Princetonlaan 6
3584 CB Utrecht
P.O. Box 80015
3508 TA Utrecht
The Netherlands

www.tno.nl

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

TNO report

TNO 2016 R11143

Emergent risks to workplace safety as a result of IT connections of and between work equipment

Date	6 September 2016
Author(s)	Wouter Steijn; Johan van der Vorm; Eric Luiijf; Raphäel Gallis; Dolf van der Beek (contact person)
Copy no	
No. of copies	
Number of pages	40 (incl. appendices)
Number of appendices	0
Sponsor	
Project name	Emergent risks to workplace safety as a result of IT connections of work equipment
Project number	060.17532

Contents

1 Introduction

The ever-greater integration of new technologies in work equipment is regarded by some as the fourth industrial revolution[1] and referred to as 'smart industry'[2]. Examples that come to mind include automation through the use of embedded software, remotely controlling heavy materials, and the connecting of work equipment to local and public networks such as the internet (for some examples, see the text box on page 6). As well as the opportunities this entails for industry, new threats are also presenting themselves. This includes employees who have to move among robots or autonomous freight vehicles, but also malicious actors who can penetrate computers and computer networks and thereby disrupt processes or bring them to a standstill. The focus in this report lies on the connection between work equipment and cyberspace, including connections to local and public networks such as the internet.

Industrial Control Systems (ICS)[3] are increasingly deployed in crucial business processes[4]. ICS are also being connected more and more to internal business networks and directly or indirectly to public networks such as the internet. As a result, ICT and ICS have an ever-more important role in monitoring and controlling processes and work equipment in companies and organizations, and even in the living environment. This means that cyber security has a direct impact on workplace safety. The cyber security of these systems and networks has therefore become a prerequisite for workplace safety.

1. Recent newspaper headlines underline the risk: "*Nieuw lek onthuld: 13.656 bedrijven zijn 'eenvoudig' te hacken*" ["new leak revealed: 13,656 companies can be hacked 'easily'"] (2012) and "*Russen hacken westerse energiebedrijven*" ["Russians hack Western energy companies"] (2014). This shows that it is not just individuals and gangs who are involved, but also groups operating from or on behalf of a state.

2. In 2010, Royal Friesland Campina was the victim of a modified Conficker virus that disrupted their ICS resulting in loss of production of milk products that lasted nine hours. It is not clear how, if at all, this has put the quality of their products at risk.

3. In 2005, the ICS of a number of North Sea oil and gas platforms were affected by the Zotob.E worm. The only way to remove the work was by flying extra staff to the platforms. The level of risk to safety is not known.

[1] The first industrial revolution involved cast iron and the steam engine, the second steel, electricity, turbines, and the combustion engine, and the third, computers, communications, and globalization.
[2] See the initiative at www.smartindustry.nl
[3] ICS is defined here as the full range of industrial automation, including SCADA (and RTUs), EMS, IACS, DCS, PLC and their specific protocols and networks.
[4] Luiijf, H.A.M., & te Paske, B.J. (2015). *Cyber Security of Industrial Control Systems*: https://www.tno.nl/ics-security/; Luiijf, H.A.M. (2009). *Process Control Security in het Informatieknooppunt Cybercrime*, NICC.

4. In 2014, a cyber attack led to major physical damage to an iron-producing factory in Germany. The safety-related risk is evident. [5]

5. In Lodz, Poland, a teenager succeeded in causing two trams to collide by manipulating the track points, with several people injured as a result. [6]

However, cybercrime (where the damage can be expressed in terms of assets and information) is not the only risk of the fourth industrial revolution. The integration of ICT and work equipment creates both emergent risks (i.e., 'black swans'[7], or unknown risks[8]) and emerging risks (i.e., risks that are already known about that change in an unexpected way and with unexpected consequences). Some of these risk factors will also have a direct influence on the work-related health and safety of employees who use this equipment. Examples that come to mind are the increased use and complexity of embedded software, which could lead to new and unpredictable behaviour on the part of technology (with effects in the physical world), and the ability to influence ICS from outside a company through cyber attacks (malware or hacking) and therefore the risk of unauthorized operation of one or more machines.

A quick inventory carried out by TNO shows that this problem is very much a 'terra nova' in the international arena. The Dutch private sector, too, is not well prepared for these developments, although it is better placed than it used to be. This is why the Ministry of Social Affairs and Employment put the following knowledge question to TNO in 2015: *with regard to the field of workplace safety, where are the risks in the areas mentioned, and what measures (especially technical ones) could be used for controlling these risks?*

In the context of this knowledge question, TNO will concentrate primarily on the risks to workplace safety that result from the connecting of work equipment to (telecommunication) networks, including the internet. Cybersecurity is currently an important part of the societal discussion involving private citizens and both the private and public sectors. Nonetheless, the discussion is taking place mostly from the perspective of the cybersecurity of assets and information. The effect of failing cybersecurity of the ICS of high-risk business processes on workplace safety is still largely unexplored. The examples in the text box show that the internet and telecommunications in combination with ICS are applied by the industry in many different ways.

