Princetonlaan 6
3584 CB Utrecht
PO Box 80015
3508 TA Utrecht

www.tno.nl

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

TNO-rapport

TNO 2016 R11488

Emergent risk to workplace safety as a result of the use of robots in the work place

Datum	3 November 2016
Authors	Wouter Steijn; Eric Luiijf; Dolf van der Beek (contact person)
Exemplaarnummer	
Oplage	
Aantal pagina's	54
Aantal bijlagen	2
Opdrachtgever	Ministry of Social Affairs and Employment
Projectnaam	Emerging risk to work safety through the use of robots in the work place
Projectnummer	060.20710/01.06

Inhoudsopgave

List of abbreviations

AGV	Automated Guided Vehicle
CEN	European Committee for Standardization
CENELEC	European Committee for Electrotechnical Standardization
ICS (1)	Industrial Control Systems
ICS (2)	International Classification for Standards
ICT	Information and Communication Technology
IoT	Internet of Things
ISO	International Organization for Standardization
LoRa	Long Range
LPWAN	Low Power Wide Area Network
MANET	Mobile Ad hoc NETwork
NEN	Dutch Standards Institute
OSHA	Occupational Safety & Health Administration
PPE	Personal Protective Equipment
RAN	Robot Area Network
RUR	Rossum’s Universal Robots
SZW	Ministry of Social Affairs and Employment
Wi-Fi	Wireless network

1 Introduction

For decades now, robots have been a key part of future visions in films and books. As long ago as 1920, Karel Čapek wrote a play called RUR (Rossum's Universal Robots). The first real robot, 'Gargantuan', was constructed between 1935 and 1937. It was made completely out of Meccano®[1]. Today's industrial robots strongly resemble those introduced on General Motors' car production lines in 1961[2]. In the past fifty years, robots have become much faster and more accurate, but in many cases they do no more than operate in one particular location or on rails, automatically carrying out perhaps only a single task within a fixed hazardous zone or inside a safety cage. The box on the next page shows several examples of the application of modern-day industrial robots in different sectors. These robots are still a far cry from the intelligent and autonomous robots described in science-fiction films and books. It is because of these depictions that many people imagine robots as being like humans - able to move independently, to interact with people, and to respond to their surroundings.

1.1 The need to identify new risk

Despite the aforementioned limitations, today's industrial robots have introduced new risk to the work place even though their areas of operation are clearly defined in safety zones or cages. This was brought home only too clearly in 2015 when a worker was crushed to death by a robot at a car plant[3]. Given that industrial robots are increasingly being used in agriculture, horticulture, the manufacturing sector and distribution warehouses, it is likely that similar accidents will occur more frequently in the future. Moreover, the programming of industrial robots will become increasingly complex as their tasks continue to increase either in scope or complexity. Progress is also being made with regard to robots that can move and 'see' and respond to their surroundings[4]. It is therefore quite conceivable that people will be working alongside robots in the near future, in settings that are no longer limited to a fixed location or inside a cage. People and robots will also be moving around in the same areas or rooms. This means that the risk of injury as a direct result of collisions between people and robots will increase, but indirect work-safety risk will be heightened too because of the equipment that robots may be using, and which could pose dangers to employees in the vicinity. Examples include lasers, radiation sources, welding electrodes, and mechanical equipment.

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

[2] Martijn Wisse (2015). De robot de baas: De toekomst van werk in het tweede machinetijdperk. *Scientific Council for Government Policy, p.73.*

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

[4] Amsterdam Airport Schiphol recently conducted experiments using a robot that is able to guide people who are lost: http://www.telegraaf.nl/digitaal/24800958/__Robot_wijst_de_weg_op_Schiphol__.html

It is important, as far as this trend is concerned, to look ahead and to define the machine safety of the future, so that robots can proactively be made intrinsically safe as early as the design and development stages. This calls to mind Asimov's Three Laws of Robotics[5], which robots must observe. The question is whether compliance with these laws is enough to guarantee the safety of everyone involved. Moral dilemmas could also play a role in the future - must a robot give precedence to an action to minimise a catastrophic failure over the safety of an individual employee who happens to be in the area?

Box: examples of applications of modern-day robots in the work place

Assembly lines

Welding robot

Agricultural robot

Care robot

Image sources (clockwise, from top left). Located on 26-05-2016 at:

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

Effective laws and standards - perhaps inspired by Asimov's laws - will be required in order to control the risk posed by robotisation to safety in the work place. Concrete recommendations will also have to be formulated for businesses as a means of limiting this risk. Against this background, the Ministry of Social Affairs and Employment has put the following knowledge question to TNO:

[5] *First Law*: a robot may not injure a human being or, through inaction, allow a human being to come to harm. *Second Law:* a robot must obey the orders given it by human beings, except where such orders would conflict with the First Law. *Third Law:* a robot must protect its own existence as long as such protection does not conflict with the First or Second Laws.

What risk does robotisation pose for the work place, and what control measures could be taken in order to control this risk?

This knowledge question has been incorporated in the TNO ‘Emerging Risk’ knowledge investment project. The project is looking into the possible consequences of increasing robotisation for the work place and the associated risk to the health and safety of people. The aim is to offer a basis for the safe deployment of robots in areas where people work.

Strictly speaking, current legislation on robots is silent, although legislation on machine safety is contradictory when it is strictly applied in the case of process automation. Reports in 2015[6] and the analyses, conclusions, and recommendations in this report provide insights that could function as areas for change at national and European level - in this case, the Working Conditions Act, the European Machinery Directive, and the like[7]. It is clear that robots in the vicinity of employees (and visitors) will have to meet a number of basic work-safety principles. Depending on the work-hygiene strategy, for example, this could take the form of source measures (such as the elimination and isolation of risk), collective measures (such as shielding a group from risk), individual measures, or personal protective equipment.

Standardisation institutes like NEN, CEN/CENELEC, and ISO envisage a major impact on standardisation activities in the next few years as a result of robotisation. This will have consequences for the various European directives (such as those relating to machinery and work equipment) and the related harmonisation of European standards. The purpose of this report is partly to assist the Dutch Ministry of Social Affairs and Employment in gaining an insight into the theme of Robotics and Working Conditions, and may be helpful to standardisation institutes, for example, such as NEN, in setting up a national and international standardisation agenda in this area.

In this report, TNO has looked not just at robots that are being deployed today, but also at the development of and possibilities for industrial robots in the near future. If industrial robots start moving more autonomously in a work place where people are also present, defining safety zones or placing safety cages will no longer be a clear-cut process. Other vulnerabilities may also appear as a result of people and robots working alongside each other. Industrial robots are often deployed for heavy and hazardous work and are therefore often heavy and hazardous themselves, by definition. In contrast, care robots are built precisely to be safe for the patients they are caring for[8]. At the same time, robots may be fitted with equipment that could pose a danger to people, and even in the event that a robot stops functioning there may still be dangers present because the equipment (such as welding electrodes) may be live.

Below, TNO will set out the first stage of answering the aforementioned knowledge question asked by the Ministry of Social Affairs and Employment by making an

[6] Steijn, W., van der Vorm, J. Luiijf, H., Gallis, R., van der Beek, D. Emergent risks to workplace safety as a result of IT connections of and between work equipment, TNO report 2016 R11143.

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

[8] The RIBA lifting robot, for example, is made from soft materials in order to prevent the people it lifts being hurt: https://www.youtube.com/watch?v=wOzw71j4b78

inventory of hazards and threats and by identifying possible protective measures for prevention at source or for mitigating the risk. In doing so, we will be concentrating mostly on work-safety risk of injury or death as a result of an incident involving one or more people and a robot in the work place. Following on from the above knowledge question, this report will answer the following research question in detail:

What control measures could be put forward for minimising vulnerabilities that exist now and in the near future as a result of the deployment of robots in the work place?

1.2 Guide for the reader

In this report, we are presenting the method used for answering this research question, as well as the resulting overview of vulnerabilities and possible control measures. In Chapter 2 we explain the methodology used - a literature and internet scan, followed by interviews and a workshop with experts from various fields. Chapter 3 defines the scope of the report, and sets out what we define as a robot for the purposes of this report. We use Chapter 4 to present a summary of the results of the interviews and from the workshop. In Chapter 5, finally, we present the final inventory of vulnerabilities and possible control measures for businesses that build or use robots, in the form of a knowledge chart.

2 Approach

To be able to answer the research question asked in Chapter 1, an inventory of the risk factors and vulnerabilities is needed, and possible control measures have to be identified. In doing so, we are adopting an integrated approach with control measures that contain both safety and security elements in order to minimise the risk to work-related safety that greater robotisation in the work place brings. Bearing this focus and research question in mind, the following work plan has been drawn up:

1 The scope for this report has been demarcated using a literature and internet scan (see Chapter 3) and a framework in which relevant dangers and control measures can be described.
2 Interviews are to be held with experts in the field of security and robot development and use. An actor analysis of relevant parties for these interviews will be carried out on the basis of the framework determined in stage 1.
3 A workshop will be organised, during which the results from the interviews will be fed back to experts in the field in order to add to and give greater depth to these results.
4 A final report in the form of a report and a knowledge chart.

The starting point in this report is that we regard the interplay of people and robots, danger and threat as a socio-technical system (see Figure 1). We will therefore approach both aspects and integrate them in our report.

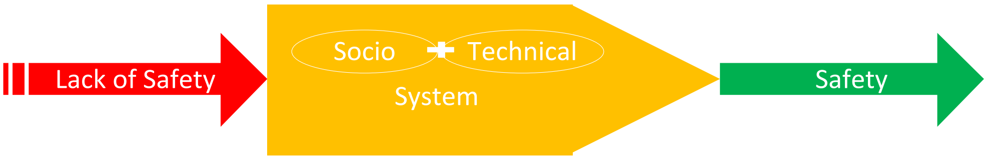

Figure 1. Safety as a socio-technical system[9]

As well as the traditional concept of *risk* in relation to the likelihood of a potential danger resulting in an actual incident and the seriousness of the injury or the damage that this leads to, we also use the terms *threat* and *vulnerability*.

In this report, we will therefore be using the following definitions for the relevant concepts. For risk, we will be using the traditional definition described above, except that we will substitute danger with threat, and add vulnerabilities as an influencer on the likelihood that a threat will actually lead to an incident: the likelihood that a potential threat will result in an actual incident is given by the vulnerabilities present, as are the seriousness of the injuries or damage that result from the incident.

[9] Adaptation from the Ministry of Housing, Spatial Planning, and the Environment (2008). *Handreiking Security Management*.

Our definition of threat is in line with that of the Belgian Privacy Commission[10]: "*every unexpected or unanticipated occurrence that could cause damage to an organisation*". Unlike danger, the concept of threat also extends to the deliberate causing of damage or injury or both. An example that comes to mind is that of a hacker who manipulates business processes without the authority to do so, as opposed to an unforeseen software error. In this connection, vulnerability can be defined as *"a weakness (inside an organisation or other entity) that can be exploited by a threat"*[11].

Establishing the definitions for these terms has been a dynamic process during this project. This is why these terms are not used entirely uniformly in the discussion on the interview and workshop results. Threat is described primarily in this context as deliberate insecurity, in addition to the concept of work risk that is based mostly on accidental insecurity.

2.1 Literature and internet scan

We first of all carried out a literature and internet scan. The purpose of the scan was threefold. We first wanted to explore the subject of robotisation and demarcate the field for this project. This is described in the next chapter. Second, we wanted to find the frameworks on the basis of which we would be able to approach the threats, vulnerabilities, and control measures, and put them into meaningful categories. Third, we wished to create an overview of relevant parties that could make a useful contribution in the interviews and workshop.

Below, we explain in brief the frameworks we have selected, the work-hygiene strategy and the life cycle, and how, using these frameworks, we arrived at an actor analysis in order to involve relevant parties with the interviews and the workshop.

