een robot die voor de voedingswarensector wordt ontwikkeld niet uit bepaalde materialen mogen bestaan.

---

[84] Heijting, Kempenaar, & Nieuwenhuizen, (2013). Veiligheid van autonome voertuigen in open teelten. Wet- en regelgeving en aanbevelingen voor de veiligheid. *PPL project nr 79/ZGLE.11.0108.*

[85] Sinds het rapport is uitgekomen is er een nieuwe trekker richtlijn uitgekomen Regulation No 167/2013 (http://eur-lex.europa.eu/legal-ontent/EN/TXT/HTML/?uri=CELEX:32013R0167&from=sv). Deze richtlijn benoemt autonome trekkers ook niet.

Maar ook toepassingen zoals de zelfrijdende voertuigen die Domino's pizza's wil gebruiken voor het laten bezorgen kunnen in de problemen komen met wet- en regelgeving[86].

5.5 Ketenaansprakelijkheid

Om tot een veilige robot te komen is de gehele keten die betrokken is bij de levenscyclus van de robot nodig. Dit begint bij een veilig ontwerp voor de robot van de leverancier. Vervolgens moeten de systeemintegrators de robot met veiligheid voorop samenstellen, installeren en configureren bij de klant met bijbehorend certificaat. De robot moet vervolgens op veilige wijze worden gebruikt, systematisch en op veilige wijze worden onderhouden (inclusief de software) en tot slot op veilige wijze vernieuwd of op de juiste wijze gedemonteerd en worden afgevoerd wanneer de robot verouderd is.

Hier ligt een gedeelde verantwoordelijkheid om de risico's uit te bannen. Iedere partij moet binnen zijn eigen proces verantwoordelijk (en gecertificeerd) aan de slag gaan en een risico-inventarisatie en –evaluatie uitvoeren, maar het houdt niet op bij de eigen werkzaamheden. De leverancier geeft instructies mee aan de integrator, de integrator traint de klant in het gebruik van de robot, de klant geeft feedback over het functioneren van de robot. Inmiddels worden industriële robots op afstand vanuit bijvoorbeeld India onderhouden[87]. Door gezamenlijk te opereren en elkaar goed te informeren kan het proces worden geoptimaliseerd.

5.6 Toekomst industriële robot

Terugvallend op onze definitie gesteld aan het begin van het rapport:

> *"Een robot is een machine die kan worden geprogrammeerd, sensoren heeft, en een bepaalde gradatie van mobiliteit heeft waardoor de robot autonoom een taak kan uitvoeren."*

zien we dat er voor de industriële robot op elk van de genoemde sleutelwoorden ontwikkelingen kunnen worden verwacht in de nabije of verdere toekomst.

Naarmate mens en robot nauwer gaan samenwerken zullen betere *sensoren* nodig zijn die de omgeving accuraat in kaart brengen en de robot goed in staat stelt zijn omgeving te lezen. Hierbij gaat het dus niet alleen om 'end of arm tooling' (waarmee een robot problemen kan herkennen; bijvoorbeeld wanneer een product verkeerd ligt of het verkeerde product wordt aangeboden), maar ook om veiligheidssensoren die een botsing kunnen voorkomen, of een mens herkennen wanneer deze in de buurt komt.

Naast betere sensoren zal ook de onderliggende programmatuur verder worden ontwikkeld en zal kunstmatige intelligentie worden toegevoegd om adequaat te kunnen reageren op de input. Hierbij kan men denken aan de noodzaak dat de robot ook de intentie van een mens om zich heen kan beoordelen om een botsing te voorkomen (bijv. steekt die persoon wel of niet over?). Waar de grens ligt van de

[86] http://www.nu.nl/gadgets/4232354/dominos-wil-zelfrijdend-autootje-pizzas-laten-bezorgen.html
[87] Zie bijv. Angela Merkel en YuMi: https://www.youtube.com/watch?v=ytC9WC3ec_0

kunstmatige intelligentie die een robot (in de nabije toekomst) kan bereiken is moeilijk te bepalen. Voor een zelfdenkende robot die buiten zijn *programmatuur* kan stappen zal een geheel aparte verzameling aan beheersmaatregelen nodig zijn (denk bijvoorbeeld aan de drie wetten van Asimov), en zal samengaan met een keur aan maatschappelijke discussies (e.g., juridische autonomie van een robot, robotrechten?). De industrie lijkt niet per se te wachten op de uitkomst van dergelijke discussies en focust zich op het verbeteren van de efficiëntie en productiviteit door verdere robotisering. Een zelfdenkende robot is echter niet geheel ondenkbaar omdat een veiligere robot vooral lijkt te liggen in slimmere besturingssoftware van een dergelijke robot.

