"De werkgever zorgt voor de veiligheid en de gezondheid van de werknemers inzake alle met de arbeid verbonden aspecten. Heeft u het functioneren van uw robots en het daaraan verbonden risico voor uw medewerkers op hun werkplek volledig onder controle?"

Dankzij robotisering hebben organisaties grote stappen kunnen zetten in termen van efficiëntie. Deze ontwikkeling brengt echter ook nieuwe dreigingen en kwetsbaarheden. Vooral nu er een trend ontstaat waarbij de fysieke barrières tussen mens en robot verdwijnen. De mens en robot gaan steeds vaker samen op de werkvloer opereren, daardoor kunnen er onveilige arbeidssituaties optreden. Denk hierbij aan operators of onderhoudsmonteurs die bekneld raken na een onverwachte beweging van de robot of een situatie waarbij het door de robot gehanteerde hulpmiddel zoals bijvoorbeeld een laser een gevaarlijke situatie voor mensen kan opleveren. Gezien de snelle technologische ontwikkelingen en mogelijkheden moeten bedrijven en organisaties blijven anticiperen en meegroeien om eventuele incidenten tussen robots en mensen voor te zijn. Voorkomen is beter dan genezen. U, als een van de actoren in de levenscyclus van arbeidsmiddelen, bent aan zet!

Tabel 1. Wat zijn kwetsbaarheden en dreigingen die de kans op bovengenoemd risico vergroten?

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

Kijk voor meer informatie in het bijbehorende rapport *Opkomend risico voor arbeidsveiligheid door inzet van robots op de werkvloer* te vinden op www.arboportaal.nl;
of neem contact op: Dolf.vanderbeek@tno.nl

Bron plaatje, Gevonden d.d. 26-05-2016:
https://www.mechatronicamachinebouw.nl/fileadmin/uploads_redactie_mm/images/2012/MM07/Rethink_Robotics_Baxter.jpg

Tabel 2. Maatregelen om het risico te minimaliseren op basis van expert sessies.