2.1.1 Work-hygiene strategy

The work-hygiene strategy[12] uses the following hierarchy of possible control measures, as described in the Working Conditions Act[13]:

- Source measures (such as the elimination and isolation of risk).
- Collective measures (such as shielding a group from risk).
- Individual measures.
- Personal protective equipment.

According to the work-hygiene strategy, this hierarchy must emphatically be adhered to when applying the control measures. That means that an organisation must start with source measures, while the use of personal protective equipment is regarded only as a last solution. However, the work-hygiene strategy encourages

[10] Lexicon of the Belgian Privacy Commission: https://www.privacycommission.be/nl/lexicon#letter_d

[11] Hafkamp, W.H.M. (2008). Als alle informatie telt: een onderzoek naar kwetsbaarheden- en incidentenresponse bij ICT-organisaties. PhD dissertation, University of Amsterdam: http://dare.uva.nl/document/2/54173

[12] Working conditions portal: http://www.arboportaal.nl/onderwerpen/arbeidshygienische-strategie

[13] Working Conditions Act, online: http://wetten.overheid.nl/BWBR0010346

the combination of multiple measures from various levels (the reasonableness principle).

Given the complexity of the safety-security problem and the need to resolve it from a systemic or chain perspective, the design and development phase of products and installations is the preferred phase for finding the optimum solution. This calls to mind a system perspective - the entirety of networks of every component and relationship of persons, machines, computers, logical connections, and means of communication. Although it is paradoxical in the context of work safety, the exclusion of people is a source measure, from a security perspective.

The strengthening of work safety therefore means that the entire life cycle of a product or installation should be included and the removal of surplus and discarded products should not be overlooked.

2.1.2 Life cycle and actor analysis

In this project we have decided to approach the new risk aspects from the perspective of the life cycle of work equipment. This approach means that we consider work equipment applications from the point of view of a) design/ engineering, b) production/integrators/supply/installation, c) use, d) maintenance, e) innovation, all the way to f) disposal. There are similar phases for the entire life cycle of robots. As well as these phases, we have identified three other groups of parties that influence each part of the above life cycle:

1) Knowledge developers, such as universities and other knowledge institutes.
2) Policy developers, regulatory bodies and standards; e.g. legislators, inspection or certification bodies, standardisation institutes.
3) Service providers, such as insurance companies or telecommunication providers.

In order to create an overview of threats and control measures for these life phases, people who are experts in one or more phases and/or who can identify relevant developments had to be approached. During the literature scan, a list was drawn up of potential interview and workshop candidates for each of the phases.

2.2 Interviews

2.2.1 Interview protocol

The interviews were semi-structured - in other words, a protocol was drawn up in advance with questions as a guide. However, the interviews mainly involved follow-up questions on the matters that the interviewees were able to talk about at length. Each of the interviews lasted no more than half an hour. The protocol used can be found in Appendix A. Where necessary, questions were modified according to the background of the interviewee.

2.2.2 Participants

Based on the literature and internet scan, an actor analysis was carried out, with actors from the entire product life cycle being selected. These experts were subsequently invited by email. The aim was to find a maximum of ten participants.

The first series of 34 invitations was sent out on 18 February. A reminder was sent on 29 February, as well as a series of invitations to eleven new experts. Anonymous descriptions of the participants who were interviewed are listed in Table 1.

Table 1. Background interviews.

	Life cycle	Background/type
1	User	Producer of foodstuffs
2	User	Producer of foodstuffs
3	Knowledge institute	Interactive robotics
4	Knowledge institute	Agriculture
5	Knowledge institute	Exoskeleton
6	Policy	Business association
7	Integrator	Logistics
8	Policy	Standardisation development
9	Supplier	Industrial robots
10	Supplier	Security robots

2.3 Workshop

A workshop entitled, '*Human-robot collaboration: prevent the conflict!; what is needed to safeguard the safety of people at work'* was held on 21 April 2016. The experts were invited to attend the workshop at the end of their interviews, and invitations were also sent to the same list of actors that was used to compile the list of interviewees.

This ultimately resulted in seven participants, as well as three TNO project members. Unfortunately, a number of people were unable to attend because of another robot event being held elsewhere in the Netherlands; we were unable to hold the workshop on another occasion due to logistical reasons. The seven participants included four of the interviewees. The participants represented a large proportion of the robot life cycle, from design to use, and of knowledge and policy, as shown in Table 2.

The purpose of the workshop was to examine threats, vulnerabilities, and control measures in greater depth. To this end, the group was split into two. The two newly formed groups then brainstormed in two half-hour parallel sessions on either risk and vulnerabilities, or control measures, based on the robot life cycle. After forty minutes, the groups swapped subjects for the second round. During the sessions, the participants were asked to write ideas on Post-It notes by means of mind mapping, and to attach them to particular locations on an overview. At the end, the participants were asked to mark the most important ideas using stickers. Appendix B shows an overview of the ideas that resulted from these sessions.

Table 2. Workshop participants.

	Life cycle	Background/type
1	Designer	Industrial robots
2	Designer	Industrial robots
3	Integrator	Industrial robots
4	User	Technology

5	Knowledge institute	Exoskeleton
6	Policy	Standardisation development
7	Policy	Policy development

3 Robotics: demarcation of the report

Robotics is being applied in various industries and sectors, ranging from healthcare to manufacturing. The Dutch Smart Industry action agenda[14] is the basis for a strong commitment to the development of new product technologies and the further integration of information and communication technology (ICT) in the entire design, manufacture, and distribution process in industry (in this case, far-reaching digitisation and interweaving of devices, production resources, and organisations - the 'Internet of Things'). The primary aim here is to strengthen Dutch industry by making as much use as possible of the latest developments in ICT so that it is able to produce more efficiently, more flexibly, better in terms of quality, and more accurately when it comes to custom-made goods. There are also examples in healthcare, for instance, where investments are being made in the development of robots that fulfil functions involving repetitive precision tasks or more onerous care tasks (such as lifting beds) for patients and the elderly.

These developments primarily concern robot functionality. This means that security risk, including cyber security risk, are not the primary driver and in many cases are not an important area for attention in the development of a robot.

Given the extensive scope of the robot's working arena, it is important to clearly demarcate this in this report. We are basing this on the findings from our initial literature scan. In this report, we are interested primarily in robots in relation to safety at work. We begin by giving a general definition of a robot in the context of this research.
Because we are also interested in future developments that industrial robots may undergo, we are taking a broad look at the opportunities that are expected in the robotics field. For that reason, we will explain the concept of industrial robot in greater detail below. What developments may be expected in robotics? What could this mean for the industrial robot in relation to safety in the work place? Starting points and questions were formulated for the telephone interviews that were held with robotics experts on the basis of this information, together with the definition that has been drawn up.

Finally, we mention several important aspects that we have encountered in the literature. These aspects will be discussed later in this report, according to the direct or indirect effect they could have on safety in the work place.

3.1 Definition of robot

Nowadays, the concept of robots entails not just physical robots, but also 'smart' sensor networks, analysis software, or artificial intelligence in general[15]. A physical

[14] http://www.smartindustry.nl/wp-content/uploads/2014/11/Smart-Industry-actieagenda-LR.pdf
[15] van Est, R., & Kool, L. (2015). *Werken aan de robotsamenleving: Visies en inzichten uit de wetenschap over de relatie technologie en werkgelegenheid.* Rathenau Instituut: The Hague.

robot can be regarded as a machine with software, as a result of which the possibilities are greater than those of a standard machine.

In this report, we look primarily at the physical machine that is deployed as an industrial robot. We regard the software as a part of this robot. However, purely software robots are not being considered here. Even when it comes to the physical industrial robots, there are multiple definitions. Here are some of the definitions we found:

> *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*[16].
>
> *A robot is a machine with (a) sensors for perceiving its surroundings, (b) computer algorithms for taking decisions based on sensor data, and (c) engines for starting machinery*[17]*.*
>
> *A robot is a mechanical or virtual artificial agent, usually an electro-mechanical machine that is guided by a computer program or electronic circuitry*[18]*.*
>
> *[An industrial robot is an] automatically controlled, reprogrammable, multipurpose manipulator, programmable in three or more axes which can be either fixed in place or mobile for use in industrial automation applications*[19]*.*

Based on these definitions, we can state that:

> A robot is a machine that can be *programmed,* has *sensors*, and a certain degree of *mobility*, as a result of which the robot is able to carry out a task *autonomously*.

This definition is intended purely to make clear what we mean by the term ‘robot’ in the context of this report. The key word in this definition is the autonomy of the robot, which is determined by how it is programmed, what kind of sensors it has, and how mobile the robot is. These factors may play a role in making a distinction between various types of robot. Below, we explain the various gradations of these factors in relation to the purpose of this research.

3.1.1 Programmable

Robots are currently often programmed to be able to carry out one or a few tasks (see the box for an example of programming a simple task). When exceptional situations arise, outside the program settings, the robot runs into trouble. Robot developers are working on multi-purpose robots - robots that can perform more than one task. However, these robots have not yet reached the level of speed and accuracy that those developed for one specific task have achieved[20]. Nonetheless,

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

[17] Martijn Wisse (2015). De robot de baas: De toekomst van werk in het tweede machinetijdperk. *Scientific Council for Government Policy, p.73.*

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

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

[20] See, for example, https://www.youtube.com/watch?v=8P9geWwi9e0

they are approaching the level of those with artificial intelligence that are able to respond to and interact with their surroundings. The addition of 'emotions' and reward and penalty systems to robots is another area of research for closing the gap between people and robots as a machine. [21]

3.1.2 *Sensors*

Even robots with a relatively simple task have to recognise whether they have taken hold of a product. They have to recognise how large a screw is that needs to be picked up, or where it is located, how to scan an area in order to determine where it can move to safely, without colliding with anything.

An alternative is to actively scan an area, thereby creating a model of the area, on the basis of which the robot is able to recognise how it should operate and how it can move through the area without colliding with any other object. This technique is also used in self-driving cars.

3.1.3 *Mobility*

Where no or hardly any mobility is involved, a robot operates from a fixed location. Another possibility is that a robot sits on rails or runs along a fixed path (which may be painted red, for example, or shown with milled magnets).

In mobile robotics, the type of mobility also plays a major role, varying from wheels and caterpillar tracks to robots with two or more legs, and to suction cups[22]. This distinction is of lesser importance as far as this report is concerned.

What is important is whether a robot stays in a fixed location or has a clearly set route, or moves around autonomously using a dynamically changing route.

In relation to autonomous vehicles in open fields the report entitled *'Veiligheid van autonome voertuigen in open teelten'*[23] ('*Safety of autonomous vehicles in open fields*') is useful as it deals with the safety of vehicles of this kind in precision agriculture. Current legislation, including the EU Tractors Directive (2003/37/EC) and the EU Machinery Directive (2006/42/EC) are discussed in the context of the increasing 'robotisation' of agriculture.

3.2 Industrial robot: now

The greatest benefits of robots are that they do not tire, get bored, or complain, and that they are strong and accurate. These characteristics make them ideal for dangerous, heavy, and repetitive work[24]. Robots are therefore currently used for moving sometimes heavy materials inside a building or to lorries, for welding, spraying, and assembly work (on cars, for example), and for picking fruit and vegetables in greenhouses.

[21] See M. Seijlhouwer, Meelevende machines, De Ingenieur, 2016, volume 128, no. 4, pp. 12-19.

[22] A robot for cleaning windows, for example

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

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

The box entitled ‘Examples of applications of modern-day robots in the work place’ shows examples of industrial robots being used on assembly lines and of welding robots.

In general, industrial robots that are used extensively in factories[25]:

- are often in controlled environments,
- carry out repetitive and pre-programmed tasks,
- have no direct interaction with people (including third parties and visitors) around them,
- are not yet able to adapt to new situations.

Examples of parameters within which robots are defined and can be improved are[26]:

- the number of axes (‘degrees of freedom’) on which the robot is able to move,
- the maximum length that the robot can reach,
- the number of joints the robot has (movable parts),
- the speed and acceleration of its movements,
- its accuracy in carrying out a task,
- its accuracy when repeating a task.