Tot slot zal ook het aantal *autonoom* voortbewegende robot toenemen op de werkvloer. Er zijn al verschillende autonome voortbewegende robots op de markt (e.g. autonome grasmaaiers of bewakingsrobots, maar ook al veel type automated guided vehicles (AGVs[88]), maar ook op de werkvloer worden ze al ingezet[89]. De huidige hype rondom zelfrijdende auto's zal er waarschijnlijk voor zorgen dat deze ontwikkelingen razendsnel gaan. Met de toename in flexibiliteit die een *bewegende* robot heeft ten opzichte van een robot die op een vaste locatie opereert, zal het aantal zelf voortbewegende robots rondom personen waarschijnlijk gaan toenemen.

De exacte snelheid waarmee deze technologieën zich ontwikkelen laat zich moeilijk voorspellen. De snelheid van innovatie is grotendeels commercieel bepaald. Zolang de technologie nog duur is, zal er niet zo snel een markt voor ontstaan wat verdere ontwikkelingen kan afremmen. Zodra de markt er is kan het echter heel snel gaan met technologische ontwikkelingen.

Het lijkt evident dat deze ontwikkelingen er aan komen, de vraag is voornamelijk wanneer. Het is daardoor van belang dat men zich goed voorbereid op deze komende verandering. Dit rapport geeft een inventarisatie van kwetsbaarheden en dreigingen die met deze ontwikkelingen gepaard gaan. Op basis daarvan is een overzicht opgesteld van beheersmaatregelen die hier tegen kunnen worden genomen. Op deze manier komen we weer een stap dichterbij een toekomstige generatie van robots die niet alleen sneller, beter, en slimmer is, maar ook veiliger zijn.

[88] AGVs zijn semiautonome robots of machines die een voor gedefinieerd traject volgen. Deze worden al veel toegepast in fabrieken en magazijnen.

[89] Bijvoorbeeld zelfrijdende transportwagens die de containers verplaatsen in de APM-terminal op Maasvlakte-2.

6 Ondertekening

Utrecht, 1 juli 2016

Naam tweede lezer:

J. van der Eerenbeemt MSc.

Ondertekening:

F.A. van der Beek MSc.
Projectleider

Autorisatie vrijgave:

Drs. H.C. Borst
Researchmanager

A Appendix: Protocol interviews

1. *Introductie en opening van gesprek*

2. *Huidige context uitvragen*
   - Wat is achtergrond met betrekking tot robots?
   - Met welk type robots werkt u? *of* Welke toepassingen van robots in het arbeidsdomein kent u?
   - In welke context? *of* In welke sectoren en/ of branches?
   - Wat zijn de voornaamste voordelen van deze robots?
   - Wat zijn de voornaamste gevaren voor arbeids-/persoonlijke veiligheid?
   - Hoe vaak komen gevaarlijke situaties voor? / Bent u bekend met (bijna)ongelukken?
   - Welke veiligheidsmaatregelen worden genomen?
   - Welke veiligheidsmaatregelen ontbreken naar uw idee?
   - Wat is de preferente risicomanagement strategie/ aanpak (life-cycle benadering, certificatie, verzekeren, etc.)?
   - Wordt er voldoende gecommuniceerd en gerapporteerd over potentiële Arborisico's in relatie tot robots?

3. *Nabije / verre (5-30 jaar) toekomst*
   - Welke ontwikkelingen verwacht u op het gebied van robotica?
   - Wat zullen de voornaamste voordelen zijn van deze ontwikkelingen?
   - Wat zullen de voornaamste gevaren zijn van deze ontwikkelingen?
   - Hoe worden onzekerheden in de ontwikkeling van robots gemanaged?
   - Welke extra/nieuwe veiligheidsmaatregelen zullen er dan (nu al) moeten worden genomen?