Levenscyclus		Beheersmaatregelen
Ontwerp/ Engineering	BA	✓ Bij ontwerp rekening houden met de functie van de robot, bijvoorbeeld door het uitvoeren van een risicoanalyse voor elke denkbare toekomstige toepassing ✓ Het betrekken van de uiteindelijke gebruikers (de medewerkers die met de robot moeten werken) bij het ontwerp, voor het benutten van kennistaken en het creëren van een draagvlak voor acceptatie ✓ Implementeren van de drie wetten van Asimov ✓ Rekening houden met gebruiks- en onderhoudsergonomie bij het ontwerp van de robot ✓ Software wordt virtueel getest ✓ Bij ontwerp rekening houden met onderhoudswerkzaamheden die aan de robot moeten worden gepleegd, bijvoorbeeld door de periferie van de robot mee te nemen in ontwerp
	CM	✓ Implementeren van een goed bereikbare noodstopfunctionaliteit in het ontwerp. Waarbij de robot veilig tot stilstand komt (safe modus) ✓ Het delen van 'best practices' sector breed en tussen sectoren ✓ Ontwikkel gestandaardiseerde of geharmoniseerde symbolen ter ondersteun van instructies voor het werken met robots ✓ Transparantie omtrent bevoegdheden en competenties rondom het ontwerp, samenbouw, onderhoud en ontmanteling van de robot ✓ Gebruik maken van de best beschikbare technologie en software in het ontwerp ✓ Gebruik waar mogelijk gecertificeerde onderdelen
	IM	-
	PBM	-
Productie tot configuratie	BA	✓ Borging veilig gedrag, veiligheidscultuur en -kennis bij het personeel dat de robot moet configureren ✓ Het verzorgen van een intrinsiek veilige arbeidsomgeving voor installatie, samenbouw en onderhoud, door onnodige risico's – op basis van een risico analyse- te voorkomen.
	CM	✓ Communicatie met- en tussen onder andere de veiligheidskundige, klant en leverancier over veilig gebruik van de robot ✓ Aanvullende instructies voor de robot leveren in verband met de integratie van verschillende componenten
	IM	✓ De interfaces om robots te programmeren en bedienen standaardiseren
	PBM	-
Gebruik	BA	✓ Veiligheid mens is prioritair, dan pas zelfbehoud van het product of robot (= Asimov) ✓ Het werkproces inrichten vanuit de mens ondersteund door de robot, en niet andersom ✓ Het uitvoeren van een Taak-Risico analyse
	CM	✓ Het delen van 'best practices' sector breed en tussen sectoren ✓ Implementeren van good housekeeping en zorgen voor onder andere een schone werkvloer ✓ Richten op gebruiksgemak en gemakkelijk programmeren en configureren ✓ Intern periodieke en systematische controle of veiligheidssystemen nog goed werken uitvoeren ✓ Intern periodieke en systematische conformiteitsbeoordeling aan veiligheidseisen uitvoeren ✓ Training effectief volgen die door de leverancier wordt verzorgd en zorgen voor interne opvolging van noodzakelijke trainingen en opleidingen ✓ Geven van geschrevenen mondelinge voorlichting en instructies aan medewerkers die met de robot gaan werken en zorgen dat deze begrepen zijn ✓ Uitvoeren van een risicoanalyse, en het opstellen van een plan van aanpak omtrent het gebruik van robots (hulpmiddelen online, digitale vragenlijst) ✓ Monitoren en registreren van ervaringen (en het terugkoppelen van deze informatie aan de leverancier) ✓ Het op orde hebben van de cybersecurity met betrekking tot de datacommunicatiestromen van en naar de robot ✓ Opstellen van voorschriften en gedragsregels met betrekking tot de omgang met robots op de werkvloer ✓ Gebruik maken van verbeterloops om continue verbetering na te streven voor de inzet van robots ✓ Monitoren op afwijkingen in programmatuur en tijdig bijstellen
	IM	✓ Het geven van feedback aan medewerkers bij overtreding van veiligheidsregels ✓ Aanspreekgedrag stimuleren op de werkvloer zowel op onveilig werken met robots als op gewenst gedrag
	PBM	-
Onderhoud	BA	-
	CM	✓ Lock-out (LoTo) procedures die garanderen dat de robot onder controle staat van de onderhoudsmedewerker ✓ Het uitvoeren van een Taak-Risico analyse ✓ Opstellen van onderhoud regimes ✓ Registeren van gevaarlijke situaties en hier terugkoppeling op geven
	IM	✓ Goede communicatie tussen gebruiker en leverancier vooraf aan onderhoudswerkzaamheden (over eventuele noodzakelijke veiligheidsmaatregelen) en het opstellen van een plan van aanpak ✓ Gebruik maken van een Last Minute Risk Analysis (LMRA) ✓ Het invoeren of verplichten van een werkvergunning voor het plegen van onderhoud
	PBM	-
Vernieuwing	BA	✓ Zorg dat robots aan te passen zijn naar nieuwe wet en regelgeving of nieuwe hard- of software (om veroudering te voorkomen)
	CM	✓ Toezien dat eventueel hergebruik van oude componenten in nieuwe installaties verantwoord gebeurt ✓ Richtlijnenregimes ter bevordering van tijdige hernieuwing invoeren
	IM	-
	PBM	-
Afvoeren	BA	✓ Op veilige wijze vernietigen van software en configuratiegegevens (overschrijven of componenten vernietigen) ✓ Voorkomen dat afgevoerde oude (onveilige) robots kunnen worden gebruikt
	CM	✓ Kennis verkrijgen 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
	IM	-
	PBM	-

Note: BA = Bron aanpak, CM = Collectieve Maatregel, IM = Individuele Maatregel, PBM = Persoonlijke Beschermingsmiddel