It is currently often the case that robots are only useful for carrying out the specific task for which they are deployed, although the flexibility with which robots can be programmed for a new task is increasing. However, these are similar tasks for which a few coordinates have to be altered or a different tool has to be used in the same location (such as a screwdriver instead of a drill). The robots that are able to carry out different types of actions are nowhere near as efficient as industrial robots that are built for one task (see, for example, the DARPA Robotics Challenge[27]).

3.3 Industrial robot: the future

In science fiction films and books, robots are often depicted as useful companions; robots that are fully autonomous, able to adapt to any situation, and very rarely run out of energy. Creating robots like this still requires a considerable degree of development in the field of visual and auditory perception, speech (listening and speaking), manipulation, the ability to reason, to adapt and to learn, emotions[28], and understanding social conventions. Much effort is therefore being expended in the field of robotics on developing robots that can move autonomously, that are able to ‘see’ their surroundings and respond accordingly, that can work alongside people, and that are suitable for more than one task. These are referred to as ‘general purpose robots’.

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

[26] https://en.wikipedia.org/wiki/Industrial_robot

[27] https://www.youtube.com/watch?v=8P9geWwi9e0

[28] See M. Seijlhouwer, Meelevende machines, De Ingenieur, 2016, volume 128, no. 4, pp. 12-19,

Elements of this are already applied sporadically in society:

- In the ALIZ-E project, in which an interaction robot is being developed that helps diabetic children learn more about their condition[29].
- Project SPENCER is aimed at the development of robots with smart interaction systems (such as a robot that assists lost passengers at Amsterdam Airport Schiphol (2015))[30].
- Care robot LEA, which has been developed to help the elderly to continue to live independently[31].
- Robots that serve as entertainers, chefs, and waiters in a restaurant in China (2014)[32].
- The Bigdog robot and the LS3 Legged Squad Support System that are able to carry heavy loads - like a kind of pack animal - across rough terrain for infantrymen on the move[33].
- 2015 saw the finals of the DARPA Robotics Challenge, involving the development of a robot able to carry out multiple tasks autonomously (that is, opening a door, going up stairs, turning on a switch, and turning a screw)[34].
- SAM, the security robot[35].
- The 'Titan the Robot' project focuses on robots as a type of entertainment[36].

These projects show that a certain degree of humanity or a human environment in robots is being sought. It should also be mentioned that the level of interaction with these robots is still a long way off from that of interaction between people. They are also nowhere near as fast or efficient as today's industrial robots. However, it is quite conceivable that these problems will be overcome in the future. There are also elements in the development of these robots that could be of relevance to an industrial environment.

The industrial robots of the future will, in due course, be more autonomous and more adaptable in the dynamic environmental of the work place. In such an environment, they will have to adapt to dynamic changes (one container more or one container less, a temporarily blocked doorway, and so on), and they will have to work together with people, and avoid them while carrying out their own tasks. They many also have to be able to switch from one task to another in order to be able to work with products that vary in size, weight, vulnerability, and position.[37]

An important aspect is what these developments mean for the safety of people who share their work environment with robots of this kind. A big difference between industrial robots and social or care robots is that whereas the latter are developed specifically to 'handle' people, industrial robots by contrast are used primarily to

[29] http://www.aliz-e.org
[30] http://www.spencer.eu/
[31] http://www.robotcaresystems.com/wat-is-het/
[32] http://www.chinadaily.com.cn/m/jiangsu/kunshan/2014-08/08/content_18274963.htm
[33] http://www.bostondynamics.com/robot_bigdog.html
[34] https://www.youtube.com/watch?v=8P9geWwi9e0 - it is clear that robots of this type are still relatively limited in terms of efficiency.
[35] http://www.robots.nu/nederlandse-sam-robot-beveiligt-je-pand/
[36] https://www.youtube.com/watch?v=cjfPFr9SswA
[37] One example is that of picking up a component from a container in which the products are lying at a difficult angle. Martijn Wisse (2015). De robot de baas: De toekomst van werk in het tweede machinetijdperk. *Scientific Council for Government Policy, p.73.*

carry out heavy, dangerous, and repetitive work. They will therefore by definition be more risky to the safety of people, either directly or indirectly.

Every robot contains or is linked to one or more computer systems that generally interact with the outside world, and contains industrial process control systems (ICS) that operate the motors for arms and movement. These ICS and communications entail a safety-related cyber risk in the cyber-physical world - robots, in this case. More information in relation to this specific risk and the starting points can be found in a recent TNO report[38] and in Section 3.5 below, respectively.

Important drivers from industry for greater robotisation will be the functionality and usefulness of the robots. For the time being, however, autonomous or general purpose robots cannot compete with today's industrial robots when it comes to speed and efficiency. This difference will probably disappear quickly once entire industries commit to the development and large-scale deployment of robots. Such a development would be comparable to the development of self-driving cars, which has proceeded more quickly than many experts previously expected.[39]

In the context of the definition that has been set out, the following developments may be expected in relation to industrial robots in widespread use:

- **Programmable and flexible regarding tasks:** robots that can perform more than one task. This will make the process of programming more complex for the industry itself.
- **Mobility**: robots that are able to move around the work place autonomously without pre-defined paths, in order to transport materials and products or to carry out tasks in different locations. To a certain degree, this already happens with self-driving container transport at the APM container terminal in Rotterdam, for example, but in the future may happen in places where greater numbers of people are to be found.
- **Sensors**: the more mobile robots become and the more tasks they carry out, the greater the importance of their being able to 'see' their surroundings and respond accordingly will be. Sensors will also become smarter - new developments include the measuring of the force exerted by robots. In the event of unexpected resistance to an arm movement, for example, this could mean the exerted force being reduced or stopped altogether.

3.4 Types of scenarios for application of robots

The world population is expected to be in excess of nine billion by 2050[40]. This increase and the greater proportion of older people in the Western world is leading to a higher demand for products, services, and care. It is believed that robots will be used to an ever-greater degree in all kinds of sectors as an addition to the available labour, because they work accurately and because they enable new forms of production.

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

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

[40] https://nl.wikipedia.org/wiki/Wereldbevolking

To illustrate the diversity of applications of robots, here are several examples of the types of robot where work-related safety may play a role: welding robots[41], assembly robots[42], receptionists[43], transport robots (for example, robots in a container terminal[44], agrobots[45] and hospital logistics[46]), social robots (such as Nao[47] and Alica[48]), care robots (such as RIBA II[49]), service robots (such as Infinium Serve[50]), military robots (such as BigDog[51]), and security robots (such as fire-extinguishing robots[52] and security robots[53]). These examples also show that the use of robots can be expected in many different sectors or settings, such as in care, hospitality, agriculture, manufacturing, industry, leisure (at funfairs, for example), transport (such as at airports), defence, aid, inspection bodies, and Rijkswaterstaat[54].

3.5 Cyber-physical security

Robots are operated by software. In addition, they are increasingly using mobile and fixed telecommunications networks for their situational ‘awareness’, such as a map of the surroundings in which they operate or an indication of authorised persons who are in their vicinity, acquiring new orders, and interaction with other robots. Robots can be connected directly or indirectly via these networks to public networks, including the internet.

Computers, sensors, artificial intelligence software and networks give robots much potential. At the same time, it could be their Achilles’ heel. Because of malware, hacking, and technical and human errors, robots may behave differently in their physical environment to what is expected, as a result of which unsafe situations (for people) may arise. This could be directly - where a robot collides with a person - or indirectly - where a robot deviates from its normal course and knocks over a container of store chemicals, for example, or where a robot is carrying equipment (such as lasers, radiation sources, welding electrodes, mechanical equipment) that could pose a danger to people.

Below is a brief description of possible risk factors as well as a short explanation and possible mitigating measures for each of the risk factors mentioned:

[41] https://www.youtube.com/watch?v=kbi2Jd4-mu8

[42] https://www.youtube.com/watch?v=JIC0SIkmbjk

[43] Hotel robotisation of reception services and baggage handling. An extreme example is that of the Henn-na Hotel in Japan (http://www.theguardian.com/travel/2015/aug/14/japan-henn-na-hotel-staffed-by-robots). The first robots in this sector have also appeared in the Netherlands and Belgium (http://customerfirst.nl/nieuws/2015/06/servicerobot-marriot-hotel-in-gent-herkent-gasten/index.xml)

[44] https://www.youtube.com/watch?v=22SvOhI47Tw

[45] https://www.youtube.com/watch?v=LFfod3EYdqc

[46] https://www.youtube.com/watch?v=Q0gNDFXy8YI

[47] https://www.youtube.com/watch?v=aLMmGCwNfNk

[48] https://www.youtube.com/watch?v=vlh73k4ybeo

[49] https://www.youtube.com/watch?v=wOzw71j4b78

[50] https://www.youtube.com/watch?v=cLY56vefkFE

[51] https://www.youtube.com/watch?v=afeBlgRF-4g

[52] https://www.youtube.com/watch?v=e3Z7kXLQRu0

[53] http://www.robots.nu/nederlandse-sam-robot-beveiligt-je-pand/

[54] Rijkswaterstaat is part of the Dutch Ministry of Infrastructure and the Environment and responsible for the design, construction, management and maintenance of the main infrastructure facilities in the Netherlands.

1 Inaccurate sensor information.
It is expected that more and more sensors will be used in work environments that can give robots situational 'awareness'. However, sensors can provide information that does not correspond with 'reality' as a result of deliberate manipulation (malware, hackers), technical malfunction, or human error (configuration errors, for example).
Counter-measures are a self-protected node so that unexpected irregularities are not accepted and multiple information sources are correlated.

2 Disrupted communications between the sensors and the robot.
Communications between the robot and the sensors takes place mostly using wireless technology. Examples include Wi-Fi, Zigbee, Bluetooth or, in the near future, LoRa, an LPWAN technology[55].

3 A communications channel may be blocked (jamming of frequencies, denial-of-service attacks / overloading of channel) or provide incorrect information, through manipulation of the signal, for example.
Counter-measures include robust communications, strong encryption, and anti-disruption measures (industrial communications).

4 Disrupted communications between the robot and the 'home base'.
Using this communication channel, a robot may receive instructions for subsequent work activities or amended priorities; at the same time, it can pass on its current status to a control centre. Communications will take place in the same way as in the previous point, or via fixed communications as soon as a mobile robot connects itself to a charging station.
Counter-measures include robust communications, strong encryption, and anti-disruption measures (industrial communications).

5 Disrupted communications between robots themselves.
It is to be expected that autonomous robots will exchange information between themselves via their robot area network (RAN) in order to carry out their tasks as efficiently as possible. RANs can be based on technologies like Wi-Fi, but also on Mobile Ad hoc NETworks (MANETs). In the last few decades, the field of artificial intelligence has been working on the creation of intelligent agents that work together in order to do a particular job. (An example of this is swarming - where a large number of separate entities act like a coordinated swarm. This can be compared to a group of ants carrying a large insect to their colony.)
Deliberate breaches of the communications may lead to incorrect instructions and situational 'insight', which could lead to danger to people sharing the same physical space.
Counter-measures include robust communications, self-protecting node measures, strong encryption, and anti-disruption measures (industrial communications).

6 Manipulated software or instructions.
Malware may find its way unexpectedly to a robot during reprogramming work, via a laptop or portable medium like a USB drive, for example.
Counter-measures include anti-malware, intrusion detection, and separately layered networks.

[55] LoRA stands for Long Range and is a technology according to the LPWAN (Low Power Wide Area Network) specification that is intended for the massive linking of wireless 'things' to batteries. It will be used primarily for intelligent sensors. LoRa will be available from KPN throughout the Netherlands in the second quarter of 2016.

7 Unreliable control centre.
Malware, break-ins and human error at the control centre can lead to incorrect instructions being given to robots in the work place. Putting robots on a night setting during the day, for example, or changing to a 'normal' setting while maintenance work is being carried out may cause robots to unintentionally enter areas where people are working.
Counter-measures include anti-malware, separate networks, intrusion detection, and strong program-related measures that only permit transfers to less secure operational modes under strict supervision (for example, with the consent of two people).

