

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	17 mei 2015
Auteurs	Wouter Steijn; Eric Luijff; Dolf van der Beek (contactpersoon)
Exemplaarnummer	
Oplage	
Aantal pagina's	48
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

1	Inleiding	4
1.1	Leeswijzer	6
2	Aanpak	8
2.1	Literatuur- en internetscan	9
2.2	Interviews	10
2.3	Workshop	11
3	Robotica: afbakening van het rapport	13
3.1	Definitie robot	13
3.2	Industriële robot: nu	16
3.3	Industriële robot: toekomst	17
3.4	Type scenario's toepassing robots	19
3.5	Cyber-fysieke veiligheid	20
3.6	De rol van wet- en regelgeving	21
4	Interview- en workshopresultaten	25
4.1	Voordelen van robotisering	25
4.2	Definitie robots	25
4.3	Verwachte ontwikkelingen in nabije toekomst	26
4.4	Dreigingen en kwetsbaarheden	27
4.5	Beheersmaatregelen	31
5	Discussie	40
5.1	Robotica als container begrip	41
5.2	Veilig ontwerp	41
5.3	De human factor	42
5.4	Wet- en regelgeving	43
5.5	Ketenaansprakelijkheid	45
5.6	Toekomst industriële robot	46
6	Ondertekening	48

Bijlage(n)

A Appendix: Resultaten Workshop

B Kenniskaart

1 Inleiding

Al decennia lang spelen robots tot de verbeelding in toekomstvisioenen in films en boeken. 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 die die in 1961 in de autoproduktielijnen van General Motors zijn geïntroduceerd². 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 gevarenszone 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 die in sciencefiction boeken en films worden neergezet. Door deze verhalen is de beeldvorming van robots voor veel mensen gericht op machines met een menselijke vorm, die zich zichzelf kunnen voortbewegen, met mensen om kunnen gaan en op hun omgeving kunnen reageren.

Ondanks bovenstaande beperkingen introduceren de huidige industriële robots al nieuwe risico's op de werkvloer ondanks de definiëring van veiligheidszones of kooien. Dit werd afgelopen jaar nog maar eens duidelijk na een dodelijk ongeluk waarbij een arbeider door een robot werd doodgedrukt³. 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 stil⁴. Het is dus voorstelbaar dat in de nabije toekomst arbeiders ook met autonome robots zullen gaan samenwerken in omgevingen die niet meer tot een vaste locatie of kooi beperkt zal zijn. Ook zullen mensen en autonome robots samen door dezelfde ruimten bewegen.

Het is dan ook 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 Asimov⁵ 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

¹ https://en.wikipedia.org/wiki/Industrial_robot

² Martijn Wisse (2015). De robot de baas: De toekomst van werk in het tweede machinetijdperk. *Wetenschappelijke raad voor het regeeringsbeleid*. 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

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 gegeven worden, 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.

Daarboven is nog een principe, ook wel *nulde wet*, gedefinieerd: een robot mag geen schade toebrengen aan de mensheid, of toelaten dat de mensheid schade toegebracht wordt door zijn nalatigheid (https://nl.wikipedia.org/wiki/Drie_wetten_van_de_robotica).

garanderen? Maar ook morele dilemma'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?

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 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?

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

Assemblagelijnen



Lasrobot



Landbouwrobot



Zorgrobot



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 werknemers. In de huidige wet- en regelgeving is hierover nog niets opgenomen, dan wel conflicteert de wet- en regelgeving voor machineveiligheid bij strikte toepassing met het gebruik van (proces)automatisering. Rapportages in 2015⁶ en de in dit rapport opgenomen analyses, conclusies en aanbevelingen leveren inzichten op die kunnen fungeren als aanhaakpunten voor

⁶ Steijn, W., Luijff, H., Gallis, R., Opkomende risico's voor arbeidsveiligheid als gevolg van IT-koppelingen van en tussen arbeidsmiddelen, TNO rapport 2016 R10096; Luijff, H., Steijn, W., Quick-scan analysis of Directive 2006/42/EC with respect to the emerging cyber risk, (draft) TNO report, 2016; en Luijff, H., Steijn, W., Quick-scan analyse Arboret m.b.t. het toenemend cyberrisico, (concept) TNO rapport, 2016.

wijzigingen op nationaal en Europees niveau, in dit geval van de Arbowet, de Europese machinerichtlijn⁷ en dergelijke. Ook normalisatie-instituten zoals NEN, CEN/CENELEC en ISO voorzien in de komende jaren een grote impact door robotisering op standaardisering activiteiten. Dit zal gevolgen hebben op de verschillende Europese richtlijnen (machinerichtlijn, drukapparatuur, Personal Protective Equipment (PPE), etc.) en de daaraan gelieerde geharmoniseerde Europese normen. Het is van groot belang om met de betrokken bedrijven, overheden en kennis- en normalisatie-instituten een normalisatieagenda op te zetten voor wat betreft Robotica en Arbeidsomstandigheden. Dit rapport dient dan ook in eerste instantie ter ondersteuning van het Ministerie SZW en normalisatie-instituten bij het opzetten van een dergelijke nationale en internationale agenda.

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 autonoom bewegen over de werkvloer waar zich ook mensen 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 gebouwd worden om veilig te zijn voor de mensen waar ze voor zorgen⁸.

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 mensen 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?

1.1 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

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>

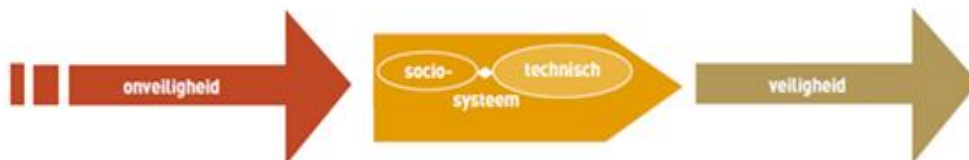
van kwetsbaarheden en mogelijke beheersmaatregelen voor bedrijven die robots bouwen en/of toepassen in de vorm van een kenniskaart.

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 korte 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 *risicobegrip* 'de kans dat een potentieel gevaar resulteert in een daadwerkelijk incident en de ernst van het letsel of de schade die dit tot gevolg heeft'¹⁰, ook 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 dan 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 potentiële dreiging resulteert in een daadwerkelijk incident geven de aanwezige kwetsbaarheden, en de ernst van het letsel of de schade die dit tot gevolg heeft'

⁹ VROM (2008). *Handreiking Security Management*.

¹⁰ Wikipedia: <https://nl.wikipedia.org/wiki/Risico> (23-12-2015)

Dreiging definiëren we hier in lijn met de definitie van de Privacycommissie¹¹ 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*”¹².

Het komen tot 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 korte 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 een framework 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 het gekozen framework, de levenscyclus, toe en hoe wij met dit framework tot een actoranalyse zijn gekomen om relevante partijen te betrekken bij de interviews en de workshop.

2.1.1 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 gecertificeerde, normalisatie-instituten.

¹¹ Lexicon van de Belgische Commissie voor de bescherming van de persoonlijke levenssfeer (CBPL): https://www.privacycommission.be/nl/lexicon#letter_d

¹² Hafkamp, W.H.M. (2008). Als alle informatie telt: een onderzoek naar kwetsbaarheden- en incidentenresponse bij ICT-organisaties. PhD dissertatie, Universiteit van Amsterdam: <http://dare.uva.nl/document/2/54173>

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. Hieronder staat het gehanteerde protocol. Vragen werden indien nodig aangepast aan de achtergrond van de geïnterviewde.

-
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?