Below, TNO will set out the first stage of answering this knowledge question by making an inventory of hazards and threats and by eliminating or reducing risks as

[5] BSI (2014), Cyberattack on a German iron plant, Bonn, Germany. Online: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2014.pdf

[6] John Leyden (2008), "Polish teen derails tram after hacking train network: Turns city network into a Hornby set", The Register, UK. Online: www.theregister.co.uk/2008/01/11/tram_hack

[7] Taleb, N.N. (2007). *The Black Swan: The Impact of the Highly Improbable.* Random House

[8] To quote Donald Rumsfeld (2002): "There are known knowns. These are things we know that we know. There are known unknowns. That is to say, there are things that we know we don't know. But there are also unknown unknowns. There are things we don't know we don't know."

far as possible (inherently safe machinery design and construction) and mitigating the remaining risks. In doing so, we will focus specifically on the societal developments concerning the increasing connections between work equipment and the internet or telecommunications. The objective of this project is therefore summarized as follows, in this research question:

What control measures could be put forward in order to minimize the vulnerabilities to emerging and emergent workplace safety related risks caused by connecting work equipment through the internet or telecommunications?

With a view to the converging of security and work-safety aspects of work equipment and the systems of which they form part, the terms ‘threat and vulnerability’ will be introduced wherever necessary. This is to emphasize that we are also referring to the concept of deliberate threats and the consequences for the security and safety thereof.

In this report, we are presenting the method used for answering this knowledge question, as well as the resulting overview of vulnerabilities and control measures. In Chapter 2 we explain the methodology used – interviews and a workshop with experts from various fields. Chapter 3 presents the results of the interviews, and Chapter 4 presents the results from the workshop. Chapter 5 contains a brief discussion about the most important results, with an additional contribution from the experts at TNO. In Chapter 6, finally, we present the final inventory of vulnerabilities and control measures for businesses, in the form of a knowledge chart.

Box

The fourth industrial revolution is characterized by the integration of new technologies and work equipment. A number of examples are given below.

Connecting work equipment to the internet

Thanks to the internet, an increasing number of everyday devices are being connected to each other, such as computers, mobile phones, and televisions. An internet of things (IoT) is also being creating in industry, with installations and machines being linked up together. This is in order to enhance machine-to-machine communications in long and complex processes, but also to make it possible to operate devices remotely. An example that comes to mind here is the remote monitoring of off-shore wind farms. This increase in interconnectivity using public networks like the internet also entails new risks, however, such as cybercrime, cyber activism, and ultimately the threat of cyber conflicts, and the need on the part of industry to protect itself against this*.

Figure 1. Off-shore wind farm

Operating work equipment remotely

With increasing frequency, employees are able to operate work equipment remotely in situations where hazardous work is involved or at hazardous locations. At the same time, this brings new vulnerabilities regarding workplace safety. Wireless signals can fail or be disrupted, which can lead to a vehicle of machinery operating out of control. The employee may also find himself in the path of the vehicle in question or an area in which the machinery poses a danger. Moreover, it is not inconceivable that control over a particular item of work equipment is lost to a hacker, or that it is adversely affected by malware or an unauthorized individual who is 'playing' with the technology.

Figure 2. The remotely controllable steamroller, 'Fikkie'.

Embedded software in work equipment

Embedded software refers to the integration of software in a machine in order to enable it to perform more 'intelligently'. Examples in the car industry include the ABS that automatically supports the brakes, or climate control that regulates the temperature inside cars. Automation appears to be the key word. An important application of embedded software is allowing machines to carry out certain actions autonomously (that is, automatically) as cost-effectively as possible. Examples that come to mind are the self-driving transport vehicles that move containers around the APM terminal at Maasvlakte 2. This raises the question of what risks this entails to the employees who work there. There is also the risk of hackers being able to modify the script of a self-driving vehicle or of malware causing dangerous vehicle or crane movements.

Figure 3. Automated transport vehicle at the APM terminal, Maasvlakte 2

* This has already been examined, as apparent from the resolve of the Port of Rotterdam to fight cybercrime (http://www.distriparkbotlek.nl/?EventID=2).