3.6 The role of legislation

Safety in relation to non-mobile industrial robots is currently largely safeguarded by placing a safety cage around them, or by creating a safety zone using other methods so that employees can stay at a safe distance from the robots[56]. However, the more intelligent and mobile robots become (that is, more complex) in the work place, the more complex the measures for guaranteeing safety will be.

It is important here to make an inventory of what the possible applications will be and what new threats in relation to work-related safety they entail. This way, attempts can be made to anticipate situations that could occur in the near future. Literature also serves as a source of inspiration. Asimov's three laws are often mentioned, for example, as a possible starting point for robots with a high level of artificial intelligence:

- First Law: A robot may not injure a human being or, through inaction, allow a human being to come to harm.
- Second Law: A robot must obey the orders given it by human beings, except where such orders would conflict with the First Law.
- Third Law: A robot must protect its own existence as long as such protection does not conflict with the First or Second Laws.

Murphy and Woods reformulated these three laws in 2009 in order to make them usable in practice[57]:

- A human may not deploy a robot without the human–robot work system meeting the highest legal and professional standards of safety and ethics.
- A robot must respond to humans as appropriate for their roles.
- A robot must be endowed with sufficient situated autonomy to protect its own existence as long as such protection provides smooth transfer of control to other agents consistent with the First and Second Laws.

[56] The limitations of this approach are apparent from the example given at the beginning, in which the maintenance employee was situated inside the safety cage, by way of necessity, at the time of the accident.

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

Legislation may also play a role in managing the societal debate concerning robots which, as well as that of safety, encompasses many other aspects. We refer to some of these aspects below:

- *Liability and responsibility*
  Using a robot involves multiple parties - the designer and builder of the robot, the installer and integrator who put it in place, and the eventual user. Who is responsible (and therefore liable) if something is wrong with the robot or if an accident happens?
- *Acceptance by society*
  The acceptance of robots by society depends on several aspects, which first need to be addressed. Robotisation is often associated with fears of fewer jobs and therefore more unemployment. However, robotisation could lead to the creation of new employment opportunities by offering cognitive support to people with limited cognitive abilities.
  In addition, there is the question of whether a care robot is able to take over the care that a person provides. Nor is it clear how society will respond to accidents involving robots, such as when a delivery drone drops a package onto someone or collides with someone. Even the term 'robots' itself causes us to respond differently to when we are talking about a machine[58]. This is as true in the work place as it is on the street.
  The way in which robots are presented to society also plays a role here. If robots are presented as better and more precise than people, this will lead to greater acceptance among managers, but employees could feel threatened.
- *Privacy*
  Like people, robots depend on sensory information to be able to respond to their surroundings. However, it is easier for this information to be stored by robots. This makes robots a potential risk to privacy. Examples of this include a social robot with which intimate details are shared, or a care robot that involves the placing of a camera in a person's home. The privacy of people in the work place will also have to be considered, the greater the number of cameras and sensors that are placed there.
- *Morality*
  As more robots work with people and are able to take more autonomous decisions, the more important the question of whether a robot needs morality will be. Do robots have to be able to make ethical decisions, and if so, what should they be based on? Should a self-driving car opt to crash into a wall in order to avoid a child, or should the lives of its occupants have priority[59]? Should a robot put a single employee in danger in order to maintain the overall safety of the plant? In many cases, we do not even know how a person would react in these situations, so can it be pre-programmed for a robot?[60]
- *Robots' rights*
  As robots become more and more autonomous and intelligent - in other words, as they become more like people - the question arises as to whether they

[58] http://jalopnik.com/the-way-were-reacting-to-the-vw-worker-killed-by-a-robo-1715462359

[59] See also: http://jalopnik.com/what-should-robot-cars-ethical-rules-be-1579407463

[60] Another alternative is that the robot learns this itself through learning strategies involving reward and penalty systems. See M. Seijlhouwer, Meelevende machines, De Ingenieur, 2016, volume 128, no. 4, pp. 12-19.

deserve similar rights. Possible examples include the right to be maintained, or the right not to be turned off.

Some of these aspects seem a long way off when looking the current application of industrial robots. But as robotisation of society increases, these aspects will have to be resolved; they could also have an indirect effect on industrial robots and the way in which they are deployed.

4 Interview and workshop results

This chapter provides a summary of the opinions and suggestions that emerged from the interviews and workshop.

4.1 Definition of robots

Experts were asked to define the term ‘robot’. This revealed that the term can be regarded as an umbrella term that covers many machines. Below, we give a few definitions of robot characteristics that came out of the interviews:

- **Machines that are programmed for a particular purpose**.
  You do not have to operate them yourself; they are programmed to have a beginning and an end. The terms robotisation and automation are not interchangeable, but there is also no difference in principle. A robot can carry out a complex action independently. However, a robot has no will of its own; it will always operate on the basis of programmed rules.
- **All physical robots or ICT systems that assume tasks carried out by people**.
  Important elements are the sensors, a cognitive process (information processing) and execution. This also includes exoskeletons, which have to observe what a person wants to do and process the information before operating the motors with the correct timing and strength.
- **Robots can move independently**.
- **The only thing that sets robots apart from machines is that they think for themselves and are self-learning**.
  Robots are programmed to do something; it is only when the machine is able to act outside the software that it is a robot.
- **Robots are machines that have taken over tasks from people, either partly or wholly**.
  It is possible to describe a robot on the basis of a sub-division of mobility and the action it carries out. Software robots are in a category of their own.
- **Robotisation primarily concerns logistical functions**.

By way of reminder, here again is the definition that we set out at the start of this research:

> *A robot is a machine that can be programmed, has sensors, and a certain degree of mobility, as a result of which the robot is able to carry out a task autonomously.*

Finally, it emerged from the interviews that the term ‘autonomy’ is not clear. People think of autonomy as referring to robots that are able to operate entirely independently. In our definition, however, we emphasise the fact that a robot is only able to carry out autonomously the task for which it is intended. There are therefore autonomous robots in a ‘collaborative work place’, even though they work alongside people, by definition.

4.2 Advantages of robotisation

According to the experts, the benefits of robotisation relate to the opportunities for businesses to achieve greater productivity at lower costs and at a better standard of quality (greater precision). Robots are also capable of taking over physically demanding, repetitive, or dangerous work from people.

4.3 Expected developments in the near future

In general, the experts found it difficult to assess what developments could be expected in the near future. They were therefore not always able to agree on the kind of time frames involved. However, they did agree that developments are now moving at a fast pace.

Where a large proportion of the experts did concur was that a shift can be expected from the traditional robot in a fixed work place to ‘collaborative work places’ in which robots and people work together. This applies not just to demanding or dangerous work: the experts also expect a trend in which robots gain a function for smaller tasks - bring this, answer that, take me there. In addition, this collaboration means that there will always be a person in the vicinity of a robot who can assist it. A possible example is a situation in which a robot is unable to pick up a pallet because it is not quite in the right position, although robots are increasingly better able to deal with these situations thanks to the development of sensors. Three roles have been identified in agricultural technology that still have to be carried out by people in collaborative work places:

1. Steering;
   However, this role will quickly disappear given that autonomous robots are already on the market[61].
2. Safeguarding safety;
   A great deal can already be achieved using lasers and sensors, but depending on the predictability of the surroundings, a person often still needs to be on hand.
3. Checking the work being carried out;
   This seems to be something that robots are unable to do, for the time being.

As far as the shift towards collaborative work places is concerned, the experts made a specific distinction between work places with a focus on mass production and those with a focus on custom-made products. In the case of the former, the shift will be less rapid because robots will be able to carry out the work quickly and efficiently themselves. However, when customer wishes vary, such as in the car industry[62], people are still needed for the finishing touches, and the focus will lie more on the collaboration between people and robots.

Genuine interaction between people and robots is not considered likely very soon. Scenarios that involve robots interacting with humans (such as a robotic teacher)

[61] http://www.precisionmakers.com/nl/

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

are very demanding. To achieve this, the interaction between people and machines first needs to be better researched. According to some experts, it will be some ten to fifteen years before robots possess the basic skills that people have for an affordable (and marketable) price, such as being able to properly feel what they have taken hold of and to see their surroundings.

Developments are also expected with regard to robots that are capable of performing more tasks, of operating regardless of format, and of moving freely around a particular space. Below are a few specific examples that have been mentioned in relation to developments in the area of programming, sensors, and mobility.

- Progress in robotics in the next few years is expected in the area of software development in particular. The activities of major parties like Google are being monitored very closely. For example, Google recently made its artificial intelligence (AI) software open source and made it available to others[63].

- In the short term, however, it appears that the preference will be for simpler programs that are less time-consuming. In many cases, robots can currently be deployed for only one task at a time. They can be reprogrammed for a different task, but this takes a great deal of effort, in relative terms.

- The developments in programming go hand in hand with those in the field of sensors. There are now robots equipped with cameras that are able to recognise products that they have been 'taught' about, but the preference is for a robot that is capable of recognising and learning about new products automatically. By being better able to recognise products that are in the 'wrong' position, for example, robots will be less dependent on interventions from people.

- Development of sensors is also needed for greater mobility. It is expected that the first robots able to move themselves and to respond to their surroundings will be on the market within five to ten years. This forecast obviously depends on the surroundings in which the robots will be deployed: it is more likely to happen in a warehouse than in a less structured setting. As already mentioned, however, there are already robots on the market that are capable of moving both indoors[64] and outdoors[65].

4.4 Threats and vulnerabilities

In the introduction, we referred to the risk of a collision between people and robots as an area of focus in this report. The risk in question concern such matters as injury as a direct result of contact between people and robots, as well as indirect risk caused by dangerous equipment attached to robots, such as lasers, sources of radiation, welding electrodes, and mechanical equipment. This risk has added

[63] http://www.nu.nl/internet/4161514/google-maakt-zelflerende-software-beschikbaar-iedereen.html

[64] http://www.robots.nu/nederlandse-sam-robot-beveiligt-je-pand/

[65] http://www.precisionmakers.com/nl/

relevance, given the expected shift from the non-mobile and isolated robot to situations with greater interaction and collaboration between people and robots.

The focus in this report lies on the risk of a collision between a person (torso, head, and limbs) and a robot and the related direct and indirect work risk. In the interviews, we were curious to learn about possible vulnerabilities that could increase this risk. In Table 3, specific vulnerabilities that emerged during the literature scan, the interviews, and the workshop are sub-divided into seven themes.

Table 3. Overview of the vulnerabilities that were mentioned in the interviews, with a summary of the most important elements to emerge from the interviews.

Vulnerabilities and threats	Summary
Change of task	Because of the deployment of robots, the tasks that people carry out are changing. As a result of this change, employees' 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 on?
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 law 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.

4.4.1 *Change of task (overload / loss of skills)*

Robots do not always replace people in the work place, but where they are used there are changes to the tasks carried out by people. Robots are currently often dependent on people in order to be able to function (through the supply of semi-manufactured goods and materials, for example) and to check on the process. The tasks that people still have to carry out are often regarded as dull and have various implications, such as the loss of skills and under and overloading.

Because robots are able to carry out many tasks, certain skills possessed by employees may become rusty. Whenever an abnormal situation occurs, it is then questionable as to whether people will be able to respond promptly and effectively. This is the case with self-driving cars, for example, where drivers have to be able to intervene in certain emergency situations. With industrial robots too, employees have to be able to act when a robot cuts out or breaks down.

Because of the erosion of tasks performed by people, their work is becoming less attractive and there is a greater chance of loss of concentration, resulting in errors being committed. This could lead to dangerous interactions with robots, something referred to as cognitive underload.

Cognitive overload can occur when people have a monitoring task involving multiple robots at the same time. This could result in certain aspects not being noticed, or noticed too late, as a result of which an unsafe situation could arise.