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. Geïnterviewden werden direct aan het eind van het interview uitgenodigd en verder 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. 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 plakken in een overzicht. Afsluitend werd aan de deelnemers gevraagd om met stickers de belangrijkste ideeën te markeren. In Appendix A 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 actieagenda¹³ 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 precies op maat kan produceren. Of, zoals in de gezondheidszorg, 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) aan 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 algemeen¹⁴. Een fysieke robot kan dan beschouwd worden als een machine die is aangesloten op betere software, waardoor de mogelijkheden van wat de machine kan groter worden.

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

¹³ <http://www.smartindustry.nl/wp-content/uploads/2014/11/Smart-Industry-actieagenda-LR.pdf>

¹⁴ 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.

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, especially dangerous, repetitive or heavy tasks. A robot can be equipped with sensors to perceive its surroundings and adapt to new situations.*¹⁵.

*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*¹⁶.

*A **robot** is a mechanical or virtual artificial agent, usually an electro-mechanical machine that is guided by a computer program or electronic circuitry*¹⁷.

*An **industrial robot** is defined by ISO 8373 as an automatically controlled, reprogrammable, multipurpose manipulator programmable in three or more axes which may be either fixed in place or mobile for use in industrial automation applications*¹⁸.

Aan de hand van deze definities kunnen we stellen dat:

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

Het sleutelwoord in deze definitie is de autonomie van de robot die bepaald wordt door hoe deze geprogrammeerd is, wat voor sensoren de robot heeft, en hoe mobiel (of niet) de robot is. 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 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 ontwikkeld¹⁹. Wel komen deze multipurpose robots al dichterbij de buurt van robots met echte kunstmatige intelligentie die op hun omgeving kunnen reageren en daarmee kunnen interacteren. Het toevoegen van

¹⁵ IGI Global. Lesson 1. Humanoid robots.
<https://www.youtube.com/watch?v=3FXRw2CWACg&feature=youtu.be>

¹⁶ Martijn Wisse (2015). De robot de baas: De toekomst van werk in het tweede machinetijdperk. *Wetenschappelijke raad voor het regeeringsbeleid*. P 73.

¹⁷ <https://en.wikipedia.org/wiki/Robot>

¹⁸ https://en.wikipedia.org/wiki/Industrial_robot;
https://oshwiki.eu/wiki/A_review_on_the_future_of_work:_robotics

¹⁹ Zie bijvoorbeeld: <https://www.youtube.com/watch?v=8P9geWwi9e0>

‘emoties’ en beloning- en strafsystemen aan robots is een ander onderzoeksgebied om de kloof tussen mens en de robot als machine te verkleinen.²⁰

Voorbeeld programmering simpele taak “Pak en plaats”

Definieer punten P1–P5:

1. Veilig boven werkgebied (gedefinieerd als P1)
2. 10 cm boven bak A (gedefinieerd als P2)
3. In positie om een onderdeel uit bak A te pakken (gedefinieerd als P3)
4. 10 cm boven bak B (gedefinieerd als P4)
5. In positie om een onderdeel in bak B te leggen (gedefinieerd als P5)

Definieer programma:

1. Ga naar P1
2. Ga naar P2
3. Ga naar P3
4. Sluit gripper
5. Ga naar P2
6. Ga naar P4
7. Ga naar P5
8. Open gripper
9. Ga naar P4
10. Ga naar P1 en sluit af

Bron: https://en.wikipedia.org/wiki/Industrial_robot

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 opgepakt moet worden, 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 conflictvrij 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 zuignappen²¹. 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.

²⁰ Zie M. Seijlhouwer, Meelevende machines, De Ingenieur, 2016, jaargang 128, no 4, pg 12-19.

²¹ Bijv. een ramenwasrobot

Met betrekking tot autonome voertuigen in open teelten is het rapport Veiligheid van autonome voertuigen in open teelten²² interessant omdat het ingaat op de veiligheid van autonoom werkende machines in de precisielandbouw. Vigerende wet- en regelgeving waaronder de EU trekkerrichtlijn en de EU machinerichtlijn 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 gevaarlijk, zwaar en repetitief werk²³. 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 ze²⁴:

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

Parameters waarbinnen robots worden gedefinieerd en verbeterd kunnen worden zijn²⁵:

- over hoeveel assen (‘vrijheidsgraden’) 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 die ene taak waar ze voor worden ingezet, al neemt de flexibiliteit waarmee robots geprogrammeerd kunnen worden 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

²² S. Heijting, C. Kempenaar en A. Nieuwenhuizen, Veiligheid van autonome voertuigen in open teelten, PPL project 79/ZGLE.11.0108 (2013).

²³ <http://www.nrc.nl/next/2015/10/31/robot-wordt-eerder-arts-of-advocaat-dan-kapper-1551807>

²⁴ IGI Global. Lesson 1. Humanoid robots.

<https://www.youtube.com/watch?v=3FXRw2CWACg&feature=youtu.be>

²⁵ https://en.wikipedia.org/wiki/Industrial_robot

nog lang niet zo efficiënt als industriële robots die voor de uitvoering van één taak gebouwd zijn (zie bijvoorbeeld de DARPA Robotics Challenge²⁶).

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, redeneervermogen, adaptievermogen, lerend vermogen, emoties²⁷, 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 mensen, 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 leren²⁸.
- Project SPENCER is gericht op de ontwikkeling van robots met slimme interactiesystemen (bijv. een robot die verdwaalde reizigers op Schiphol begeleidt (2015))²⁹.
- Zorgrobot LEA die is ontwikkeld om ouderen te ondersteunen om zelfstandig te blijven functioneren³⁰.
- Robots die dienen als vermakers, koks en serveerders in een restaurant in China (2014)³¹.
- De Bigdog robot en de LS3 Legged Squad Support System die als een soort van rennende "lastdieren" zware spullen voor uitgestegen militairen kunnen vervoeren door ruw terrein³².
- 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)³³.
- De bewakingsrobot SAM³⁴.
- In het project 'Titan the robot' wordt er gefocust op robots als vermaak³⁵.

De namen van de projecten geven aan dat er naar een zekere mate van menselijkheid of mensomgeving in robots wordt nagestreefd. Wel zijn deze robots nog verre van gelijkwaardig met menselijke interactie. Zo komen ze nog niet in de

²⁶ (<https://www.youtube.com/watch?v=8P9geWwi9e0>)

²⁷ Zie M. Seijlhouwer, Meelevende machines, De Ingenieur, 2016, jaargang 128, no 4, pg 12-19,

²⁸ <http://www.aliz-e.org>

²⁹ <http://www.spencer.eu/>

³⁰ <http://www.robotcaresystems.com/wat-is-het/>

³¹ http://www.chinadaily.com.cn/m/jiangsu/kunshan/2014-08/08/content_18274963.htm

³² http://www.bostondynamics.com/robot_bigdog.html en de Youtube file "LS3 Robotic Pack Mule Field Testing by US Military"

³³ <https://www.youtube.com/watch?v=8P9geWwi9e0> - te zien is dat dit type robots nog relatief beperkt zijn qua efficiëntie.

³⁴ <http://www.robots.nu/nederlandse-sam-robot-beveiligt-je-pand/>

³⁵ <https://www.youtube.com/watch?v=cjFPFr9SswA>

buurt van de snelheid en efficiëntie waarmee huidige industriële robots hun taak uitvoeren. Dit kan echter alleen een kwestie van tijd zijn. 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 dan ook autonomer en adaptiever in de dynamische omgeving van een werkvloer worden. In deze omgeving zouden ze zich dan moeten aanpassen aan dynamische veranderingen van de omgeving (een container meer of minder, een tijdelijk geblokkeerde doorgang, enzovoorts), samen moeten werken met arbeiders en deze dynamisch moeten ontwijken bij het uitvoeren van hun eigen taken. Verder zouden ze eventueel kunnen switchen tussen taken om te kunnen gaan met producten die variëren in grootte, gewicht, kwetsbaarheid en positie.³⁶

Een belangrijk aspect is wat deze ontwikkelingen voor de veiligheid betekenen voor arbeiders in hun werkomgeving die gedeeld wordt 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 mensen 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 ook risicovoller zijn voor de veiligheid van de mens.