2 Method

To be able to answer the research question, an inventory of the risks and vulnerabilities is needed, while possible control measures have to be identified. In the process, we are aiming at an integrated approach featuring both safety and security elements in relation to measures against unauthorized control of work equipment, especially by cybercriminals endangering industry (that is, criminals who use ICT as a means and as a target). In particular, we are focusing on minimizing the workplace safety risks and vulnerabilities that arise in relation to the use and maintenance of connections between work equipment and local networks as well as public networks such as the internet. Bearing this focus and the research question in mind, the following work plan has been drawn up:

1) On the basis of a brief internet and literature scan, a framework is to be developed in which the relevant risks, vulnerabilities and control measures can be described. This also serves as preparation for stage 2.
2) Interviews will be held with security and safety experts. An actor analysis of relevant parties for these interviews will be carried out on the basis of the framework determined in stage 1. This also serves as preparation for stage 3.
3) A workshop will be organized, at which the results from the interviews will be fed back to experts in the field, and these results will be further added to.

Given the convergence of the workplace safety and security (cyber and otherwise) aspects of machines and work equipment, a joint conceptual framework is needed. The starting point is that we regard the interplay of people and machines, danger and threat as a socio-technical system (see Figure 1).

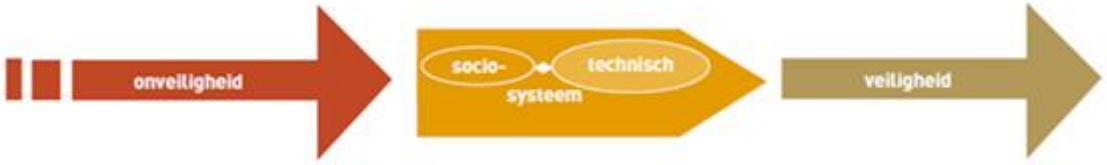

Figure 1. Safety as a socio-technical system.[9]

In order to describe the degree of safety, the concept of threat and vulnerability is needed, alongside the traditional concept of risk: the likelihood that a potential danger results in an actual incident and the seriousness of the injury or the damage that this leads to[10].

[9] Dutch Ministry of Housing, Spatial Planning, and the Environment (2008). *Handreiking Security Management*.
[10] Wikipedia: https://nl.wikipedia.org/wiki/Risico (23-12-2015)

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. Our definition of threat is in line with that of the Privacy Committee[11] as "*every unexpected or unanticipated occurrence that could cause damage to an organization*". It therefore covers deliberately and accidentally influencing business processes in such a way that damage or injury is caused. Unlike danger, the concept of threat also extends to the deliberate causing of damage or injury or both. In this connection, vulnerability can be defined as a weakness (inside an organization or other entity) that can be exploited by a threat[12].

The creation of this glossary was a dynamic process within 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, as an addition to the concept of work risks that are based mostly on accidental insecurity.

2.1 Literature and internet scan

First, we carried out a brief literature and internet scan. The purpose of this scan was twofold. First, we wanted to find a framework on the basis of which we would be able to approach the threats, vulnerabilities, and control measures, and put them into meaningful categories. Second, we wished to create an overview of relevant parties that could make a useful contribution for this project.

The scan revealed the industrial hygiene strategy and the life cycle of an item of work equipment as usable frameworks, for the purpose of categorizing the control measures in particular. Using these frameworks, we can make a structured hierarchical distinction in relation to which control measures should be preferred. This also allows us to show where in the life cycle the control measure should be applied, and by which party. Both frameworks are explained in greater detail below. We will then show how, on the basis of the life cycle, we arrived at an actor analysis in order to involve relevant parties with the interviews.

2.1.1 Industrial hygiene strategy

The industrial hygiene strategy[13] uses the following hierarchy of possible control measures, as described in the Working Conditions Act[14]:

- Source measures (such as the elimination and isolation of danger).
- Collective measures (such as protecting a group from danger).

[11] Lexicon of the Commission for the protection of privacy (CBPL): https://www.privacycommission.be/nl/lexicon#letter_d
[12] Hafkamp, W.H.M. (2008*). Als alle informatie telt: een onderzoek naar kwetsbaarheden- en incidentenresponse bij ICT-organisaties*. PhD dissertation, University of Amsterdam: http://dare.uva.nl/document/2/54173
[13] Working conditions portal: http://www.arboportaal.nl/onderwerpen/arbeidshygienische-strategie
[14] Working Conditions Act, online: http://wetten.overheid.nl/BWBR0010346

- Individual measures.
- Personal protection equipment.

According to the industrial hygiene strategy, this hierarchy must emphatically be adhered to when applying the control measures. That means that an organization must start with source measures, while the use of personal protection equipment is regarded only as the last solution. However, the industrial hygiene strategy encourages 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 this is paradoxical in the context of workplace safety, the exclusion of people is a source measure, from a security perspective.

The strengthening of workplace 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

Emerging risks are risks that are already known but which manifest themselves in unexpected ways and with unexpected consequences, while *emergent risks* are unknown unknown risks (that is, the black swans). Here, we will approach potential new risks from the perspective of the life cycle of the work equipment. This approach means that we consider work equipment applications from the point of view of a) design/engineering, b) production/supply/installation, c) use, d) maintenance, e) upgrade, all the way to f) disposal. There are similar phases in the entire cyber security life cycle: a) design and development, b) installation, system integration, entering into service, c) use, d) maintenance, e) update/upgrade, and f) disposal.