Finally, there is the danger of physical overload. Possible examples include repetitive and monotonous work carried out at a rate determined by the robot. In a lot of cases, industry would like to see robots working as quickly as possible. The physical capacity of people may then come to play a subordinate role, as the ‘assistant’ to the robot.

4.4.2 *Unforeseen situations*

A robot that performs its function to an excellent standard could become a danger to people if it is used in a context for which it is not intended. One example is that of a security robot designed to move around a place of work when no people are present, but which is used when the business is operating with people in the work place. A robot may also find itself in a situation that was not foreseen when it was being programmed. Take autonomous agricultural robots, for instance, which in principle work at locations where people do not go. These machines do not usually have sensors for ‘seeing’ people. However, this will not stop unauthorised people from being in the fields where robots are operating.

Factoring in every possible scenario that could occur is often an impossible task for those designing robots. After all, people are highly unpredictable. Nonetheless, it is important to consider unforeseen situations during the design stage of every robot. Robots that have to transport heavy loads pose a direct and indirect[66] danger to people who may be in the vicinity, but even a safe assembly-line robot can become unsafe if it has to use a knife as part of its operations. It is therefore not necessarily the robot that is unsafe in itself, but the ultimate use to which it is put.

[66] A heavy load may fall from a robot, but the robot may also run into a storage unit, causing the materials stored in it to fall on a person who may be some distance from the robot itself.

‘Management of change’ is also important when upgrading or integrating existing and new systems. Even though every machine and device has individual CE certification, it is possible that the interlinking of systems and the concomitant complexities lead to the creation of new and complex interactions. By way of example, an emergency stop may no longer work because new connections have been added to the system that the emergency stop does not control.

There are also situations that can be foreseen, but which are not always considered - unsafe situations during maintenance, for example, if no account has been taken of this during the design stage. A simple example that was mentioned is that of a large robot where an engineer has to carry out maintenance work at an unsafe height. There is room for improvement at sector level when it comes to sharing safety-related information, through the sharing of best practices, for instance.

4.4.3 Trust in machines

According to one expert, people generally have too high a level of trust in the functioning of machines and technology. The internet was named as an example: people often assume that information they find online to be true, regardless of the source. But it should be remembered that all technology is man-made. This includes the software that controls robots; this software too may contain errors that can lead to the robot behaving unpredictably. Robot software has to be tested, but also properly maintained.

In addition, there is the question of who should determine what kind of choices robots should make. Suppose that a robot enters into a situation in which an accident is inevitable. Does it then opt for a ‘limited’ accident (with possible fatal consequences for one person) or for a potentially unsafe situation for multiple people? Is it possible to rationally pre-program decisions of this kind? Is the assumption that a robot will always make the right choice, or should people be in a position to overrule them?

4.4.4 Shared responsibility

The construction, configuration, installation and programming of robots are often outsourced. As a result, situations may arise in which the ultimate user of a robot knows little or nothing about the exact instructions about the robot or how it works. This could lead to an employee being hit by an unexpected movement, or to the user not knowing what to do in the event of a breakdown. Where does the responsibility lie for preventing this type of situation - with the developer of the robot, the installer, or with the end-user? Another situation is that of a sole trader using a robot in another company - who is responsible for safety then? One expert expressed concern that the lack of clarity with regard to responsibility could lead to nobody accepting it.

4.4.5 Regulatory gaps

A major vulnerability that emerged during the interviews was the influence of legislation. Given that technological developments are moving so quickly, laws and regulations rapidly become out of date, not least because amendments take so long to be enacted.

One example that was mentioned was the fact that there are still no guidelines for self-driving machines. Despite this, there are several examples of robots of this kind on the market[67]. The Occupational Safety and Health Administration in the USA (OSHA), for example, devotes a whole chapter to industrial robots and safety, although it relates primarily to non-mobile robots[68]. As more parties start using autonomously moving robots, the greater the likelihood of sub-standard designs entering the market and therefore the likelihood of unsafe situations arising. Moreover, using an old standards framework could hinder the development of better safety if it is applied to new technologies.

4.4.6 *Non-compliance*

Most accidents involving robots appear to be related to a failure to observe safety zones or instructions. In other words, users do not always comply with the safety guidelines. The chances of this happening are many times greater if the prevailing procedures are inefficient or appear to be nonsensical, or if a safety function frequently gives false alarms (such as the case of a machine that stops whenever a bird happens to fly by). Experts state that these situations can cause irritation among the users and there is an increased likelihood that they will look for ways to ignore or circumvent safety measures, or even make modifications to the robot. Time is money, after all, and people have no desire to be irritated by a 'useless' waste of time during their work. This is especially true of small companies and the self-employed.

4.4.7 *Cyber security*

If ICT security is weak, this forms a clear vulnerability that can result in the threat from hackers or loss of control becoming real possibilities. Experts recognise the risk that arise if a robot is hacked. Self-driving robots especially can become potential weapons. Although cyber security is on suppliers' agendas, it is difficult to guarantee 100% security, given the speed at which the industry is developing. An example of how this vulnerability can arise is the access to the network for suppliers who wish to carry out maintenance on robots remotely.

4.5 Control measures

In this section, we give an overview of the various control measures that emerged from the interviews. The control measures have been divided according to the life cycle of robots. The experts appeared to envisage many benefits being gained during the design phase of robots. Many risk factors can be mitigated if a robot is designed safely.

Table 4 shows an overview of the control measures for each phase of the life cycle, subdivided into the categories of the work-hygiene strategy. This is a rough subdivision, because overlapping may obviously occur, with control measures not necessarily fitting exactly into one category. Within each category, the control measures are ranked on the basis of the importance ascribed to them during the workshop (marked with an asterisk). It can be seen that the focus of the experts lay on tackling the sources and on collective or individual measures; no personal protection resources were mentioned during the workshop.

[67] Autonomous lawn mowers, for example (http://www.precisionmakers.com/) and security robots (http://www.robots.nu/nederlandse-sam-robot-beveiligt-je-pand/)

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

The table also gives an indication of what threats or vulnerabilities the control measures can reduce. Most control measures appear to be aimed at prevention of non-compliance or unforeseen situations.

We then give an explanation for each phase in relation to the control measures described as being the most important.

Table 4. Overview of the control measures that were mentioned in the interviews and the workshop, sub-divided according to phases of the life cycle.

Life cycle	Control measures	Example of vulnerability and/or threat that has been tackled
Design/ Engineering		
Source measures	✓ 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 (******)	Unforeseen situations
	✓ 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 (***)	Unforeseen situations
	✓ Implementing Asimov's three laws (**)	Regulatory gaps
	✓ Taking account of user and maintenance ergonomics when designing the robot (**)	Unforeseen situations
	✓ Testing software virtually (*)	Shared responsibility
	✓ 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	Change of task
Collective measures	✓ Incorporating an easily accessible emergency stop function in the design, where the robot safely comes to a standstill (safe mode) (*)	Unforeseen situations
	✓ Sharing best practices throughout the sector and between sectors	Non-compliance
	✓ Developing standardised or harmonised symbols in support of the instructions for working with robots	Non-compliance
	✓ Transparency concerning powers and competencies in relation to the design, construction, maintenance, and dismantling of a robot	Non-compliance
	✓ Using the best available technology and software in the design	Unforeseen situations / cyber security
	✓ Using certified components where possible	Unforeseen situations
Individual measures	*Not put forward during the workshop.*	
Personal protective equipment	*Not put forward during the workshop.*	
Production to configuration		
Tackling the source	✓ Safeguarding safe behaviour, safety culture and knowledge of safety among the employees who have to configure the robot (*****)	Non-compliance Non-compliance
	✓ Providing an intrinsically safe working environment for installation, construction, and maintenance by preventing unnecessary risk, on the basis of a risk analysis (*)	

Collective measures	✓ Communicating with and between the safety expert, customer, and supplier regarding using the robot safely	Unforeseen situations
	✓ Providing additional instructions about the robot in relation to integrating various components	Unforeseen situations
Individual measures	✓ Standardising the interfaces for programming and operating robots	Non-compliance
Personal protective equipment	*Not put forward during the workshop.*	

Life cycle	**Control measures**	**Example of vulnerability and/or threat that has been tackled**
Use		
Source measures	✓ The safety of people is the top priority, followed by self-preservation of the product or robot (= Asimov)	Trust in machines
	✓ Organising the work place around people's needs, supported by the robot, and not the other way round	Change of task
	✓ Performing a task-risk analysis	Unforeseen situations
Collective measures	✓ Sharing best practices throughout the sector and between sectors (**)	Unforeseen situations
	✓ Implementing good housekeeping and ensuring a clean work place, etc.	Non-compliance
	✓ Aiming for ease-of-use and easy programming and configuration (*)	Non-compliance
	✓ Holding periodic internal and systematic checks to see whether safety systems are working properly (*)	Shared responsibility
	✓ Holding periodic and systematic conformity assessment of the safety requirements (*)	Unforeseen situations
	✓ Following the training offered by the supplier and providing any necessary internal training courses (*)	Shared responsibility
	✓ Giving written and verbal instructions and information to employees who will be working with the robot and making sure they understand what they have been told	Non-compliance
	✓ Carrying out a risk analysis and drawing up a plan of action concerning the use of robots (online resources, digital questionnaire)	
	✓ Monitoring and recording experiences (and feeding this information back to the supplier)	Unforeseen situations
	✓ 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	Unforeseen situations
	✓ Using improvement loops in order to aim for continuous improvement for the deployment of robots	Cyber security
	✓ Looking out for any irregularities in the software, and making adjustments in good time	Non-compliance
		Non-compliance
		Unforeseen situations
Individual measures	✓ Giving feedback to employees in the event of a breach of the safety rules (*)	Non-compliance
	✓ Encouraging employees to engage with each other in the work place in relation to unsafe working practices with robots and in relation to undesirable behaviour	Non-compliance
Personal protective equipment	*Not put forward during the workshop.*	
Maintenance		
Source measures	*Not put forward during the workshop.*	
Collective measures	✓ Lock-out (LoTo) procedures that guarantee that the robot is under the control of the maintenance employee (***)	Trust in machines
	✓ Performing a task-risk analysis (***)	Unforeseen situations
	✓ Drawing up maintenance regimes	Non-compliance
	✓ Recording dangerous situations and providing feedback on them	Shared responsibility

Individual measures	✓	Good communications between the user and the supplier before maintenance work begins (on any necessary safety measures) and drawing up a plan of action (***)	Unforeseen situations
	✓	Using a Last Minute Risk Analysis (LMRA)	Unforeseen situations
	✓	Introducing or making compulsory a permit for carrying out maintenance	Non-compliance
Personal protective equipment		*Not put forward during the workshop.*	

Life cycle		**Control measures**	**Example of vulnerability and/or threat that has been tackled**
Innovation			
Source measures	✓	Making sure that robots can be adapted to new legislation or new hardware and software (in order to prevent them getting outdated) (*****)	Regulatory gaps
Collective measures	✓	Ensuring that any recycling of old components in new installations is carried out responsibly (*)	Unforeseen situations
	✓	Introducing guideline regimes for encouraging prompt updating	Unforeseen situations
Individual measures		*Not put forward during the workshop.*	
Personal protective equipment		*Not put forward during the workshop.*	
Disposal			
Source measures	✓	Destroying software and configuration data safely (overwriting, or destruction of components) (*)	Cyber security
	✓	Preventing the re-use of old (unsafe) robots that have been disposed of	Non-compliance
Collective measures	✓	Acquiring knowledge of what dangers there are when dismantling the robot (*****)	Shared responsibility
	✓	Separating scarce metals and plastics in connection with the toxicity of this type of ‘waste’ (***)	Shared responsibility
	✓	Transparency regarding the environmental burden of the remaining components	Shared responsibility
Individual measures		*Not put forward during the workshop.*	
Personal protective equipment		*Not put forward during the workshop.*	

4.5.1 *Design and engineering*

It became clear during the workshop that the experts believe that the most important control measures are taken during the design phase. One important measure is that careful consideration is given as early as the design phase to the eventual function that a robot will be fulfilling and the maintenance that will have to be performed on it. Indeed, in accordance with European Machinery Directive 2006/42/EC, a risk analysis is required when a new robot (that is, ‘machine’) is being designed, based on its intended application. For example, it may be the case that the paint fumes that result from the operation of a painting robot form a hazard for people. In the case of a different robot, it could be that a heated surface causes burns. A useful preventive approach would be to involve those who will actually be using the robot during this phase in order to use their knowledge.