Verder bevat elke robot één of meer met de buitenwereld interacterende computersystemen en industriële control systems (ICS) die een cyberrisico met zich mee brengen. Meer informatie met betrekking tot dit specifieke risico en de aangrijpingspunten is respectievelijk te vinden in een recent TNO rapport³⁷, en in paragraaf 3.5.

Belangrijke drivers vanuit de industrie voor verdergaande robotisering zullen de functionaliteit en bruikbaarheid van de robots zijn. Vooralsnog zijn autonome of 'general purpose' robots echter nog niet concurrerend met de huidige industriële robots op het gebied van snelheid en efficiëntie. Het kan snel gaan als complete industrieën gaan inzetten op de ontwikkeling en grootschalige inzet van robots. Een dergelijke ontwikkeling zou vergelijkbaar zijn met de ontwikkeling van de zelfrijdende auto's die sneller is gegaan en gaat dan veel experts vooraf vermoeden.³⁸

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. De programmering wordt hier potentieel nog meer een black box 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

³⁶ Bijvoorbeeld het pakken van een onderdeel uit een bak waar de producten schot en scheef in liggen. Martijn Wisse (2015). De robot de baas: De toekomst van werk in het tweede machinetijdperk. *Wetenschappelijke raad voor het overheidsbeleid*. P 73.

³⁷ Steijn, W., Luijck, H., Gallis, R., Opkomende risico's voor arbeidsveiligheid als gevolg van IT-koppelingen van en tussen arbeidsmiddelen, TNO rapport 2016 R10096.

³⁸ <http://www.nrc.nl/next/2015/10/31/robot-wordt-eerder-arts-of-advocaat-dan-kapper-1551807>

zelfrijdend containertransport op bijvoorbeeld de APM containerterminal in Rotterdam, maar zou in de toekomst ook kunnen gebeuren op locaties waar zich meer mensen 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 en bij onverwachte weerstand bijvoorbeeld op de armbeweging de uitgeoefende kracht verminderen dan wel afbreken.

3.4 Type scenario's toepassing robots

Naar verwachting zal de wereldpopulatie aan mensen ruim negen miljard zijn in 2050³⁹. Met deze toenemende populatie en toenemende vergrijzing in de 'westerse wereld' groeit de vraag naar producten, diensten en zorg mee. 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. Hieronder geven wij een niet uitputtend overzicht van typen robots die nu of binnenkort gebruikt zullen worden en de sectoren waar deze robots gebruikt (kunnen gaan) worden, waarbij er mogelijke gevolgen zijn voor arbeidsveiligheid.

Type robots

- Lasrobots
 - Lasrobot: <https://www.youtube.com/watch?v=kbi2Jd4-mu8>
- Assemblagerobots
 - Assemblagerobot: <https://www.youtube.com/watch?v=JIC0SIkmbjk>
- Transportrobots (goederen/ plukken)
 - Robots in container terminal: <https://www.youtube.com/watch?v=22SvOhl47Tw>
 - Agrobot: <https://www.youtube.com/watch?v=LFfod3EYdqC>
 - Ziekenhuis: <https://www.youtube.com/watch?v=Q0gNDFXy8YI>
- Sociale robots (educatief/zorg)
 - Nao: <https://www.youtube.com/watch?v=aLMmGCwNfNk>
 - Alica: <https://www.youtube.com/watch?v=vlh73k4ybeo>
- Zorgrobots (bijv. tegen doorliggen)
 - <https://www.youtube.com/watch?v=wOzw71j4b78>
- Bedieningsrobots
 - Flying robots: <https://www.youtube.com/watch?v=cLY56vefkFE>
- Militaire robots
 - BigDog: <https://www.youtube.com/watch?v=afeBlgRF-4g>
- Veiligheidsrobots
 - Blusrobot: <https://www.youtube.com/watch?v=e3Z7kXLQRu0>
 - Bewakingsrobot: <http://www.robots.nu/nederlandse-sam-robot-beveiligt-je-pand/>

³⁹ <https://nl.wikipedia.org/wiki/Wereldbevolking>

Sectoren (niet uitputtend)

- Zorg
- Horeca
- Landbouw
- Productie
- Industrie
- Recreatie (e.g., pretparken)
- Transport (e.g., vliegvelden)
- Defensie
- Hulpverlening

3.5 Cyber-fysieke veiligheid

Robots worden bestuurd middels programmatuur. Daarnaast gebruiken ze in toenemende mate netwerken voor hun situationele 'bewustzijn', het verkrijgen van nieuwe opdrachten en de interactie met andere robots. Computers, sensoren, kunstmatige intelligentieprogrammatuur en netwerken geven robots een grote potentie. Tegelijkertijd kan het een Achillespees zijn. Door malware, hacking, technische en menselijke fouten kunnen robots zich anders in de fysieke omgeving gedragen dan gedacht waardoor zich 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 omverrijdt.

Hieronder een korte, niet uitputtende schets van mogelijke risicofactoren:

- 1 Verkeerde sensorinformatie.
Verwacht wordt dat de werkomgeving steeds meer sensoren gaat bevatten die een robot situationele 'bewustwording' 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: self protected node door onverwachte afwijkingen niet te accepteren en correlatie 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.⁴⁰
Een communicatiekanaal kan geblokkeerd worden/zijn (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).
- 3 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

⁴⁰ LoRa staat voor Low Power Wide Area Network, een techniek volgens de LPWAN specificatie die bedoeld is voor de (massieve) koppeling van draadloze "things" op batterijen. Dit is met name een techniek die ingezet zal gaan worden voor intelligente sensoren. LoRa van KPN zal in het tweede kwartaal van 2016 in heel Nederland beschikbaar zijn.

- 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).
- 4 Verstoorde communicatie tussen robots onderling.
Verwacht mag worden dat autonome robots met elkaar 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 agents die samenwerken om een klus te klaren (o.a. swarming). 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).
- 5 Gemanipuleerde programmatuur of instructies.
Tijdens herprogrammering, bijvoorbeeld via een laptop of een overdraagbaar medium als USB, kan ongedacht malware in een robot terechtkomen. Tegenmaatregelen zijn onder andere anti-malware, intrusion detection, gelaagd gescheiden netwerken.
- 6 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 mensen 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 omtrent 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 blijven⁴¹. 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.

Het huidige juridische kader is nog niet ingesteld op de technologische ontwikkelingen die nu plaats vinden op het gebied van robotica. Het is op dit gebied dat dit rapport een belangrijke rol kan spelen. Zoals eerder benoemd zullen de

⁴¹ 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.

resultaten en conclusies in dit rapport inzichten opleveren die kunnen fungeren als aanhaakpunten voor wijzigingen in wet- en regelgeving op nationaal en Europees niveau, i.c. de Arbowet, de Europese machinerichtlijn⁴² en dergelijke.

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 kan men ook in de literatuur kijken voor inspiratie. Zo worden de drie wetten van Asimov⁴³ 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.
- Tweede Wet: Een robot moet de bevelen uitvoeren die hem door mensen gegeven worden, 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 zijn⁴⁴:

- 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.