2.1.3 Actor analysis

In order to create an overview of threats and control measures for these life phases, experts in one or more of these life-cycle phases will be approached. Examples that come to mind are design companies, manufacturers, maintenance firms, and the industry itself as user. As supplement, we identified three additional parties that could influence each part of the life phase:

1) Knowledge developers, such as universities and other knowledge institutes.
2) Policy developers and regulators, such as inspectorates and certification bodies.
3) Service providers, such as insurance companies and telecom providers.

Table 1. Actor analysis based on the life cycle of work equipment

	Organization		Organization
Life cycle of work equipment		**Policy developers and regulators**	
Design	Triodor	Government	Ministry of Social Affairs and Employment/ policy department
	Total productivity		Inspectorate SZW
Production/supply/installation	Alewijnse		SODM
	Croon		DCMR
Use	APM terminal, Maasvlakte 2		HSE
	ENECO (off-shore wind farm)	Certification bodies	Lloyds
	FloraHolland Aalsmeer		Aboma
	Smart welding factory		TUV
	Scania		DNV
	VDL		
	BMP8500 (Fikkie)		
	Port of Rotterdam		
	Tata Steel		
Maintenance	Stork		
	Alewijnse		
	Kone Cranes		
	Cofely		
Innovation	-		
Disposal	-		
Knowledge developers		**Service providers**	
Universities	TU Delft Safety & Security Science section	Insurance companies	Van Lanschot
	Radboud University		Chabot
	TILT Tilburg University		Dutch Association of Insurers
Standards institute	NEN	Experts	NVVK
Knowledge institutes	Smart Industry	Advisors	Fox-IT
	Rathenau Institute		PSJ Advies
	CIO Platform Nederland		Tebodin
	TNO	Telecom providers	KPN

2.2 Interviews

Based on the above list (Table 1), 64 experts from different organizations have been approached to take part in an interview. Thirteen experts took part – see Table 2.

The interviews were held between 10 and 24 November 2015. The interviews lasted around 45 minutes each and were conducted by telephone by two TNO

employees, one of whom held the interview while the other took notes. The interviews were semi-structured. The following questions served as the basis for the conversations:

- Are you familiar with the subject? Which applications do you know about/ do you use?
  Possible examples include assembly line, automated machines themselves, or their operating systems.
- What is your opinion of the growing integration of work equipment with public networks such as the internet and the risks associated with this?
- What are the most important developments regarding this subject, in your field of work?
- What new and existing risks do you see to workplace safety as a result of the new technologies? Which do you regard as the most important?
  I would like to ask you to think in terms of a. threats and dangers, and then b. vulnerabilities.
- What control measures exist for limiting these risks?
- Who are the most important actors in companies and their suppliers who influence this?
- Do you believe there is a role for lawmakers? For regulators?
- What other major steps could be taken for the purpose of finding solutions?
- Do you have, or are you aware of, any reports – from conferences or elsewhere – in relation to this subject that you would like to share with us? The same goes for papers, articles, and presentations.
- Do you know anyone who could make a valuable contribution in the context of our research?
- This has been an initial exploratory interview. Would it be possible to contact you again at a later time in order to cover the subject in greater depth? We are considering giving each of the interviewees a preview of our report and asking your response to it.

Table 2. Participants in the interviews.

Interview	Organization	Type
1	Croon Elektrotechniek	Production/supply/installation
2	Cofely West Industrie	Maintenance
3	Tebodin	Advisors
4	TNO Industrie/www.smartindustrie.nl	Knowledge institute
5	TNO Industrie/www.smartindustrie.nl	Knowledge institute
6	Alewijnse Industrial Automation	Production/supply/installation
7	PSJ Advies	Advisors
8	Tilburg University	University
9	VDL Steelweld	Use
10	Total productivity	Design
11	Cyber Security Academy The Hague (CSA)	University
12	TNO Information Security	Knowledge institute
13	CIO Platform Nederland	Knowledge institute

2.3 Workshop

On 2 December 2015, a workshop entitled, '*Cyberspace connects safety and security: your challenge too! What is needed to tackle workplace safety of the future*?' was held. At the end of their interview the interviewees were invited to attend. Invitations were also sent to the same list of actors that were used in the interviews. This ultimately resulted in fifteen participants, including five project members and ten external participants, two of whom were interviewees.

Table 3. External participants at the workshop.