The above is in keeping with the European Machinery Directive 2006/42/EC, which states that risk analyses must be carried out so that the design of the machine (in this case, a robot) is such that, on the basis of its expected use, as well as on any possible misuse, all the dangers identified in relation to the robot - at whatever point in its life cycle - are eliminated as far as possible. In the case of robots that will be working extensively with people, one method could involve implementing pads or making the robot lighter or less strong. This means no (or less) harm will occur in the event of a collision with a person (direct risk) or with an object that poses a danger to people (indirect risk). Given that robots are not currently mentioned in European Machinery Directive 2006/42/EC (Annex 4), the manufacturer must himself demonstrate that a robot meets the essential safety requirements (Annex 1), without having to involve an external party in the process. The Directive also states that any residual risk must be described in the instructions (Annex 1, section 1.7.4.2, (l)).

Another example is that of a robot that moves around freely, but which is designed to move more slowly and is made more visible in response to a wish by the customer for the robot to move among people. The behaviour of a robot can also be made more predictable with the help of traffic rules during normal working hours, rather than calculating the shortest route.

Furthermore, it is important that the design of a robot factors in ergonomics. Taking into account - during the design phase - the people who will ultimately be using the robot or who may be in its vicinity, either during normal operations or maintenance work, means that many of the dangers associated with the robot can be eliminated. For example, it is possible to prevent a person from being physically overloaded when using an exoskeleton by looking into what the relevant human limits are in advance and by looking at what exactly the exoskeleton is to be used for. The speed and acceleration of the movements can be adjusted accordingly.

Even in a so-called lights-out factory, in which no people are involved with the primary process, the human factor will still play a role. Here, people will be needed to monitor the robots and to maintain and repair them, and to carry out error diagnoses. In relation to the monitoring task, the prevention of cognitive underloading and overloading will be a challenge, which can be met by making the work interesting and challenging (the focus can also be placed on designing the work place specifically for employees with an impairment or a particular talent). The operator system will have to be optimised for this by looking at where crucial errors may not be made and offering assistance accordingly. This means a certain level of knowledge will be needed in order to be able to work with the operator system. As far as the task of maintenance is concerned, it is important that a robot is designed or located so that maintenance work can be carried out safely (working at a great height is a case in point).

Adaptive automation is the concept by which software monitors people who work with robots, thereby adapting the speed of the process in order to prevent overloading. This means that people remain in control of the work process, and it will lead to greater acceptance in the work place.

Two specific technological aspects that need to be considered during the robot design phase emerged from the interviews - the sensors and an emergency stop function.

Historically, there has generally been a physical barrier between robots and people for safety purposes. Robots nowadays do not have to be fully protected because they have sensors, which enable them to detect the presence of people; they then run more slowly or stop altogether if a person enters the robot's range of operation. The advantage of these sensors is that they keep people safe whenever the robots have to be approached, such as during maintenance work. If the intrinsic safety of components cannot be demonstrated, it will be necessary to revert to putting a physical barrier in place as an additional safety measure.

As well as preventing collisions, sensors can also be used to establish whether every safety condition has been met. This could be to determine whether anyone is in the control seat of a driver-assisted vehicle, for instance. An example of where this could be useful is in the agriculture sector, where it is very tempting for farmers to get in and out of a slow-moving semi-autonomous tractor.

A physical emergency stop button for instantly deactivating a robot is an obvious control measure. Ideally, it should be possible for it to be activated remotely. This would allow an immediate intervention whenever a dangerous situation threatens to arise. In tests involving agricultural robots, for example, one person is always given the task of walking near the robot, carrying the emergency stop device. This should also be the only task assigned to that person. Of course, this does raise the risk of a potentially mind-numbing task, in which the likelihood of distraction and error becomes greater.

Finally, it is important to continue to develop robots and the safety functions and to remain up to date with the most recent technological possibilities. Collision bars and lasers for stopping robots that threaten to run into an object are the first steps towards greater safety. However, new developments, including intuitive software such as fuzzy logic, are moving towards smarter robots that are able to predict what moving objects like people are going to do in their spatial interactions with them. Conversely, it is possible that the behaviour of a robot can be used to 'steer' a person around it if it is clear what the aim and direction of the robot is. For example, people would be more inclined to step to one side if a robot was moving in a straight line at a constant speed than if the robot was moving from side to side as it attempted to manoeuvre its way past them.

This is easier to achieve in a structured environment than it is outside, for example. Outdoors, robots have to be able to distinguish people from, say, moving objects such as branches or a piece of paper flying around, while shadows too could result in an unnecessary stop. Another example is being able to determine that braking completely is not necessary if there is a bird in the way; the problem will probably resolve itself if the speed is simply reduced.

These developments will ultimately lead to fewer false alarms as a result of safety functions, and this will make robots more people-friendly and safer for people. Consequently, the chances of irritation among users will diminish, as will those of non-compliance with the safety regulations. Nonetheless, as robots become smarter, the necessity of programming certain rules into the robot, such as Asimov's three laws, will grow. However, it does not appear that this will be necessary in the near future, at least.

4.5.2 Production, delivery, composition, installation, and configuration

When it comes to interacting with robots, the expertise of employees working with them is important at every stage of the robots' life span. This includes giving clear and accurate instructions, which come under the responsibility of employers and manufacturers. One challenge that emerged from the workshop is that multiple manufacturers are often involved with one robot. It could be, for example, that various manufacturers are involved separately with the robot itself, the operating system, and the software. Ultimately, the robot will have to fall under the responsibility of a single manufacturer once it is brought onto the market. These responsibilities are contained in Machinery Directive 2006/42/EC and state, inter alia, that robots must comply with the essential health and safety requirements (Annex 1) and have instructions for use (Annex 5).

Ensuring safe behaviour, a safety culture and knowledge of safety among employees who configure and operate robots emerged in the workshop as the most important control measure during this phase. In other words, it is important that robots are correctly put together, configured, and positioned at a company's premises. One way of achieving this is to guarantee that skilled employees are charged with these tasks.

Additionally, training users in how to use robots safely was mentioned as an important control measure. As well as testing whether a robot has been correctly positioned and works, suppliers, system integrators and installers must provide instructions on how robots should be used. Responsibility for following these instructions lies both with the customer (the end-user of the robot) and the supplier/installer. The latter must provide the instructions and the former must be certain that employees have sufficient knowledge of the robot. This implies a certain level of knowledge on the part of the customer. Information and communications are important, especially now that ever-fewer physical partitions are being used.

An example of this is traffic rules that are drawn up in order to prevent collisions with autonomously moving robots. The rules should be drawn up in consultation with the designer, but responsibility for ensuring that every employee (and third party, such as visitors) knows the rules lie with the organisation where the robot is used.

Suppliers often teach customers how to handle and operate the robots they supply, and how to program them.

Moreover, the sharing of best practices between integrators and installers should be done more frequently.

4.5.3 *Use*

During the usage phase, too, the sharing of best practices was mentioned as an important control measure. Otherwise, the experts had no particular preferences regarding control measures, but various ones were described as being important. These included the importance of housekeeping (asset management) relating to robots or the ease with which robots can be used or programmed.

Reference was also made to training in the use of a robot. It is important that people who work with robots know how they work and what they do. They have to be able to answer the question, "What movements can the robot make and what does this mean for me?" Employees must have a complete understanding of the robot, know how to deal with breakdowns, and know how to minimise the risk to themselves. Training, information, and adherence to internal procedures are essential aspects of this.

However, robotisation also has consequences for demand for training courses. The increase in robotisation will result in changes to the composition of workforces in organisations due to changes in the requirements of tasks. There will be a greater need for employees with technical qualifications in manufacturing and processing lines, who will be needed to carry out complex tasks and prevent or resolve breakdowns.

As far as the workload is concerned, there are two distinct trends:

1 Physical and monotonous work will be eliminated over time and monitoring tasks will increase. This will raise the required level of educational qualifications in organisations where robots are used. It is important in this context that technological and digital components quickly gain a more prominent role in training courses and study programmes. The general level of knowledge will therefore have to be adapted to technological and other developments in society.

2 The work will become dull and monotonous if people become assistants to robots who have to carry out tedious tasks in order to enable the robots to function (for example, straightening a crate not recognised by a robot). It is therefore important to properly define the tasks performed by people and machines so that it is clear when and how people should intervene. At present, work processes are often designed according to what is technically possible. A better method would be to structure work processes from the point of view of employees being assisted by robots.

It is also currently the case that most robots are better able to 'understand' their surroundings if these are structured. Wherever possible, people should therefore be kept away from areas where robots work.

Organisations can carry out risk inventories and risk evaluations on robots. The work place and process can then be organised and a plan of action drawn up on the basis of the results.

Finally, internal procedures could be an important control measure while robots are being used. Possible examples include 'life-saving rules'[69], a willingness to point out to others when they are acting incorrectly, feedback when breaching safety rules, periodic checks on whether safety systems are still working, and a periodic conformity assessment (in relation to safety regulations).

Finally, improvement loops can help to continuously raise the standards of processes to a higher level. This means looking at imperfections throughout the process and improving them.

It is becoming increasingly difficult to write a concrete manual that users have to keep to in order to use robots safely or work with them. This is because, unlike a microwave, the function and context in which robots are used are becoming more and more difficult to define in clear-cut terms. In consequence, it is becoming ever more difficult to determine how tasks relating to the management of risk factors should be designated.

4.5.4 *Maintenance*

An important control measure for maintenance concerns communication with the customer, whether beforehand regarding any necessary safety measures, drawing up a formal job safety plan, or applying for a permit to work. This makes it possible to exclude the possibility of maintenance employees running unnecessary risk.

At the same time, it is important that maintenance employees are able to switch off or overrule robots at all times. An example of a good method is the LTT principle[70]:

- Lock out: switching off and then locking a machine,
- Tag out: placing a tag stating why a machine has been switched off, and by whom,
- Test: whether the machine really is switched off.

Suppliers also keep their own statistics up to date in relation to dangerous situations. These often concern notifications by people who have encountered reduced functional safety as a result of obsolescence or because access to a robot is not as it should be. Customers are then warned about this.

In addition, today's mobile robots regularly return to a synchronisation position, where any irregularities can be detected, on the basis of which they can be switched off or adjusted.

Organisations will also have to introduce safety and cyber security requirements relating to employees and third-party services, such as maintenance, whether carried out remotely or not, to the robots.

[69] See for example the Shell Life Saving Rules: http://www.shell.nl/sustainability/veiligheid.html
[70] http://www.hamer.net/algemeen/lock-tag of http://www.verbondpk.nl/Arbocatalogus/LTT

4.5.5 Innovation

The opinion of the experts regarding the innovation phase was generally that it differs little from the installation phase. What did emerge, however, was the importance of remaining flexible in relation to future developments. Examples in point include that of changes to legislation that make a particular application for a robot no longer possible, or indeed possible, or when a better component comes onto the market, making it unnecessary to replace an entire robot.

4.5.6 Destruction/disassembly and disposal

For the final phase, destruction/disassembly and disposal, two control measures were given particular prominence. First, there should be clear instructions about what the specific dangers are during the physical dismantling of a robot. The second control measure concerned the toxicity of the resulting ‘waste’ from a robot: the scarce metals and plastics have to be carefully separated.