Deze drie wetten zijn echter niet de enige manier waarop dit vraagstuk kan worden benaderd. Zeker gezien de focus bij industriële robots vooral op het proces zal zijn en mens-robotinteractie mogelijk miniem blijft met betrekking tot deze toepassing.

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 nu verantwoordelijk als er iets mis is met de robot of wanneer er een ongeluk gebeurt, en dus aansprakelijk?

⁴² <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:157:0024:0086:nl:PDF>

⁴³ Hier is later ook een nulde wet aan toegevoegd: *Een robot mag geen schade toebrengen aan de mensheid, of toelaten dat de mensheid schade toegebracht wordt door zijn nalatigheid.* (https://nl.wikipedia.org/wiki/Drie_wetten_van_de_robotica)

⁴⁴ Murphy, R.R., & Woods, D.D. (2009). Beyond Asimov: The three laws of responsible robotics. *IEEE Intelligent Systems*, 24(4), 14-20.

- *Acceptatie door de maatschappij*

Acceptatie van robots in de maatschappij is van meerdere aspecten afhankelijk die eerst geadresseerd moeten worden. Zo gaat robotisering gepaard met een angst op minder banen en daardoor toenemende werkloosheid, en is er de vraag of een zorgrobot de zorg die een mens biedt kan overnemen. Verder kan men zich afvragen hoe de maatschappij gaat 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 benaming robot zorgt er voor dat we anders reageren dan wanneer we het over een machine hebben⁴⁵. 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 hogere acceptatie leiden bij managers, maar zouden arbeiders zich bedreigd kunnen voelen.

- *Privacy*

Robots zijn zoals mensen, afhankelijk van sensorische informatie om op hun omgeving te kunnen reageren. Bij robots kan deze informatie echter makkelijker weer worden opgeslagen. Hierdoor zijn robots in potentie een risico voor de privacy. Denk hierbij bijvoorbeeld aan een sociale robot waar intieme geheimen mee gedeeld worden, of een zorgrobot waarmee ook een camera in huis gehaald wordt. Ook de privacy van arbeiders op de werkvloer zal in beschouwing moeten worden genomen naarmate meer camera's, en sensoren op de werkplek komen.

- *Moraliteit*

Naarmate robots meer mensen 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 krijgen⁴⁶? Moet een robot een enkele arbeider 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?⁴⁷

- *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 gesteld worden of een robot dan soortgelijke rechten verdiend. Denk bijvoorbeeld aan het om onderhouden te worden, of het recht om niet uitgezet te worden.

Sommige van deze aspecten lijken nog ver weg te staan van de huidige toepassing van industriële robots. Maar naarmate de robotisering van de

⁴⁵ <http://jalopnik.com/the-way-were-reacting-to-the-vw-worker-killed-by-a-robo-1715462359>

⁴⁶ Zie bijvoorbeeld ook: <http://jalopnik.com/what-should-robot-cars-ethical-rules-be-1579407463>

⁴⁷ 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,

maatschappij in het algemeen zal toenemen, zullen deze aspecten opgelost moeten worden en zullen ze mogelijk ook een indirect effect hebben op de industriële robots en de manier waarop ze worden ingezet.

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 Voordelen van robotisering

De voordelen van robotisering worden gevonden 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.

4.2 Definitie robots

Geïnterviewden 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 hoeft 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 uitgevoerd wordt. Software robots zijn een aparte categorie.
- **Robotisering gaat vooral over logistieke functies.**

In aanvulling op de definitie die wij voorafgaand aan dit onderzoek hebben gesteld:

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

noteerden wij de volgende aanvulling:

- Met robotisering kunnen nieuwe arbeidskansen gecreëerd worden door cognitieve ondersteuning te bieden aan mensen met een cognitieve beperking.

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.

4.3 Verwachte ontwikkelingen in nabije toekomst

Geïnterviewden 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 geïnterviewden. Wel was men het er over eens dat de ontwikkelingen nu in een hoog tempo gaan.

Waar een groot deel van de geïnterviewden op een lijn zat is dat er een verschuiving wordt verwacht van een klassieke robot op een vaste werkplek naar 'collaborative workplaces' waar robotten en mensen samenwerken. Dit geldt niet alleen voor zwaar of gevaarlijk werk. De geïnterviewden verwachten ook een trend dat 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 mensen nog moeten uitvoeren omtrent robots:

- 1 De aansturing;
Deze rol zal echter snel verdwijnen aangezien autonome robots al op de markt komen.⁴⁸
- 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 geïnterviewden 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 autoindustrie⁴⁹, is de mens nog noodzakelijk voor de afwerking en zal de focus meer op samenwerking tussen mens en robot liggen.

⁴⁸ <http://www.precisionmakers.com/nl/>

⁴⁹ http://www.theregister.co.uk/2016/02/25/mercedes_deautomates_production_lines/?mt=1456477368984

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 onderzocht worden. Voordat robots tegen een betaalbare (en 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 geïnterviewden nog tien tot vijftien jaar wachten.

Verder worden er ontwikkelingen verwacht naar typen robots die meer taken kunnen uitvoeren, productonafhankelijk van formaat kunnen manipuleren, 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 anderen⁵⁰.
- 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 geprogrammeerd worden 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 vaak om ingrijpen door een mens vragen.
- 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 ingezet moet gaan worden: binnen een magazijn zal dit eerder gebeuren dan in een ongestructureerde omgeving. Zoals eerder aangegeven zijn er echter al robots op de markt die binnen⁵¹ en buiten zelf voortbewegen⁵². Dit laat zien dat robotisering zich op het moment in een grijs gebied bevindt. Er zijn al enkele zelf voortbewegende robots te koop,, maar het grootste deel de robots die nu in gebruik zijn staan hier nog ver vandaan.

4.4 Dreigingen en kwetsbaarheden

In de introductie noemden wij het risico van een botsing tussen mens en robot als focusgebied van dit rapport. Dit risico is extra relevant gezien de verwachte

⁵⁰ <http://www.nu.nl/internet/4161514/google-maakt-zelflerende-software-beschikbaar-iedereen.html>

⁵¹ <http://www.robots.nu/nederlandse-sam-robot-beveiligt-je-pand/>

⁵² <http://www.precisionmakers.com/nl/>

verschuiving van de robot opgesteld op een geïsoleerde en vaste werkplek naar een toenemende interactie en samenwerking van mens en robots.

Onze focus in dit rapport blijft echter bij het risico op een botsing tussen mens (romp, hoofd en ledematen) en robot. 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 korte samenvatting van belangrijkste elementen die uit de interviews naar voren kwamen.

Kwetsbaarheden en dreigingen	Samenvatting
Regulatory gaps	Als gevolg van de snelle technologische ontwikkelingen heeft wet- en regelgeving moeite om bij te blijven. 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 betere veiligheid tegenwerken.
Non-compliance	De meeste ongelukken met robots lijken gerelateerd te zijn aan het overtreden van veiligheidszones of instructies. Inefficiënte procedures of veiligheidsfuncties kunnen hierbij een rol spelen, omdat de gebruiker op zoek gaat naar manieren om de veiligheidsmaatregelen te omzeilen.
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.
Taakverandering	Door de inzet van robots vindt er een verandering plaats van de taak die mensen 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	Mensen 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 mensen gemaakt en kunnen dus fouten bevatten. Maakt een robot altijd betere keuzes en wie bepaalt waar deze keuzes op gebaseerd zijn?
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 wordt verloren.