Organization	Type
Mercon	Production/supply/installation
Croon	Production/supply/installation
Researcher/Specialist Public Safety	University
TNO Information Services	Knowledge institute
EXIV	Design
NEN	Standards institute
Prorail	Use
TNO Information Security	Knowledge institute
Tebodin	Advisors
Ministry of Social Affairs and Employment	Government

The purpose of the workshop was to provide brief feedback from the interview results in order to be able to develop the list of risks, vulnerabilities, and control measures in more detail. To this end, the participants were split into two groups, who then brainstormed in two parallel sessions on either the risks and vulnerabilities, or the control measures for half an hour. Then the groups swapped subjects during a second half-hour session. During the sessions, the participants were able to share their ideas by writing them down on post-it notes.

3 Interview results

Below is a summary of the findings that emerged from the interviews. The results are basically divided into two subjects – vulnerabilities which allow threats to find ways to materialise, and the control measures. The results below are all paraphrased statements from the interviews. Any additions by TNO are explicitly shown as such, using footnotes.

3.1 Risk and vulnerabilities

The interviews involved discussions with actors from various disciplines on the new risks resulting from connections between work equipment through the internet or other forms of telecommunications, such as telemetry and radiographic control. Different examples were put forward, such as the Stuxnet'-attack in 2010 on an Iranian uranium enrichment plant, the use of crypto viruses, hackware, and jamming devices for disrupting systems or making them unusable. However, each example can be traced back to one clear theme: *The possibility that one or more individuals may gain unauthorized access to systems monitoring and controlling workplace equipment of companies and disrupting them to the extent that a situation could arise that poses a danger to workplace safety.*

Interviewees considered this risk primarily as a side-effect of the focus of companies on mainly the opportunities and convenience of new technological developments. It is all in keeping with the current 'zeitgeist' and the greater ease of using new communication and machine technology. For example, managers and employees like to be able to view processes from home or while they are travelling. Maintenance service providers, for example, wish to be able to carry out maintenance or to examine disruptions remotely in order to resolve them, thereby minimizing the 'time to fix'. A case in point is the example of automated cars. The discussion around self-driving cars is often centred around the technological opportunities and around limitations that still need to be resolved. Now, though, there are reports in the media that unauthorized parties are succeeding in gaining access to the cars' software[15].

In other words, it appears that the risk in terms of cyber security and in the context of the life cycle of products is often only considered retrospectively in safety discussions of this kind, rather than from the very start of the innovation or design process.

[15] Tweakers (21 June, 2015). '*Hackers kunnen op afstand remmen uitschakelen op Chrysler-auto's.'* http://tweakers.net/nieuws/104341/hackers-kunnen-op-afstand-remmen-uitschakelen-op-chrysler-autos.html

Table 4. Overview of the vulnerabilities that were mentioned in the interviews. It contains a brief summary of the most important elements to emerge from the interviews.

Vulnerability	Summary
3.1.1 Rapid technological developments	Technological developments mean that the software and security of work equipment quickly become outdated. Similarly, the complexity of system processes is also increasing.
3.1.2 The 'distance' between the IT department and other departments that are functionally responsible for work equipment (which, to an increasing degree, 'house' ICT)	The IT department is often a world away from other departments, including those in which ICS is used. As a result, no integrated risk management is carried out in which account is taken of each other's 'world'.
3.1.3 Costs of cyber security	The current competitive market ensures that small companies in particular are not keen to invest in cyber security, and instead focus on functionality. An underlying factor here is that there have so far only been a few major incidents (that are publicized, at least).
3.1.4 Little awareness of the impact threats could actually have on security/safety	The cyber situational awareness and knowledge about what hackers can and want is still relatively low in most organizations. An underlying factor here is a reluctance to report incidents (from which society could subsequently learn).
3.1.5 The unconsciously unskilled	Even when cyber security is properly organized from a technological point of view, it may be undermined by inappropriate actions by employees, as a result of which systems remain vulnerable. Present-day risk analyses often do not consider this risk and assume that employees act correctly.

The interviewees stated that on the one hand they understand why organizations use new technological means, but on the other found it shocking that the same organizations devote relatively little attention to inherent risks and that security and safety are not sufficiently evaluated from the system perspective. This is all the more so given that multiple factors and actors have been identified that could enhance the risk. Based on the interviews, we have identified five categories of the factors that could increase vulnerability to the risk of unauthorized access to ICS and ICT networks in the employment environment. Table 4 contains a summary of the results. Below, we discuss these categories in no particular order; it is clear that there are overlaps and interactions between the factors.

3.1.1 Rapid technological developments

A frequently heard cliché is that modern technological development is moving a breakneck speed. By contrast, certain items of work equipment are replaced in industry only very rarely. It seems that there is not always an awareness of how quickly security and ICT systems and ICS can age, which leads to exposure to new external threats. For example, there are cases of installations that still run on MS-DOS with dial-up modems, which could be unintentionally fatal to operational processes.