4. *Cyberrisico*
   - In hoeverre communiceren robots nu met andere robots ofwel communiceren ze draadloos?
   - Indien nee: wordt deze ontwikkeling (op korte termijn) verwacht?
   - Worden er al maatregelen genomen tegen eventuele cyberinbreuken? Zo ja, welke?
   - Wat is de invloed van de (werk)omgeving waarbinnen robots opereren op hun handelen?

5. *Afsluiting*
   - Wat is de rol van (pseudo) wet en regelgeving om dit te begeleiden?
   - Zijn er belangrijke andere actoren op dit gebied of documenten waar wij van af moeten weten?

B Appendix: Resultaten Workshop

Overzicht van de input op de posters tijdens de workshop. Nadien kon men met stickers de belangrijkste ideeën markeren. Met asterisken is per idee aangegeven hoeveel stickers er op geplakt waren.

Dreigingen

- Geen rekening houden met het feit dat een robot moet worden onderhouden (**)
- Wie mag wanneer overrulen? Mens – Robot
- Dilemma: Keuze voor beperkt ongeval (met eventuele dodelijke afloop mens) versus onveiligheid van velen
- Onverwachte (niet voorziene/geprogrammeerde) acties van mens of robot (*)
- De onlogische acterende mens (onvoorspelbaar)
- Basisveiligheid industrial control systems (of onveiligheid)
- Is het ontwerp “testbaar”/”bewijsbaar” veilig (**)
- Wanneer kunnen kwetsbaarheden optreden: Design (programmeren); systeem integratie; in bedrijfstellen; operatie; onderhoud (software upgrade); Afvoer
- Veiligheid bij mobiele robots in grote of openbare ruimte
- Machine (robot) in publieke ruimte
- Is de veiligheidsruimte bewijsbaar veilig indien meer robots (mobiel) samenwerken/ op de werkvloer opereren
- Idiot-proof maken robot? Nee, de mentaliteit van personen aanpakken, het veiligheidsniveau lager en de robot trager (**)
- Achterhaalde normenkaders belemmeren “betere veiligheid”
- Verlies werkgelegenheid
- Nieuwe gezondheidsrisico’s, fysieke over- of onderbelasting (****)
- Leidt taakverandering mens tot slechtere concentratie op werkplek en gevaarlijke interactie met mobiele robot?
- Uitholling van functies (waardoor minder attractief) bij mens-robot samenwerking
- Onderhoud en software updates: controleerbaarheid, certificatie veiligheid
- Onveiligheid door onderhoud software op afstand
- Gevoeligheid voor toegang/invloed van buiten: denk aan hacken/overnemen van besturing (**)
- Onderhoudsissues; aansprakelijkheidsissues
- Applicaties bepalen mate van gevaar, niet (alleen) de robot
- Toepassing versus verkeerde toepassing
- Snelheid versus veiligheid, smart industrie is hot
- Leer curve betekent onzekerheid: snel leren is noodzaak
- Security issues: …. (*)

Kwetsbaarheden

- Niet delen op brancheniveau van incidenten tussen actoren
- Hoe krijg je sector brede good practices in deze sector (of internationaal)

- Onvoldoende software kwaliteit (onverwacht gedrag)
- Kennis en kunde voor engineer of operator
- Zwakke ICT-beveiliging (risico voor manipulatie)
- Algoritme van de software betrouwbaar? Is ook door een mens bedacht! (*)
- Safety PLC, verkeerd programmeren (**)
- Hoe veilig te installeren, hoe veilig samen te stellen?
- Faalgedrag van mens en machine (tweezijdig): fail safe, damage tolerant (beide kanten op), full proof
- Dilemma: als ongeval onvermijdbaar is, welke keuze? Wie mag/moet dood!
- Falen sensor: wat dan? Noodsituaties en sensoren (bijv. mist) (**)
- Organisatorisch indien zzp'er een (ramenwas)robot inzet bij een bedrijf: wie is dan verantwoordelijk voor veiligheid? (**)
- Hoe kan veilig onderhoud worden verricht?
- Hoe kan ik alle situaties testen? Hoe weet ik wat alle mogelijke combinaties zijn? (*****)
  Weerstand bij gebruiker: Verlies autonomie, grotere/grote afhankelijkheid van proces die robot oplegt (**)
- Robot is sneller en beter/preciezer dan mens: hogere acceptatie door gebruiker (management), lagere acceptatie door (mede)werker
- Geen "Self protecting node" principe in 'keten' componenten
- Innovatiebeperking
- Veiligheidskundige geen gesprekspartner bij inkoop robot: gebrekkig kennisniveau (*)
- Interactie tussen robots (nu en in de toekomst)
- Gedrag werknemer/werker: intuïtieve besturing in relatie tot overnemend gedrag door robot
- Is de wijzigingslog van software/betrouwbaar?