4.4.1 *Regulatory gaps*

Dit project is opgezet om een blik vooruit te werpen naar welke technologische toepassingen binnen robotica worden verwacht, zodat wet- en regelgeving hier anticiperend op kan worden aangepast. Hiermee wordt ook gelijk een groot kwetsbaarheid zichtbaar die ook tijdens de interviews naar voren kwam. 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 markt⁵³. Naarmate meer partijen hiermee 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 wanneer die wordt toegepast op nieuwe technologieën de ontwikkeling van betere veiligheid tegenwerken.

4.4.2 *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). Geïnterviewden 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.

4.4.3 *Gedeelde verantwoordelijkheid*

Het samenstellen, configureren, installatie en programmering 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. Hierdoor kan het zijn dat een arbeider geraakt wordt 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 geïnterviewde uitte zijn zorg dat onduidelijkheid in deze verantwoordelijkheden kan ertoe leiden dat niemand deze op zich neemt.

4.4.4 *Taakverandering (belasting/ vervaging vaardigheden)*

Robots vervangen niet altijd mensen op de werkvloer, maar waar robots worden toegepast vindt er wel een verandering plaats van de taak van de mens. Op het moment zijn robots vaak nog afhankelijk van de mens om te kunnen functioneren, bijvoorbeeld voor het toeleveren van halfproducten en materialen en om controle uit

⁵³ Bijvoorbeeld autonome grasmaaiers (<http://www.precisionmakers.com/>) en bewakingsrobots (<http://www.robots.nu/nederlandse-sam-robot-beveiligt-je-pand/>)

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.

Omdat een robot veel taken op zich neemt kunnen bepaalde vaardigheden van de medewerkers ook 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 onvoorziene situatie. 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 monitortask 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.

4.4.5 *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 gebruikt wordt wanneer het bedrijf in werking is met mensen op de werkvloer. Anderzijds kan de robot ook terecht komen in een situatie waar programmatisch geen rekening mee gehouden is. Neem bijvoorbeeld autonome landbouwrobots die in principe op mensvrije locaties werken. Deze machines hebben daarom vaak geen sensoren om mensen te 'zien'. Toch kunnen onbevoegden zich op de akkers bevinden waar robots actief zijn. De vraag is of je bij het ontwerp van een robot alle mogelijke scenario's kan voorzien die zich mogelijk kunnen afspelen. De mens is ten slotte behoorlijk onvoorspelbaar.

Toch is het belangrijk om bij het ontwerp van iedere robot hier bij stil te staan. Robots die een zware last moeten verplaatsen zijn bij definitie direct of indirect⁵⁴ onveilig voor eventuele mensen in de buurt, maar ook een veilige assemblerobot 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.

Verder is 'management of change' belangrijk bij het upgraden en integreren van bestaande en nieuwe systemen wordt change management belangrijk. Ondanks dat alle machinerieën/apparaten individueel CE gemarkeerd zijn, kunnen door het

⁵⁴ 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.

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 voorzien kunnen worden, 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 waar de monteur op onveilige hoogte onderhoud moet plegen. Op het moment wordt er nog geen tot weinig veiligheids-gerelateerde informatie gedeeld op sectorniveau, bijvoorbeeld op het gebied van best practices.

4.4.6 *Vertrouwen in de machine*

Mensen hebben over het algemeen teveel vertrouwen in het functioneren van machines en technologie. Als voorbeeld wordt bijvoorbeeld 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 kunnen worden, maar ook goed onderhouden worden.

Verder kan men zich afvragen wie moet bepalen wat voor een keuze 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 potentiële 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?

4.4.7 *Cybersecurity*

Potentieel zwakke ICT beveiliging is een duidelijke kwetsbaarheid waardoor de dreiging van hackers of overname van de besturing actueler wordt. Geïnterviewden herkennen het risico dat ontstaat als een robot gehackt wordt. Zeker zelf voortbewegende robots kunnen potentiële wapens worden. Cybersecurity staat op de agenda bij leveranciers, echter het is moeilijk de garantie te geven dat het 100% veilig is gezien de huidige snelle ontwikkelingen. Als risicofactor wordt gewezen op 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. Als de robot veilig ontworpen is, heeft men een hoop winst te pakken. Veel minder beheersmaatregelen werden genoemd voor de laatste fasen van de levenscyclus: vernieuwen en afbreken, fasen die bij organisaties veelal onderbelicht zijn. Tabel 4 geeft een overzicht van de beheersmaatregelen per fase van de levenscyclus.

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

Levenscyclus	Beheersmaatregelen
Ontwerp/ Engineering	✓ Bij ontwerp rekening houden met de functie van de robot, bijvoorbeeld door het uitvoeren van een risico-inventarisatie voor elke mogelijke toekomstige toepassing ✓ Bij ontwerp rekening houden met onderhoudswerkzaamheden die aan de robot gepleegd moeten worden, bijvoorbeeld door de periferie van de robot mee te nemen in ontwerp ✓ Implementeren van een goed bereikbare noodstopfunctionaliteit in het ontwerp. Dit moet geen stroomonderbreking zijn, maar het veilig tot stilstand komen van de robot (safe modus) ✓ Software wordt virtueel getest ✓ Het delen van best practices sectorbreed ✓ Het betrekken van de uiteindelijke gebruikers (de medewerkers die met de robot moeten werken) bij het ontwerp, voor het benutten van kennisstaken en het creëren van een draagvlak voor acceptatie ✓ Ondersteun de instructies voor het werken met robots met gestandaardiseerde of geharmoniseerde symbolen ✓ Transparantie omtrent bevoegdheden en competenties rondom het ontwerp, samenbouw, onderhoud en ontmanteling van de robot ✓ Rekening houden met gebruiks- en onderhoudsergonomie bij het ontwerp van de robot ✓ Gebruiken van gecertificeerde onderdelen (o.a. de sensoren) ✓ Gebruik maken van de best beschikbare technologie en software in het ontwerp
Productie/ leverantie/ samenstellen/ installatie/ configureren	✓ Het delen van best practices sectorbreed ✓ Uitvoeren van een risico-inventarisatie en evaluatie ✓ Het borgen van de kwaliteit van de robot tijdens opslag en transport ✓ Het verzorgen van een intrinsiek veilige werkomgeving voor installatie, samenbouw en onderhoud ✓ Opstellen van taakallocatiecriteria gericht op performance en mens (behouden van attractiviteit van het werk) ✓ Training van de klant in het veilige gebruik van de robot ✓ Certificering voor het personeel dat de veiligheid configureert en implementeert ✓ Het gebruiken van protocollen voor veilige installatie ✓ Communicatie met en tussen veiligheidskundige, klant en leverancier ✓ De interfaces van robots standaardiseren
Gebruik	✓ Zorgen voor een schone werkvloer d.m.v. housekeeping ✓ Richten op gebruiksgemak en gemakkelijk programmeren en configureren ✓ Het delen van best practices sectorbreed ✓ Training volgen die door de leverancier wordt verzorgd en zorgen voor interne opvolging van noodzakelijke trainingen en opleidingen ✓ Het geven van feedback aan medewerkers bij overtreding van veiligheidsregels ✓ Aanspreekgedrag stimuleren op de werkvloer ✓ Afwijkingen in programmatuur monitoren en bijstellen indien nodig ✓ Periodieke en systematische controle of veiligheidssysteem nog goed werken ✓ Periodieke en systematische conformiteitsbeoordeling aan veiligheidseisen ✓ Uitvoeren van een risico-inventarisatie en -evaluatie, en het opstellen van een plan van aanpak omtrent het gebruik van robots (hulpmiddelen online, digitale vragenlijst) ✓ Veiligheid mens is prioritair, dan pas zelfbehoud van het product of robot ✓ Monitoren en registreren van incidenten (en het terugkoppelen van deze informatie aan de leverancier) ✓ Veilig stellen van datacommunicatiestromen van en naar de robot ✓ Het werkproces inrichten vanuit de mens ondersteund door de robot, en niet andersom ✓ Opstellen van interne procedures zoals Life Safing Rules ✓ Gebruik maken van verbeterloops om continue verbetering na te streven van het primaire proces