It appears that responsibility here lies with the administrator and user of the work equipment. Suppliers and system integrators state that they supply safe and up-to-date installations and software, but that it is then up to the client to keep their

systems up to date. An important underlying reason as to why installations are not always kept up to date in the way that they should is the complexity of updating critical process installations that have to operate 24/7[16] (see factor 3.1.2). Technological developments are also ensuring that the complexity of the system processes is increasing. It is stated that, as a result, nobody has any kind of overview of the system as a whole, and that situations are arising with ever-greater frequency in which processes are becoming a 'black box'. Responsibility for safety and security is also becoming fragmented. This raises the question of how we can help those who have to take decisions regarding this 'black box'. However, the ideas in this area are part of old paradigms, which are no longer applicable to the present day.
Nonetheless, technological developments are also creating new threats. In the case of a building, a reasonable estimate can be made of the external factors that could affect the physical state of the concrete, doors, and windows. These are reasonably constant factors – the chance that a type of concrete-eating precipitation will suddenly fall tomorrow is nil. In contrast, it is possible that new ICT functions (attacks) will be developed causing existing security functions to no longer be sufficient.

3.1.2 The 'distance' between the ICT department and other departments that are responsible for work equipment (which, to an increasing degree, 'house' ICT)

Reference is regularly made to the distance between the ICT department and the shop floor on one side, and top-level management on the other. The latter sees cyber security purely as a technical problem of which they have no understanding, while the ICT engineer is committed primarily to keep the processes running. This can lead to sub-optimization and an unfounded trust that the system is running properly, with safety and security responsibilities implicitly being shifted from each party to the other.
However, the processes are not integrated and there is little knowledge of each other's domain, such as between the ICT and shop floor domains, or between the safety and security domains. The ICT domain in businesses and organizations, for example, generally attaches much value to cyber security, partly due to the pressures of audits and visible risks. There is perhaps some security awareness in businesses and organizations of the need to protect access to ICS and ICS networks from the outside. However, things are more tricky in practice. In relation to maintenance and remote operations (employees who work from home, for example, or third party maintenance) gaps then quickly appear in the security of networks and ICS. Risk management is not yet completely integrated in the organization.

3.1.3 The cost price of cybersecurity

An important aspect that featured repeatedly in the interviews was the fact that cyber security costs a lot of time and money. For smaller companies especially, this can be a relatively heavy cost burden. Cyber security is often better organized in larger companies. The interviewees made repeated reference to market competition, as a result of which suppliers and installers may price themselves out of the market if they focus too much on cyber security and if they wish to add costly security functionality without there being any specific security requirements by the industry. The parties stated that there is often little demand among clients for cyber

[16] Luiijf, E., & te Paske, B.J. (2015). *Cyber Security of Industrial Control Systems*: https://www.tno.nl/ics-security/

security, and certainly not in combination with work-related safety. Businesses and organizations are not yet willing to pay much for this.
Instead, the set of requirements from businesses and organizations are aimed generally at operational functionality, cost containment, and time to market. They primarily want something that works effectively and efficiently; cyber security functions like firewalls will then automatically become less important because the installation will work without them. Cyber security therefore ranks below the efficiency of a system or installation, and is more likely to be the subject of savings. An important underlying factor here is that there are still too few publicized cases of things going wrong, as a result of which there is no urgency among companies to invest in cyber security. Several interviewees stated that it is really a question of waiting for something to go seriously wrong (and which is reported extensively in the press) before companies actually will invest in cyber security.

3.1.4 Little awareness of the possible impact of a security/safety threat

It emerged from the interviews that cyber situational awareness in organizations is generally only limited. There is a lack of knowledge, and people have no real grasp of what is actually possible. An example is the understanding that access to the networks for employees from outside is a potential channel for access for unauthorized parties. If the ICS of critical business processes are insufficiently protected, it is possible, in theory, that incorrect instructions could be uploaded – deliberately or accidentally – that disrupt the controlled processes. There are no security strategies that are based on this possibility. The interviewees also stated that little is known about the motives of hackers – so not just what they are able to do, but also what they want. It is said, for example, that the 'hacker community' includes young people who do things 'because they can'.[17] They experiment to see how far they can get. This group is interested mostly in seeing whether they can bring something to a standstill or set something off, but without any underlying malicious motives.

The fact that there is little exchange of incident information about the threat and vulnerability of embedded software and communication networks is described as an underlying cause of this low level of cyber security awareness. There is often a reluctance among organizations to report incidents (because of their reputation). This is absolutely the case with things that go wrong by accident (see 3.1.5.). Consequently, little is known about what happens, on what scale, and with what impact.

