SAFE APPLICATION OF ROBOTS IN THE WORK PLACE - SAFETY CHART

TNO innovation for life

Employers are responsible for the health and safety of employees in every aspect that is related to the work. Do you have the operations of your robots and the associated risk to your employees in their work place completely under control?

Thanks to robotisation, organisations have taken great strides in terms of efficiency. However, this also entails new threats and vulnerabilities. This is especially the case now that physical barriers between people and robots are starting to disappear. It is becoming more frequent for people and robots to be working together in the work place, as a result of which unsafe working situations may arise. Examples include operators or maintenance engineers who become trapped after a robot makes an unexpected movement, or a situation in which a tool used by a robot, such as a laser, causes a person to be in danger.

Given the fast-moving technological developments and possibilities, businesses and organisations must continue to anticipate and evolve in order to prevent incidents between robots and people. Prevention is better than cure. It's now up to you, as one of the actors in the life cycle of machinery!

TABLE 1. WHICH VULNERABILITIES AND THREATS INCREASE THE RISK?

Vulnerabilities and threats	Summary
Unforeseen situations	Because of the deployment of robots, the tasks that people carry out are changing. As a result of this change, employee skills may get rusty because they are only used in emergencies. Cognitive underload and overload may occur leading to a greater likelihood of errors being committed, or they may suffer physical overload due to the tasks that remain being very repetitive, with the robot determining the rate at which they are carried out.
Unforeseen situations	When designing robots, every effort is made to factor in all possible scenarios. This is often impossible, however, as it may depend on how the robot is ultimately used (possibly incorrectly), spontaneous and unforeseen action by people, unexpected situations arising, software interacting with other software in ways previously unanticipated, or simply because a particular scenario was not considered.
Trust in machines	In general, people have a high level of trust in the capacities and functioning of machines and technology. However, these machines and the software that are used to operate them are themselves made by people and can therefore incorporate errors. Do robots always make better choices and who determines where these choices are based upon?
Shared responsibility	Using a robot involves multiple parties - the developer of the robot, the system integrator, the installer, and the eventual user. A lack of clarity in where responsibility for safe use lies could lead to nobody taking it.
Regulatory gaps	Technological developments are moving fast and are not always easy to predict, which makes it difficult for the laws and regulations to keep up. For example, there are currently no guidelines for self-driving machines, even though they are already on the market. An out-of-date standards framework could hinder the development of safety as a whole.
Non-compliance	Until now, most accidents involving robots have been related to the ignoring of safety zones or to the failure to observe safety instructions. Inefficient procedures or safety functions may have played a role here, as users look for ways to circumvent safety measures.
Cyber security	Potentially weak security of information and communication technologies (ICT) is a clear vulnerability, as a result of which the threat from hackers or loss of control have become real possibilities. Large robots in particular can be dangerous as soon as they can no longer be controlled of if someone else has taken over control of them.

For more information, see the related report, Emergent risk to workplace safety as a result of the use of robots in the work place, at www.arboportaal.nl; or contact: Dolf.vanderbeek@tno.nl

TABLE 2. MEASURES FOR MINIMIZING THE RISK.