Levenscyclus	Beheersmaatregelen
Onderhoud	✓ Goede communicatie tussen gebruiker en leverancier vooraf aan onderhoudswerkzaamheden (over eventuele noodzakelijke veiligheidsmaatregelen) ✓ Opstellen van onderhoud regimes ✓ Transparantie in competenties binnen de onderhoudsmarkt ✓ Het opstellen van een job safety plan met de klant ✓ Lock-in procedures die garanderen dat de robot onder controle staat van de onderhoudsmedewerker ✓ Gebruik maken van een Last Minute Risk Analysis (LMRA) ✓ Registeren van gevaarlijke situaties en hier terugkoppeling op geven ✓ Het verplichten van een werkvergunning voor het plegen van onderhoud
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 toekomst ontwikkeling ✓ Richtlijnen regimes
Afvoeren	✓ ✓ Op veilige wijze vernietigen van software en configuratiegegevens (overschrijven of componenten vernietigen) ✓ Duidelijke instructies van de leverancier van wat de gevaren zijn tijdens het ontmantelen van de robot ✓ Het scheiden van zeldzame (aard)metalen en kunststoffen omwille van de toxiciteit van dit soort 'afval' ✓ Transparantie over de milieubelasting van de overgebleven componenten ✓ Voorkomen dat oude (onveilige) robots kunnen worden misbruikt.

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

4.5.1 Ontwerp en Engineering

In de workshop kwam werd duidelijk dat de experts geloofden 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 een risicoanalyse plaatsvinden op basis van de geplande toepassing. Zo kunnen 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 practice hierbij zou zijn om de uiteindelijke gebruikers te betrekken bij deze fase om hun kennis te benutten.

De risicoanalyse stelt de robotontwerpers en -ontwikkelaars vervolgens in staat om de robot zodanig te ontwerpen dat het geïdentificeerde risico geminimaliseerd wordt of zelfs geheel wordt weggenomen. Voor robots die veel met mensen moeten samenwerken kan bijvoorbeeld gedacht worden aan het implementeren van stootkussens of aan het lichter of minder sterk maken van de robot. Op deze manier zal er geen schade op treden mocht er toch een botsing met een mens (direct risico) of met een voor de mens gevaarlijk object (indirect risico) plaatsvinden. Het aangepaste ontwerp moet vervolgens conform de Europese Machinerichtlijn 2006/42/EG door een onafhankelijke partij getoetst worden op veiligheid.

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 mensen te laten voortbewegen. Ook werd het gedrag aangepast door de robot voorspelbaarder te maken 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 de ergonomie wordt meegenomen. Door tijdens de ontwerpfase de human factors mee te nemen kunnen veel gevaren, zowel die tijdens normaal gebruik als tijdens onderhoud, al in het ontwerp worden weggenomen. Zo kan fysieke overbelasting bij gebruik van een exoskelet voorkomen worden door vooraf te kijken naar wat een mens aankan en wat hij of zij ermee moet doen. De snelheid en versnellingen van de bewegingen kunnen daar op aangepast worden.

Zelfs in een zogenaamde 'lights-out' fabriek waar helemaal geen mens meer aan te pas komt in het primaire proces, zal de human factor ook een rol spelen. In een dergelijke fabriek zullen alsnog mensen nodig zijn voor het monitoren van de robots. Hier zal het de uitdaging zijn om de dreiging van cognitieve onder- of overbelasting te voorkomen door zodanig ondersteuning te bieden dat het werk interessant en uitdagend blijft (dan wel kan de focus liggen op specifiek inrichten van een werkplek voor medewerkers met autisme). Hiervoor moet het operatorsysteem worden geoptimaliseerd door te kijken waar de cruciale fouten die niet gemaakt mogen worden liggen en daar ondersteuning voor te bieden. Hierdoor zal wel een bepaald kennisniveau noodzakelijk zijn om met het operatorsysteem te mogen werken.

Adaptieve automatisering is het concept waarbij software de mens die met de robot werkt in 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 al tijdens de ontwerpfase van een robot over moet worden nagedacht kwamen uit de interviews naar voren: de sensoren en een noodstopfunctie.

Historisch wordt er vanuit veiligheidsoptiek gebruik gemaakt van een fysieke barrière tussen mens en robot. Nu hoeven robots niet meer volledig afgeschermd te worden omdat ze sensoren hebben. De robot kan met deze sensoren de aanwezigheid van mensen detecteren en gaat langzamer draaien of stilstaan als een persoon in reikwijdte van de robot komt. Het voordeel van deze sensoren is dat ze mensen ook veilig houden op die momenten dat de robots benaderd moeten worden, bijvoorbeeld tijdens onderhoud. De sensoren moeten wel CE-gecertificeerd zijn, als de intrinsieke veiligheid van de sensoren 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 gebruikt worden om vast te stellen of aan alle randvoorwaarden ten aanzien van 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, wanneer een gevaarlijke situatie dreigt te ontstaan, direct ingegrepen worden. Zo krijgt bijvoorbeeld bij tests met landbouwrobots altijd één persoon de taak om met de noodknop bij de robot te lopen. Dit mag op dat moment ook de enige taak van die persoon zijn.

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 het ergens tegen aan dreigt te rijden zijn op het moment nog maar een basale vorm van veiligheid. Waar we naar toe gaan zijn slimmere robots die kunnen voorspellen wat zich in de omgeving bewegende objecten zoals een mens gaan doen. Andersom kan dan met het gedrag van de robot de mens om zich heen gestuurd worden. Dit wordt vergeleken met het verschil van omstanders wanneer er met een strakke loopsnelheid wordt doorgelopen versus wanneer er twijfelend gelopen wordt.

In een gestructureerde omgeving is dit makkelijker te bewerkstelligen dan bijvoorbeeld buiten. Buiten moeten robots mensen 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 geremd hoeft te worden als er een vogel op het pad zit; als er snelheid terug wordt genomen zal het probleem zichzelf waarschijnlijk oplossen.

Met dit soort ontwikkelingen zullen er minder 'false alarms' als gevolg van veiligheidsfuncties ontstaan en daarmee wordt de robot mensvriendelijker en veiliger voor de mens. Hiermee verklein je de kans op irritaties bij de gebruiker en non-compliance met de veiligheidsvoorschriften.

Echter, naarmate de robot slimmer zal worden, zal de noodzaak om bepaalde regels, zoals de drie wetten van Asimov, in de robot te programmeren. Dit lijkt voorlopig nog niet noodzakelijk voor de nabije toekomst.

4.5.2 *Productie, levering, samenstellen, installatie en configuratie*

In de workshop kwam certificering voor 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 mensen mee aan de slag gaan.

Verder werd het trainen van de gebruiker in veilig gebruik van de robot benoemd als belangrijke beheersmaatregel. Leveranciers geven in samenwerking met systeemintegratoren en installateurs instructies mee hoe de robot gebruikt moet worden. Ook testen ze of de robot goed geplaatst is en werkt. Hierin ligt de

verantwoordelijkheid voor de benodigde instructie van hoe een machine beweegt bij zowel de opdrachtgever (de uiteindelijke gebruiker van de robot) en de opdrachtnemer (leverancier/installateur). De opdrachtnemer moet de instructie geven en de opdrachtgever moet zichzelf ervan overtuigen 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 gewerkt gaat worden, 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 zelf waar de robot gebruikt wordt.