3.1.5 The unconsciously unskilled

It often emerged from the interviews that cyber security has to start with the people who work with the systems. As well as cybercrime or worse (such as terrorism), there is also a lack of skills to contend with. Many of the interviewees referred to the so-called unconsciously unskilled who do 'stupid' things. Among the examples given were that of an employee who one moment was playing an internet game on his laptop, and who the next dialled up a major client on the same laptop in order to resolve a process disruption; an operator who, in order to recharge his mobile, connected it to a company computer via a USB; and an employee who used a USB stick to bypass the air gap of a closed system. Each of these acts, which are often regarded as harmless in practice, has the potential to give malware access to safety critical systems and work equipment. Employees are not aware of what the impact

[17] Examples include script kiddies and recreational hackers (white and black).

of their behaviour is or lack the personal discipline to keep their private lives separate from their work; nor do they realize that they should not open private emails at their place of work[18]. There can also be a dilemma – in terms of the relationship with clients – between security and user friendliness. For example, by not admitting much-used semi-safe software, such as Dropbox, to servers, you may improve the cyber security posture, but the client will not be so happy and be inclined to look for other shortcuts that could end up undermining cyber security anyway.

There is also a lack of awareness among managers, including security managers, of the possible consequences of unconsciously unskilled or malicious employees or service or contractor personnel. When carrying out HAZOPs, it is often assumed that all is well, and that people in the scenario act with the right intentions ('safety first'). No further risk analysis is carried out on these conditions. However, a system is only as safe as the safety awareness and conduct of the people who use it. It is therefore not just about the ICT technology and ICS but also about the method of working (process design), the organization, and the human factors (awareness, acting properly).

[18] This calls to mind the case of a ship on the North Sea that came to a standstill because a Trojan Horse found its way to the ship's propulsion system from a private e-mail inbox (source: private discussion).

Table 5. Overview of the control measures that were mentioned in the interviews, sub-divided according to sector and theme.

Sector	Themes	Generic control measures
General	3.2.1.1 Awareness raising	- Raising awareness of the risks associated with using networks. - Improve communication and the exchange of knowledge between ICT (cyber security) and departments with functional responsibility. - Convincing management of the possible impact of risks. - Description of processes, with a view to possible breaches (both logical and physical). - Rewarding good behaviour. - Looking at other sectors for examples?
	3.2.1.2 Demarcation of the problem	- Classifying sector-specific risks. - Formulating risks in terms of business continuity.
Public	3.2.2.1 Legislation	- Obligation to report breaches of cyber security (such as data leaks) to a government body [19] - Act in a way that facilitates processes, rather than governs them.
	3.2.2.2 Certification	- Make security aspects during design compulsory. - Expand existing standards with the human factor. - Formulate existing standards in language that is easy to understand.
	3.2.2.3 Frameworks of standards	- Framework of standards concerning the setting up of secure business operations. - Approach it as a process and not as a one-off solution.
Private	3.2.3.1 Mutual sharing of information about incidents	- Drawing up benchmarks for mutual comparison. - Institutionalizing the exchange of information on incidents.
	3.2.3.2 Maintenance and management	- Placing the emphasis on the need for preventive maintenance. - Making explicit who is responsible for maintenance and management.
	3.2.3.3 Education and training courses	- Raise cyber situational awareness and knowledge as early as primary school - Make refresher courses available to people already working in the field. - Having the public sector take responsibility for providing the courses and training. [20]

[19] The obligation to report serious breaches of cyber security, which took effect on 1 January 2016, could accelerate this process as soon as board rooms realize the risks of the potentially very high penalties.

[20] A starting point could be the follow-up action resulting from the *'Advies aan de Stassen van V&J en OC&W inzake cybersecurity in het onderwijs en het bedrijfsleven*', drawn up by the National Cyber Security Centre (2 November 2015).

3.2 Control measures

In this section, we give an overview of the various control measures that emerged from the interviews. The control measures are grouped into eight themes which are themselves sub-divided into measures that are generally applicable, and measures that are more appropriate to either the public sector or to the private sector. Table 5 shows the control measures and their underlying structure.

3.2.1 General themes

3.2.1.1 Awareness raising

All the interviewees agreed that some important steps still need to be taken in raising awareness of the risks associated with directly or indirectly connecting work equipment with each other through the internet or other forms of telecommunication. The example of tunnel safety is given by way of comparison. As well as legislating, governments at both Dutch and European level have devoted, and continue to do so, a great deal of attention to the importance of describing tunnel safety and thereby raising the topic profile.

However, one interviewee did warn that awareness raising is often used as a showstopper: whenever management meets to discuss cyber security and other security issues, they conclude quickly that employees have to be made aware, as if this is all that is required. The question is also whether everything can be achieved through education and training and whether employees can be expected to understand all the complexities of the problems in this area. The aim should actually be to internalize the problems and to move from unconsciously unskilled to consciously skilled. However, this is a long process and it is important to keep an eye on who should be aware of what and on who is responsible for what. Raising awareness starts with responsible management and should then develop primarily among the people who work with the systems and the ICS and who acquire machinery functionalities with embedded software.