Moreover, steps must be taken to prevent configuration data such as digital certificates, network addresses, and passwords ending up ‘on the street’, giving unauthorised persons access to the business processes and other robots involved in them.[71]

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

5 Discussion

This project is helping to contribute towards raising awareness of the risk to people associated with robotisation in the work settings of the various industries where further robotisation of the production process is planned. Our report is in response to the knowledge question asked by the Dutch Ministry of Social Affairs and Employment (SZW):

What risk does robotisation pose for the work place, and what control measures could be taken in order to control this risk?

Developments in robotics are moving fast, as shown from the increasing focus in the Netherlands and internationally on robots, robotisation, Industry 2.0, and smart industry. This is evident in publications like 'De Ingenieur'[72], 'De Lichtkogel'[73] and 'Control Design'[74], as well as in reports by the Rathenau Instituut[75]. There are also more and more lectures and meetings on the subject of robotisation[76]. This research is taking place in anticipation of developments that are expected regarding the functionality of more powerful robots. The outcome of research will be useful in the development of new robots.

The experts were aware of only very few, if any, accidents between robots and people. This is in line with a recent report by Control Systems that stated that just 25 serious robot-related work incidents had taken place in the US since 1 January 1997, of which fewer than 20 involved fatalities (in comparison to 4,679 work-related fatal incidents in 2014)[77]. What has become clear is that incidents also – or especially - occur outside of normal operation, such as during the placing, testing, or maintaining of robots[78]. This underlines the importance of considering the entire life cycle of robots.

However, the more robots are used, the number of incidents involving robots is likely to increase. As well as collisions, there are indirect risk such as contact between a robot and a storage unit, for example, or stacked goods, leading to an unsafe situation - a cracked container filled with chemicals, or heavy goods that falls over, for instance. Another possibility is that of reduced concentration on the part of

[72] M. Seijlhouwer, Meelevende machines, De Ingenieur, 2016, volume 128, no. 4, pp. 12-19.

[73] Robots in de openbare Ruimte, Lichtkogel no. 1, 2016. https://staticresources.rijkswaterstaat.nl/binaries/Lichtkogel%202016%20nr1%20Robots%20in%20de%20openbare%20ruimte_tcm21-80156.pdf

[74] Collaborative Robots in Control Design for Machine Builders (2016).

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

[76] For example, a meeting about the deployment of robots for emergency services during disasters.

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

[78] See the OSHA technical Manual Section 4, Chapter 4: https://www.osha.gov/dts/osta/otm/otm_iv/otm_iv_4.html

an employee owing to cognitive underload. So far, little is known about the psychosocial effects of working with robots, such as motivation or loss of quality of work.

This report has drawn up an inventory of threats and vulnerabilities and of control measures designed to counteract them during the various life phases of robots. In this chapter, we discuss the most important findings and several implications of the results of this report.

5.1 Robotics as an umbrella term

One of the first things to stand out during the interviews with the experts is that robots and robotics are problematic terms. What exactly is a robot; what type of robot are we talking about? A consensus regarding the definition of these terms had to be reached before any discussion could take place.

Robotics is an umbrella term that covers many different applications. Even using our definition, that a robot is a machine that can be programmed, has sensors, and a certain degree of mobility, as a result of which it is able to carry out a task autonomously, it is possible to include both intelligent robots of the kind shown in films (such as in *I, Robot*) and a simple washer dryer. The latter, after all, is a machine that can be programmed to autonomously dry clothes that have been washed, using sensors to shorten the program depending on the size of the load and the degree to which it is soiled.

We also encountered some interesting contrasts in the definitions used by the experts. One, for example, said that as long as a machine did not act beyond its software, it was not a robot. Meanwhile another said that even the most advanced robots will ultimately be no more than a collection of programmed rules.

A question that extends from this is what is ultimately possible in the field of robotics and what we can expect in the short term. This seems very much to depend on which expert you speak to. In industry, the tendency for now is to look pragmatically at the robots that they have or want. Processes have to be faster, more accurate, easier, and less costly, but must obviously be safe. In Section 5.6, we will examine what the future can be expected to hold for the industrial robot.

What matters for now, though, is that the term robot is not sufficiently distinctive as a working definition. There are even wide variations of industrial robot, depending on how they are used.

5.2 Safe design

The experts generally agreed that designing a robot is the most important time for removing most unsafe aspects from the system. This is equivalent to the principle of tackling the source in the work-hygiene strategy.

No specific recommendations were made, however, for one simple reason - there is no such thing as a universally safe robot design. The aspects that are necessary depend largely on the function for which a robot is to be deployed. A lighter frame for robots that work a lot with people can minimise any damage resulting from a collision, but in the case of those that have to lift and move heavy loads, a lighter frame will result in structural integrity that is too low, thereby creating other unsafe situations (dropping the load, for example).

It is therefore generally recommended that risk analyses be carried out in advance of the proposed application and to include these in the design and to use the most suitable technologies.

As a rule, robots consist of two parts. There is the machine or arms that perform the work, and the control system. When analysing the risk aspects, it is not just the part of the robot that carries out the work that should be looked at, but also the control system. Is it sufficiently secured against unauthorised outside influences (such as hackers); are there any programming errors; is it up to date; and who exactly has access to it? The integrity of the operating software determines to a large extent whether a robot can be used safely, as well as the degree to which it is screened from external undesirable influences. The same applies to the control of dangerous elements that form part of, or are attached to, the robot, such as lasers, sources of radiation, and machinery.

Another recommendation to emerge was that the working relationship between people and robots should be optimised as far as possible. Robots are very good at carrying out repetitive work accurately and quickly. People are creative, good at taking decisions, flexible, and adaptive. Using the best of both creates the best-possible benefit from the relationship between the two. If this is overlooked and employees become dependent on a robot, or if people no longer have any kind of challenge, there is a risk that they will not respond effectively in exceptional situations, or that the tasks that do remain are not challenging enough, thereby increasing the likelihood of errors being committed.

In addition, the experts were unanimous that robots should always have an emergency stop functionality. That is, people must always be able to switch off or overrule a robot in a safe manner. This means that people remain in control of, and responsible for, the entire process.

The role of sensors is important, too. Especially now that physical barriers are disappearing, there will have to be a greater reliance on sensors. Sensors have been able to keep up to date with developments relating to the functionality of robots[79]. It is important that they continue to be improved and that the software behind them becomes ever ‘smarter’. Examples that come to mind are the 3D scanners that recognise when a human foot comes within a certain radius[80]. One area where these sensors are used is guarding buildings. However, it is also possible to think ‘out of the box’ by creating a ‘safety shield’ around a person, for

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

[80] Example of product on the market: https://www.sick.com/media/dox/9/79/879/Industry_guide_Building_Safety_and_Security_en_IM0036879.PDF

example, to which robots would respond by stopping as soon as the shield comes close[81].

5.3 The human factor

Although the preference is to tackle the risk at the source - by designing an inherently safe robot - the human factor will also have to be taken into consideration. A significant degree of responsibility for this lies with the organisations that use the robots. This entails people in organisations adhering to the relevant guidelines and taking any necessary training courses, and regularly updating them. It also means using appropriately qualified employees or organisations for composition, installation, configuration, maintenance, and disposal.

For organisations too, it is important to include robots in risk inventories and evaluations. Organisations can be assisted in this using methods such as electronic questionnaires and checklists. A codified questionnaire will help with risk inventories and evaluations, and can also be of use for demonstrating compliance with prevailing legislative and regulatory aspects. At the same time, it can be a useful source of best practices.

We have to guard against relying too much on robots in cases where this is not justified. After all, robots are programmed by people using man-made software, which has to be checked in order to prevent any errors and to ensure that it continues to work properly. Who is going to determine or check whether robots will make moral decisions, and on the basis of what arguments?

One risk that has been mentioned is that robotisation means that robot software will soon determine what is and what is not possible. Take administrative robots, for example. They have great difficulty in dealing with exceptional circumstances that people have few problems handling, because they occur ‘outside their software’.

At the same time, organisations can quickly forget how a process takes place without the help of a robot. One example that was given was how, after a failure of the automatic check-in system at an airport, the changeover to a manual system proved very difficult.

The more robots take on tasks, the more we are likely to become dependent on robots. This is because the programme can become all-decisive, while human skills fall into disrepair. In certain situations, however, self-driving cars rely on their driver, and people are even needed in lights-out factories (where only robots are found in the work area) in order to monitor the robots and control the process. This situation therefore creates jobs.

In other words, it seems that robots will continue to depend on people for the time being. It is important to carefully integrate the human factor in robot designs as well as in the eventual work process in order to use robots to the best-possible effect.

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

5.4 Legislation

5.4.1 Legislation on general robot applications

As far as the mechanical side of today's robots is concerned, it seems that existing legislation and standards are largely sufficient. From the point of view of standards, the current generation of robots is not regarded as new but as machines[82] with electronic components (for example, talking and communication by robots) and non-electronic ones. However, because they involve a composition that is not entirely covered by current standards, existing legislation is not adequate. For example, the software and its risk of non-safety fall outside the Machinery Directive. Nonetheless, developments are afoot, with both ICS (International Classification for Standards) and ISO (International Organization for Standardization) bringing out standards. Standards ISO 10218-1:2011, ISO 10218-2:2011 and ISO 13482:2014, for example, specifically concern the safety regulations for industrial and care robots.

In practice, standards keep up with developments in society. This is set to continue for the time being, given that many technological developments are not yet ready to be launched on the market. Take the self-driving car, for example - there are already many test pilot schemes, but it will be some time before everyone has a self-driving car[83]. On the one hand, this allows time for legislation in this area to be brought up to date, but on the other, there are no relevant legal precedents that can help point legislators in the right direction. It is important to identify regulatory gaps and to fill them in good time.

The lack of legislation pertaining to autonomous underwater and seafaring vessels, and road vehicles, can be regarded as a 'regulatory gap' from a robotics perspective. This is because there are different types of autonomously moving robots on the market for which no regulations exist. There are no regulations in this area in other countries either. Experimenting with robots can also conflict current legislation, which does not provide for autonomous robots in outdoor areas. Autonomous vehicles are a clear example of legislation lagging behind the market; the robots have already been sold by various parties, after all[84]. Robots of this kind are designed on the initiative of market parties and on the basis of common sense, with customer demand being the guiding factor in what the robots are able to do and what they have to do. The market often fills up this type of gap. In cases where businesses are working on the same innovation, they work together, sometimes with government bodies, to consider what they are doing. This is not necessarily a problem, but it could lead to unsafe situations the more parties enter this area without agreements and standards.

[82] OSHA also describes robots as machines: https://www.osha.gov/Publications/Mach_SafeGuard/chapt6.html

[83] The present generation of self-driving cars, for example, has problems with poor weather conditions. See, for example, https://static.googleusercontent.com/media/www.google.com/en//selfdrivingcar/files/reports/report-1215.pdf.

[84] See, for example, http://www.precisionmakers.com/nl/; and http://robotsecuritysystems.com/

5.4.2 *Legislation specifically in the agriculture sector*

This problem also exists in the agriculture sector. It has drawn up a report[85] concerning legislation and recommendations on the application of autonomous tractors. The conclusion in the report states that semi-autonomous vehicles should be used in accordance with Directive 2009/127/EC (Directive on Machinery for Pesticide Application) that lays down a requirement for monitoring and the possibility to intervene. The reason for applying this directive is that autonomous tractors sometimes pull spraying machinery, and because the Tractors Directive (2003/37/EC[86]) and the Machinery Directive (2006/42/EC) do not yet contain any provision for this.

The complexity here is that the tractor is a vehicle and falls under this legislation, while the machinery being pulled is regarded as machinery. With the development of, for example, harvesting robots pulled by automatic vehicles, the dividing line between the Tractor Directive and the Machinery Directive will be breached.

The autonomy of an agricultural robot in terms of space and distance may also be limited by more stringent legislation of the kind being prepared for drones. This could lead to legitimate developments relating to robots being inadvertently aborted, unless a licensing option is incorporated into the legislation.

It could be that trade unions have a greater role to play here. There is CEMA, for example, a European trade union of developers of agriculture machinery, which is campaigning hard for balanced legislation in the EU that will make it possible to apply smart technologies.