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 gebruik fase kwam het delen van 'best practices' naar voren als belangrijke beheersmaatregel. Verder was er niet echt een voorkeur voor bepaalde beheersmaatregelen maar werden verschillende beheersmaatregelen door verschillende experts als van belang benoemd. Dit waren bijvoorbeeld 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 om moeten gaan en weten hoe ze het risico voor zichzelf kunnen minimaliseren. Dit zal moeten gebeuren door training en voorlichting aangeboden door de leverancier en interne opvolging.

Robotisering heeft echter ook gevolgen voor de vraag naar schoolopleidingen. Met toenemende robotisering zal het benodigde personeelsbestand van organisaties gaan veranderen. Er zal meer vraag zijn naar technisch gekwalificeerde mensen aan de fabricage/proceslijn die complexe(re) taken uitvoeren en storingen preventief kunnen oplossen. Het fysiek zware en geestdodende werk zal met de tijd geëlimineerd worden 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.

Ook is het van belang dat er bij het werkproces niet alleen naar de robot wordt gekeken. Nu wordt vaak het werkproces ontworpen vanuit wat technisch mogelijk is. Het werkproces kan echter ook worden ingericht vanuit het oogpunt van de

werknemer die geassisteerd wordt door robots. Hierbij voorkom je dat 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 herkend wordt). Hierbij is het van belang om de taken van mens en machine goed te definiëren zodat het ook duidelijk is wanneer en hoe de mens moet ingrijpen.

Verder geldt momenteel voor de meeste robots dat zij de omgeving beter kunnen 'begrijpen' als de omgeving gestructureerd is. Waar mogelijk zouden mensen dus weggehouden moeten worden 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'⁵⁵, 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 practice is bijvoorbeeld het principe van LTT⁵⁶:

- Lock out: het uit- en 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 eigen engineers van verlaagde functionele

⁵⁵ Zie bijvoorbeeld de Life Saving Rules van Shell: <http://www.shell.nl/sustainability/veiligheid.html>

⁵⁶ <http://www.hamer.net/algemeen/lock-tag> of <http://www.verbondpk.nl/Arbocatalogus/LTT>

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 kun 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 naar toekomstige ontwikkelingen. Bijvoorbeeld wanneer wet- en regelgeving zodanig verandert dat een bepaalde toepassing van een robot niet meer mag. Of wanneer een beter onderdeel op de markt komt, niet de gehele robot hoeft 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 gescheiden worden.

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

5 Discussie

Dit project draagt bij aan de bewustwording van het aan robotisering verbonden risico voor werknemers bij de arbeidsplaatsen in de diverse industrieën waar ingezet wordt op (verdere) robotisering van het productieproces. Met de 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 snel, wat ook blijkt uit de toenemende nationale en internationale aandacht voor robots, robotisering, industrie 2.0 en smart industrie blijkt. Zie bijvoorbeeld publicaties als De Ingenieur⁵⁷, de Lichtkogel⁵⁸ en Control Design⁵⁹, rapporten van bijvoorbeeld het Rathenau-instituut⁶⁰, en steeds meer lezingen en bijeenkomsten over robotisering⁶¹. Dit onderzoek vindt plaats aan de voorkant van de voorziene ontwikkelingen van de functionaliteit van diverse meer potente robottypen, met andere woorden 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 mensen. Dit kan kloppen, in een recent rapport van Control Systems 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 werkgerelateerde incidenten met een dodelijke afloop in 2014)⁶².

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

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

⁵⁷ M. Seijlhouwer, Meelevende machines, De Ingenieur, 2016, jaargang 128, no 4, pg 12-19,

⁵⁸ 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

⁵⁹ Collaborative Robots in Control Design for Machine Builders (2016).

⁶⁰ L. Royakkers, F. Daemen, R. van Est (2012), Overall 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>.

⁶¹ Bijv. een bijeenkomst over de inzet van robots door hulpdiensten bij calamiteiten.

⁶² Bacidore, M. (2016). The new world of collaborative robots. *Control Design for Machine Builders. Special report: Collaborative robots.*

5.1 Robotica als container begrip

Eén van de eerste dingen die opviel tijdens de interviews met de experts, is dat robots en robotica een problematisch begrip kan zijn. Wat wordt er precies bedoeld met robots, over welk type robot hebben we het? Deze vragen moesten aan het begin van de interviews worden afgehandeld, voordat het gesprek kon beginnen.

Robotica is een containerbegrip waar veel verschillende toepassingen onder vallen. Zelfs met de door ons gehanteerde definitie, *een robot een machine is die geprogrammeerd kan worden, 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 geprogrammeerd kan worden 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 moet sneller, preciezer, gemakkelijker en goedkoper, en dit alles natuurlijk veilig. 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 op zich niet onderscheidend genoeg is om mee te kunnen werken. 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 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, en de reden hiervoor is simpel: een universeel veilig robotontwerp bestaat niet. Welke aspecten noodzakelijk zijn hangt ook grotendeels af van de functie waar de robot voor ingezet gaat worden. Een lichter frame voor robots die veel met mensen 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.

Hierbij bestaat een robot over het algemeen uit twee delen. De machine of armen die het werk doen en het controlesysteem. Bij het kijken naar 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 softwarefouten in, is het up to date, wie heeft er allemaal toegang? De integriteit van de besturingssoftware bepaalt voor een groot deel of de robot veilig kan worden gebruikt evenals of de robot is afgeschermd voor ongewenste invloeden van buitenaf.

Een ander algemeen advies dat naar voren is gekomen is dat er gestreefd zou moeten worden 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 geprofiteerd worden van een samenwerking tussen mens en robot. Als dit wordt nagelaten, kan er afhankelijkheid groeien van de robot waardoor in abnormale situaties niet meer adequaat kan worden gereageerd of zullen de overgebleven taken niet meer uitdagend genoeg zijn waardoor de kans op fouten toeneemt.

Verder was er unanimititeit over 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 echter de ontwikkelingen in de functionaliteit van robots kunnen bijhouden⁶³. Het is dan 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 stapt⁶⁴. Deze sensoren worden bijvoorbeeld ook voor de bewaking van gebouwen ingezet. Maar er kan ook 'out of the box' gedacht worden door bijvoorbeeld een 'veiligheidsschild' rondom de mens te creëren waar robots op reageren door stil te gaan staan zodra dit schild in de buurt komt⁶⁵.

5.3 De human factor

Zelfs een inherent veilig ontworpen robot zal onveilig kunnen zijn als deze verkeerd wordt gebruikt of in de verkeerde context. Correct gebruik moet dus worden

⁶³ Bacidore, M. (2016). The new world of collaborative robots. *Control Design for Machine Builders. Special report: Collaborative robots*.

⁶⁴ Voorbeeld van product op de markt:

https://www.sick.com/media/dox/9/79/879/Industry_guide_Building_Safety_and_Security_en_IM0036879.PDF

⁶⁵ <http://www.engineersonline.nl/producten/elektrotechniek/veiligheid/id25604-veilige-werkplek.html>

gepromoot. Het komt uiteindelijk ook op neer om je gezonde verstand te gebruiken rondom robots. Dit kan binnen organisaties door de richtlijnen die bij een robot worden gegeven te volgen, eventuele trainingen volgen die noodzakelijk zijn en deze regelmatig opvolgen om up to date te blijven. Het gebruiken van gecertificeerd 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 geholpen worden door methoden als een elektronische vragenlijst of checklist. Een gecodificeerde vragenlijst helpt bij de risico-inventarisatie en –evaluatie en kan tevens helpen bij het afvinken van de compliance met vigerende wet- en regelgevingsaspecten.⁶⁶ Tevens kunnen best practices aangereikt worden.