Life cycle		Control measures
Design/ Engineering	**SM**	✔ Taking account of the function of the robot during the design phase, for example by carrying out a risk analysis for every conceivable future application
		✔ Involving the end-users (employees who will have to work with the robot) during the design phase, for using knowledge tasks and creating support for acceptance
		✔ Implementing Asimov's three laws
		✔ Taking account of user and maintenance ergonomics when designing the robot
		✔ Software is tested virtually
		✔ During the design stage, taking account of maintenance work that has to be carried out on the robot, for example by including the peripheral areas in the design
		✔ Incorporating an easily accessible emergency stop function in the design. Where the robot safely comes to a standstill (safe mode)
	CM	✔ Sharing best practices throughout the sector and between sectors
		✔ Develop standardized or harmonized symbols in support of the instructions for working with robots
		✔ Transparency concerning powers and competencies in relation to the design, construction, maintenance, and dismantling of a robot
		✔ Using the best available technology and software in the design
		✔ Using certified components where possible
	IM	–
	PPE	–
Production to configuration	**BA**	✔ Safeguarding safe behaviour, safety culture and knowledge of safety among the employees who have to configure the robot
		✔ Providing an intrinsically safe working environment for installation, construction, and maintenance by preventing unnecessary risk, on the basis of a risk analysis
	CM	✔ Communication with and between the safety expert, customer, and supplier regarding using the robot safely
		✔ Providing additional instructions about the robot in relation to integrating various components
	IM	✔ Standardizing the interfaces for programming and operating robots
	PPE	–
Use	**SM**	✔ The safety of people is the top priority, then followed by self-preservation of the product or robot (= Asimov)
		✔ Organizing the work place around people's needs, supported by the robot, and not the other way round
		✔ Performing a task-risk analysis
	CM	✔ Sharing best practices throughout the sector and between sectors
		✔ Implementing good housekeeping and ensuring a clean work place, etc.
		✔ Aim for ease-of-use and easy programming and configuration
		✔ Hold periodic internal and systematic checks to see whether safety systems are working properly
		✔ Hold periodic and systematic conformity assessment of the safety requirements
		✔ Follow the training offered by the supplier and provide any necessary internal training courses
		✔ Give written and verbal instructions and information to employees who will be working with the robot and make sure they understand what they have been told
		✔ Carry out a risk analysis and draw up a plan of action concerning the use of robots (online resources, digital questionnaire)
		✔ Monitor and record experiences (and feed this information back to the supplier)
		✔ Having cyber security in order in relation to the data communication flows to and from the robot
		✔ Drawing up regulations and rules of conduct in relation to dealing with robots in the work place
		✔ Using improvement loops in order to aim for continuous improvement for the deployment of robots
		✔ Looking out for any irregularities in the software, and ordering it in good time
	IM	✔ Giving feedback to employees in the event of a breach of the safety rules
		✔ Encouraging employees to speak to each other in the work place in relation to unsafe working practices with robots and in relation to undesirable behaviour
	PPE	–

Maintenance	**SM**	–
	CM	✔ Lock-out (LoTo) procedures that guarantee that the robot is under the control of the maintenance employee
		✔ Performing a task-risk analysis
		✔ Drawing up maintenance regimes
		✔ Recording dangerous situations and providing feedback on them
	IM	✔ Good communications between the user and the supplier before maintenance work begins (on any necessary safety measures) and drawing up a plan of action
		✔ Using a Last Minute Risk Analysis (LMRA)
		✔ Introducing or making compulsory a permit to work for carrying out maintenance
	PPE	–
Updating	**SM**	✔ Make sure that robots can be adapted to new legislation or new hardware and software (in order to prevent them getting outdated)
	CM	✔ Ensure that any recycling of old components in new installations is carried out responsibly
		✔ Introduce guideline regimes for encouraging prompt updating
	IM	–
	PPE	–
Disposal	**SM**	✔ Destroying software and configuration data safely (overwriting, or destruction of components
		✔ Preventing the re-use of old (unsafe) robots that have been disposed of
	CM	✔ Acquiring knowledge of what dangers there are when dismantling the robot
		✔ Separating scarce metals and plastics in connection with the toxicity of this type of ‘waste’
		✔ Transparency regarding the environmental burden of the remaining components
	IM	–
	PPE	–

Note: SM = Source measures, CM = Collective Measures, IM = Individual measures, PPE = Personal Protection Equipment

TNO.NL

CONTACT

TNO
Schipholweg 77-89
2316 ZL Leiden
www.tno.nl

Dolf van der Beek
E dolf.vanderbeek@tno.nl
T +31 (0)88 866 5236