5.4.3 *Need for prompt governance*

It is important for the development of new robots that a legal framework is in place. As robots and new applications are developed, thought has to be given to legislation at an early stage. If not, legislation at a later stage may prove to be a hindrance if the product is not demonstrably safe. This concept is known as ‘lock in’ and can result in the failure of a product. For start-ups, it is important to know what laws and regulations have to be met, which depends on what you are seeking to develop. By way of example, certain materials may not be used in the composition of robots being developed for the foodstuffs sector. Similarly, applications such as the self-driving vehicles that Domino’s Pizza is aiming to use for deliveries may run into problems with legislation[87].

5.5 Supply chain liability

In order to create a safe robot, the entire supply chain involved with its life cycle is needed. The process starts by the supplier making a safe robot design. The system

[85] Heijting, Kempenaar, & Nieuwenhuizen, (2013). Veiligheid van autonome voertuigen in open teelten. Wet- en regelgeving en aanbevelingen voor de veiligheid. *PPL project no. 79/ZGLE.11.0108.*

[86] A new tractor directive, Regulation no. 167/2013, has appeared the since the publication of the report (http://eur-lex.europa.eu/legal-ontent/EN/TXT/HTML/?uri=CELEX:32013R0167&from=sv). This directive does not make any mention of autonomous tractors either.

[87] http://www.nu.nl/gadgets/4232354/dominos-wil-zelfrijdend-autootje-pizzas-laten-bezorgen.html

integrators then have to put the robot together, with safety as their first priority, and install it and configure it at the customer's premises, with the related certificate. The robot then has to be used safely, and systematically and safely maintained (including the software), and finally, kept up to date, also in a safe manner, or dismantled in the correct way and disposed of when it has become outdated.

Responsibility for this is shared, in order to banish all the risk. Each party should carry out a risk inventory and risk evaluation responsibly (and be certified for doing so), but their responsibilities also extend beyond their own work activities. The supply provides instructions for the integrator, who trains the customer how to use the robot, and the customer gives feedback on how the robot is performing. Things have now reached the stage where industrial robots are controlled remotely, from India, for example[88]. Operating jointly and keeping each of the other parties properly informed helps to optimise the process.

5.6 Future of industrial robots

Going back to our definition, which we gave at the start of this report -

> *"a robot is a machine that can be programmed, has sensors, and a certain degree of mobility, as a result of which the robot is able to carry out a task autonomously"* -

we note that for industrial robots, developments in relation to each of the key words can be expected in the near or longer-term future.

As people and robots work together more closely, better *sensors* will be needed in order to accurately chart the surroundings and to enable robots to read their surroundings. This involves not just 'end of arm' tools (that enable robots to recognise problems, such as when a product is positioned incorrectly or the wrong product is presented), but also safety sensors that can prevent a collision or recognise if a person is nearby.

In addition to improved sensors, the underlying software will have to be developed further as well, while artificial intelligence will be added in order to respond effectively to the input. An example that comes to mind here is the need for a robot to be able to assess the intentions of a person in its vicinity in order to prevent a collision ('is that person going to cross my path or not?'). It is difficult to determine where the limit of artificial intelligence that robots can achieve (in the near future) lies. For robots that think for themselves and are able to operate outside their *software,* a completely separate collection of control measures will be needed (bearing Asimov's three laws in mind) and is sure to be accompanied by a range of societal discussions (legal autonomy of robots, robot rights, for example?). Industry is not seemingly too interested in waiting around for the outcomes of such discussions and is instead focusing on the efficiency and productivity to be gained from further robotisation. However, robots that think for themselves are not entirely inconceivable, given that safer robots are likely to result from the smarter operational software used in robots of this kind.

[88] See Angela Merkel and YuMi, for example, https://www.youtube.com/watch?v=ytC9WC3ec_0

Finally, the number of *autonomously* moving robots in the work place will increase. There are already various types on the market (such as autonomous grass cutters or security robots), but also many types of automated guided vehicles (AGVs[89]), which are already used in various work settings[90]. The current hype around self-driving cars will probably ensure that these developments will proceed at a rapid pace. With the greater flexibility that *moving* robots have compared to those in fixed locations, the number of self-driving robots operating in the vicinity of people will probably increase.

It is difficult to forecast exactly how quickly these developments will go. The speed of innovation is largely determined by commerce. As long as the technology is costly, there will not be a market for it, which may retard further developments. However, as soon as there is a market, technological developments can move very rapidly.

It seems obvious that these developments are coming - the main question is when. This means that it is important to be well prepared for these forthcoming changes. This report gives an inventory of vulnerabilities and threats associated with these developments. On this basis, an overview has been drawn up of control measures that can be taken to counteract them. This will take us a step closer to a future generation of robots that are not only faster, better, and smarter, but also safer.

[89] AGVs are semi-autonomous robots or machines that follow a pre-defined route. They are already used extensively in factories and warehouses.

[90] Examples that come to mind are the self-driving transport vehicles that move containers around the APM terminal at Maasvlakte 2.

6 Signatures

Utrecht, 1 July 2016

Name of second reader:

J. van der Eerenbeemt MSc.

Signature:	Authorisation for release:
F.A. van der Beek MSc. Project manager	H.C. Borst Research manager

A Appendix: Interview protocol

1. *Introduction and start of interview*

2. *Ask about current context*
   - What is your background in relation to robots?
   - What type of robots do you work with? *or* What robot applications in the field of work are you familiar with?
   - In what context? *or* In what sectors or industries?
   - What are the main benefits of these robots?
   - What are the main dangers to work-related and personal safety?
   - How often do dangerous situations arise? / Are you aware of any accidents or near misses?
   - What safety measures are in place?
   - What safety measures are lacking, in your view?
   - What is the preferred risk-management strategy / approach (life cycle approach, certification, insurance, etc.)?
   - Are communications and reports on potential risk to health and safety relating to robots sufficient?

3. *Near / distant (5-30 years) future*
   - What developments do you expect in the field of robotics?
   - What will be the main benefits of these developments?
   - What will be the main dangers of these developments?
   - How will uncertainties in the development of robots be managed?
   - What extra/new safety measures will have to be taken?

4. *Cyber risk*
   - To what extent do robots currently communicate with other robots - that is, do they communicate wirelessly?
   - If not, is such a development expected in the short term?
   - Are measures already being taken against cyber breaches? If so, which ones?
   - What is the influence of the surroundings in which robots operate on their actions?

5. *Conclusion*
   - What is the role of legislation in supervising this?
   - Are there any other important actors in this area or documents that we should know about?

B Appendix: Results from workshop

Overview of the input on the posters during the workshop. After this, the participants were able to use stickers to mark the most important ideas. Asterisk were used to show how many stickers were attached to each idea.

Threats

- No account taken of the fact that robots have to be maintained (**)
- Who may overrule, and when? People – Robot
- Dilemma: Choice between limited accident (with possible fatal outcome for a person) and the unsafety of many people
- Unexpected (not foreseen/programmed) acts by people or robots (*)
- People acting illogically (unpredictable)
- Basic safety of industrial control systems (or lack of safety)
- Is the design 'testably'/'provably' safe (**)
- When could vulnerabilities arise: design (programming); system integration; putting into operation; operation; maintenance (software upgrade); disposal
- Safety of mobile robots in large or open spaces
- Machine (robot) in public space
- Is the safety area demonstrably safe if multiple mobile robots work together / operate in the work area?
- Making a robot idiot-proof? No, tackle people's mentality, the safety level lower and the robot slower (**)
- Out-of-date standards frameworks are hindering 'better safety'
- Loss of employment
- New health risk, physical underload and overload (****)
- Does changing people's tasks lead to poorer concentration in the work place and dangerous interaction with mobile robots?
- Erosion of functions (so less attractive) when people and robots work together
- Maintenance and software updates - controllability and certification of safety
- Lack of safety caused by remote maintenance of software
- Sensitivity to external access/influence, such as hacking, outside party taking over operation (**)
- Maintenance issues; liability issues
- Applications determine the degree of danger, not just the robot
- Application versus incorrect application
- Speed versus safety, smart industry is hot
- Learning curve means uncertainty; fast learning is needed
- Security issues: …. (*)

Vulnerabilities

- Not sharing (at sector level) incidents between actors
- How do you get good practices across the sector (or at international level)
- Inadequate software quality (unexpected behaviour)
- Knowledge and skills for engineer or operator

- Weak ICY security (risk of manipulation)
- Algorithm of the software reliable? Has been created by people! (*)
- Safety PLC, incorrect programming (**)
- How safe to install, how safe to put together?
- Failures on the part of people and machines (bilateral); fail safe, damage tolerant (both ways), fool proof
- Dilemma: if accident is unavoidable, which choice to make? Who can/must die!
- Failure of sensor; what next? Emergency situations and sensors (e.g. fog) (**)
- Organisational, if sole trader uses a window cleaning robot at a company's premises; who is responsible for safety in that case? (**)
- How can maintenance be carried out safely?
- How can I test every situation? How do I know what all the possible combinations are? (*****)
  Resistance among users: Loss of autonomy, greater dependence on process imposed by robot (**)
- Robot is faster and better /more accurate than people: greater acceptance by user (management), lower acceptance by employee
- No 'self-protecting node' principle in 'supply chain' components
- Innovation restriction
- Safety expert not a discussion partner when buying robot; poor level of knowledge (*)
- Interaction between robots (now and in the future)
- Behaviour of employee: intuitive operation in relation to behaviour taken over by robot
- Is the software amendment log reliable?

Control measures

Design and engineering

- Design aimed at service and function (******)
- Risk inventory
- Asimov's Robot Laws (**)
- Emergency stop functionality: no cut to power, but stops safely (safe mode) (*)
- Visually test software (*)
- Safe design of periphery
- Sharing best practices
- Involve users (employees) with design because of knowledge-based tasks and in order to gain acceptance and support (***)
- Use standardised or harmonised symbols in support of the instructions for working with robots
- Who is authorised, and competent in design, construction, maintenance, and dismantling?
- Ergonomic design (**)

Production, supply and installation

- Sharing best practices (**)
- RI&E
- Safeguarding quality during storage and transport
- Intrinsically safe working environment for installation, construction, and maintenance (*)
- Task location criteria: performance and people (attractive work)
- Training in safe use (***)
- Safeguarding safe behaviour, safety culture and knowledge of safety among the employees who have to configure and implement safety (*****)
- Protocol for safe installation (*)
- Communication with /between safety expert, customer, and supplier
- Standardise interfaces

Use

- Housekeeping (*)
- Ease of use, ease of programming and configuring (*)
- Best practices (**)
- Training by supplier and internal adherence (*)
- Feedback when safety rule breached, speak to others who have behaved incorrectly (*)
- Adjust irregularities
- Check to see whether safety system is still working properly (*)
- Periodic conformity assessment (*)
- RI&E and plan of action
- The safety of people is the top priority, then followed by self-preservation of the product or robot
- Training courses

- Recording and monitoring incidents

Maintenance

- Good communications between user and supplier (*)
- Maintenance is part of design
- Maintenance regimes
- Competencies, maintenance market (*)
- Job safety plan with customer (**)
- Communication in advance on maintenance safety measures (**)
- Scaffolding when working on robots at height
- PPE and maintenance measures
- Climbing harness and securing attachments
- Lock-in procedures
- LMRA
- People can always switch off a robot or overrule it (***)

Innovation

- Include in regulations: recycle old components in new installations (*)
- Merger of people and machine or robot: supporting in tasks, enhancement (**)
- Flexibility towards future developments (*****)
- Regime guidelines

Destruction/disassembly and disposal

- Separation of scarce metals and plastics: new work-related risk through toxicity of ‘waste’ (***)
  Software and configuration data; destroy safely (overwriting, or destruction of components) (*)
- Clear instructions from the supplier of what dangers there are when dismantling the robot (*****)
- Robot is universal all the way to the flange; after that, it is application-specific
- What is the environmental burden of the remaining components?
- Recycle? Combat misuse.