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 ook gecontroleerd worden om fouten te voorkomen en er voor te zorgen dat deze goed blijft werken. Wie bepaald of controleert straks op basis van welke argumenten een robot (morele) keuzes gaat maken?

Een risico dat genoemd wordt is dat robotisering als risico met zich meebrengt dat de programmatuur van robots dadelijk bepalend is voor wat wel en niet mogelijk is. Een administratieve robot heeft veel moeite om uitzonderlijke situaties te behandelen waar mensen weinig problemen mee hebben omdat deze buiten ‘zijn programmatuur’ treedt al geeft dat tevens het risico van fraude. 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 een ‘lights out’ fabriek (waar alleen maar robots op de werkvloer staan) zijn mensen nodig om de robots te monitoren en het proces te controleren. Daar ontstaat dus weer werkgelegenheid.

Met andere woorden, voorlopig lijkt de robot nog afhankelijk te zijn van de mens. Het lijkt dan ook 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

Voor de huidige robots lijkt de huidige bestaande wet- en regelgeving alsmede normeringen grotendeels voldoende te zijn. Vanuit normalisatie worden huidige

⁶⁶ Zie bijvoorbeeld <http://www.wlis.nl/> voor compliance controle van vergelijkbare security/safety-onderwerpen.

robots niet als nieuw gezien maar als machines met een elektrotechnisch onderdeel (bijv. het praten en communiceren van robots) en niet-elektrotechnische delen. Hier bestaan respectievelijk ICS- (International Classification for Standards) als ISO- (International Organization for Standardization) normen voor. 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.

Regelgeving zal de techniek nooit volledig kunnen evenaren. Daar gaan de technologische ontwikkelingen op het gebied van robotica te hard voor. Pogingen om wet- en regelgeving technologieonafhankelijk te maken anderzijds lopen vaak spaak omdat de juristen van de wet- en regelgever negatieve aspecten van incidenten uit het verleden zo goed mogelijk proberen af te dekken. Komende ontwikkelingen worden daarbij onvoldoende ingebed bij gebrek aan een multidisciplinaire blik in de toekomst.

In de praktijk groeien normen wel 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 heeft⁶⁷. 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. Wel is het zaak om belangrijke 'regulatory gaps' te identificeren en deze tijdig op te vullen.

Het ontbreken van wet- en regelgeving rondom autonome 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. Autonome voertuigen zijn een duidelijk voorbeeld waar de markt voorloopt op wet- en regelgeving omdat deze al door verschillende partijen te koop wordt aangeboden⁶⁸. 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 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.

Ook in de landbouwsector speelt dit probleem. Zij hebben een document opgesteld betreffende de wet- en regelgeving en aanbevelingen rondom de toepassing van autonome trekkers. In dit document 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

⁶⁷ 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>.

⁶⁸ Zie bijvoorbeeld <http://www.precisionmakers.com/nl/>; en <http://robotsecuritysystems.com/>

moet zijn van het monitoren en mogelijkheid om in te grijpen⁶⁹. Er wordt teruggegrepen op deze richtlijn omdat autonome trekkers soms ook spuitmachines voorttrekken, en omdat de Trekker- (2003/37/EG) en de Machinerichtlijn (2006/42/EG) nog geen uitsluitel geven.

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.

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 gedacht worden aan wetgeving. Anders kan de wetgeving in een later stadium in de weg zitten omdat het product niet aantoonbaar veilig is. Dit heet 'Lock in' en kan producten doen falen. Voor startups is het belangrijk om te weten aan welke wet- en regelgeving voldaan moet worden afhankelijk van wat je wil ontwikkelen en wat een robot moet doen. Zo zal bijvoorbeeld een robot die voor de voedingswarenssector wordt ontwikkeld niet uit bepaalde materialen mogen bestaan. Maar ook toepassingen zoals de zelfrijdende voertuigen die Domino's pizza's wil laten bezorgen kunnen dus nog in de problemen komen met wet- en regelgeving⁷⁰.

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 ontworpen robot door de leverancier. Vervolgens moeten de systeemintegrators de robot veilig en correct samenstellen, installeren en configureren bij de klant met bijbehorend certificaat. De robot moet vervolgens veilig gebruikt worden, systematisch onderhouden worden (inclusief de software), en tot slot vernieuwd of op de juiste wijze gedemonteerd en afgevoerd worden wanneer de robot verouderd is.

Hier ligt een gedeelde verantwoordelijkheid om de risico's uit te bannen. Iedere partij moet binnen zijn eigen proces verantwoord (en gecertificeerd) aan de slag gaan en een risico-inventarisatie en –evaluatie uitvoeren, maar het houdt niet op bij de grens. 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. Door gezamenlijk te opereren en elkaar goed te informeren kan het proces geoptimaliseerd worden.

⁶⁹ 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*.

⁷⁰ <http://www.nu.nl/gadgets/4232354/dominos-wil-zelfrijdend-autootje-pizzas-laten-bezorgen.html>

5.6 Toekomst industriële robot

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

Een robot een machine is die *geprogrammeerd* kan worden, *sensoren* heeft, en een bepaalde gradatie van *mobilititeit* 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 software verder ontwikkelen om adequaat te kunnen reageren op de input. Hierbij kan men denken aan de behoefte van een robot die ook de intentie van een mens om zich heen kan inschatten. Waar de grens ligt van de 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 zitten wachten op de uitkomst van dergelijke discussies en focust zich op het verder 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 zo'n 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. grasmaaiers en bewakingsrobots), maar ook op de werkvloer worden ze al ingezet⁷¹. 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 werknemers 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.

⁷¹ Bijvoorbeeld zelfrijdende transportwagens die de containers verplaatsen in de APM-terminal op Maasvlakte-2.

Of deze ontwikkelingen er aan komen is voornamelijk een vraag van wanneer. Men kan er dus het beste al op voorbereid zijn. Dit rapport geeft een inventarisatie van kwetsbaarheden en dreigingen die met deze ontwikkelingen gepaard gaan. Op basis daarvan is een overzicht van beheersmaatregelen die hier tegen genomen kunnen worden opgesteld. Op deze manier komen we weer een stap dichterbij een toekomstige generatie aan robots die niet alleen sneller, beter, en slimmer is, maar ook veiliger.

6 Ondertekening

Utrecht, 18 mei 2016

Naam en paraaf tweede lezer:

A handwritten signature in blue ink, consisting of a stylized 'J' followed by a series of loops and a long horizontal stroke.

J.N. van Kampen MSc.

Ondertekening:

A handwritten signature in blue ink, featuring a large 'F' and 'A' followed by a long horizontal stroke.

F.A. van der Beek MSc.
Projectleider

Autorisatie vrijgave:

A handwritten signature in blue ink, featuring a stylized 'B' followed by a long horizontal stroke.

Drs. H.C. Borst
Researchmanager

A 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 dat een robot onderhouden moet worden (**)
- 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)
- Basis veiligheid 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 mensen 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 softwareupdates: controleerbaarheid, certificatie veiligheid
- Onveiligheid door onderhoud software op afstand
- Gevoeligheid voor toegang/invloed van buiten: denk aan hacken/overnemen van besturing (**)
- Onderhoudsissues; aansprakelijkheidsissues
- Applicaties bepaalt 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 sectorbrede 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 (***)
- Certificering 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 configureren (*)
- 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
- Onderhoudregimes
- 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.