Beheersmaatregelen

Ontwerp en engineering

- Service en functie gericht ontwerpen (******)
- Risico-inventarisatie
- Robot Laws Asimov (**)
- Noodstopfunctionaliteit: geen stroomonderbreking maar veilig stil gaan staan (safe modus) (*)
- Software virtueel testen (*)
- Periferie veilig ontwerpen
- Delen van best practices
- Gebruikers (medewerkers) betrekken bij ontwerp, vanwege kennistaken en acceptatie draagvlak (***)
- Ondersteun de instructies voor het werken met robots met gestandaardiseerde of geharmoniseerde symbolen
- Wie is bevoegd en competent tot ontwerp, samenbouw, onderhoud, ontmanteling?
- Ergonomisch ontwerpen (**)

Productie/levering en installatie

- Delen van best practices (**)
- RI&E
- Kwaliteitsborging bij opslag en transport
- Intrinsiek veilige arbeidsomgeving voor installatie, samenbouw en onderhoud (*)
- Taakallocatiecriteria: performance en mens (aantrekkelijk werk)
- Training in veilig gebruik (***)
- Borging veilig gedrag, veiligheidscultuur en -kennis bij het personeel dat veiligheid configureert en implementeert (*****)
- Protocol voor veilige installatie (*)
- Communicatie met/tussen veiligheidskundige, klant en leverancier
- Interfaces standaardiseren

Gebruik

- Housekeeping (*)
- Ease of use, ease of programming en configuren (*)
- Best practices (**)
- Training door leverancier en interne opvolging (*)
- Feedback bij overtreding veiligheidsregel, aanspreken op gedrag (*)
- Bijstellen afwijkingen
- Controle of veiligheidssysteem nog goed werkt (*)
- Periodieke conformiteitsbeoordeling (*)
- RI&E en plan van aanpak
- Veiligheid mens is prioritair, dan pas zelfbehoud van het product of robot
- Training en opleiding
- Incidenten registratie en monitoring

Onderhoud

- Goede communicatie tussen gebruiker en leverancier (*)
- Onderhoud is onderdeel van ontwerp en design
- Onderhoud regimes
- Competences, onderhoudsmarkt (*)
- Job safety plan met klant (**)
- Communicatie vooraf over veiligheidsmaatregelen voor onderhoud (**)
- Steigers bij werken op hoogte aan robots
- PBM's en maatregelen onderhoud
- Klimgordel en zekeren
- Lock-in procedures
- LMRA
- Mens kan altijd de robot uitschakelen of overrulen (***)

Vernieuwing

- In regelgeving meenemen: re-use van oude componenten in nieuwe installaties (*)
- Fusie tussen mens en machine of robot: ondersteuning in taken, enhancement (**)
- Flexibiliteit naar toekomstontwikkeling (*****)
- Richtlijnen regimes

Afbreken/ontmantelen en afvoer

- Scheiding zeldzame (aard)metalen en kunststoffen: nieuwe arbeidsrisico's door toxiciteit van 'afval' (***)
  Software en configuratie gegevens: veilige wijze vernietigen (overschrijven of componenten vernietiging) (*)
- Duidelijke instructies van de leverancier wat de gevaren zijn tijdens het ontmantelen (*****)
- Robot is universeel tot aan de flens: daarna is het applicatiespecifiek
- Wat is de milieubelasting van de overgebleven componenten?
- Hergebruik? Misuse tegengaan.