Executive employees could be victims if things go wrong. However, they also form part of the problem (see section 3.1.5). Cyber security is more than just a technical process – how employees think is also a factor. The first thing that awareness raising should achieve is to ensure that no more ‘stupid’ acts are carried out and that no malware is installed or back doors opened for hackers as a result of carelessness. There has to be the understanding that working with embedded software and networks entails new risk factors, in the same way that we know that we are taking a risk whenever we get into a car, which is why we wear our safety belts and heed traffic warning signs. This understanding has not fully permeated people’s consciousness when it comes to cyber security, as a result of which employees may click on a malware or phishing link at work, just as they might at home, when their guard is down.

ICT and security departments were also mentioned as parties that should be more aware of the problems. Major decisions are often taken during periods of crisis management, for example, but it is questionable as to whether they are able to oversee the entire process. It is also important here that the parties are brought together (see section 3.1.2).

Progress in relation to cyber security awareness, in combination with safety, is also needed among the managers of organizations, the ultimate owners of the problem. The interviewees stated that businesses are generally aware of their cyber security risks but that they rarely do much about them structurally. This involves manufacturing companies, contractors, and service suppliers alike. Many cyber security issues are not included in risk analyses, for example. Ideally businesses and organizations should take not just failures of ICT systems into account, but also the possibility that someone may maliciously seek to disrupt processes. It is important here to show conclusively what is possible – if 'we' can take over a platform, then so can others. If the upper echelons are convinced of cyber-related risks in relation to their ICS and embedded software that their company or organization is facing, action will be taken. It is noticeable that these organizations have started to take part in international working groups in the field of cyber security and that they now employ specialist security managers. Moreover, organizations must have a well-organized chain of command (that is, who should be made aware of any incident that takes place) and update charts of relevant software and installations. This should be managed from the board rooms.

Currently, though, there is a tendency to say, "*nothing will happen here".* However, if you wait until something happens, the costs in financial and image terms, and the loss of time, will be larger than if you start to consider risks in a structured and integrated manner now.
The best approach is to make a description of the process, and then to look at the possible physical and logical breaches that could occur in each section (for example, someone operating a crane remotely could be physically overpowered by someone wishing to take over the crane for malicious purposes).
The process of raising awareness in organizations is derived mostly from the public sector, but organizations can play a part in this too. It would be helpful if organizations were to reward clients whose systems were in order, but this is currently only a marginal phenomenon. The interviewees named drinking water companies and nuclear energy firms as examples of where high levels of cyber security awareness can be found.

3.2.1.2 Demarcation of the problem

It was repeatedly clear from the interviews that cyber security should not be regarded as a generic problem. Instead, cyber security and its associated risks should be defined and approached from a domain- or sector-specific angle. In the case of the Ministry of Defence, for example, cyber security is about cyber operations and cyber terrorism, while for an oil company it concerns the risk of industrial espionage or the sabotaging of oil tanks. For banks, meanwhile, it involves fraud, for hospitals the privacy of patients, and for the police, the security of information. This is all related to cyber security, but also concerns other completely different problem areas. The interviewees stated that an accurate domain-specific classification is needed in order to be able to properly assess the potential damage that hackers could perpetrate and to be able to respond appropriately.
The context of such a situation could be a determining factor in how risks should be framed. The analogy of a navy vessel in a port or a war situation is given by way of illustration. In a port, a protocol is needed to prevent the automated firing of missiles, but as soon as the vessel is at sea in a war situation, automated firing with

manual override is the protocol. The more difficult it is to describe the context of cyber security, the more difficult it is to prescribe the relevant norms and legislation.

With specific reference to the industry sector, the interviewees agreed that the risks concerning cyber security should be framed on the basis of business continuity. In other words, risks should be set out in relevant business terms, such as '*how much money do you lose if ICT fails?'* This concerns the business losses rather than the loss of ICT itself – the failure of ICT is simply the cause. In itself, cyber security does not produce anything, so there needs to be clarity about the losses that could arise, and the nature of the assurance it provides. This way, cyber risks can be translated into business problems that board rooms are likely to take notice of. It is also important that the Chief Information Officer (CIO) is able to articulate the problems in these terms.

3.2.2 Public sector

3.2.2.1 Legislation

Legislation is regarded as the natural domain of the government. Laws can be used as a means of steering behaviour in a particular direction. For example, a legislative proposal to make it compulsory to report cyber security breaches could help us better understand what takes place in practice (see 3.2.2.3)[21]. France is cited as an example of what happens where legislation makes certain cyber security measures compulsory, with penalties for non-compliance.

It should be pointed out that it is important that the government should not prescribe every detail – instead, it should act as a facilitator of the process. One of the interviewees said that the government should set down requirements with which a system must comply, but that it should not determine every exact aspect. Otherwise, there is a danger that companies and organizations will be more preoccupied with compliance instead of risk management. In other words, adhering to the rules (in order to avoid being penalized, for example) may then be regarded as more important than actually eliminating risks. Another interviewee made an analogy with traffic: the government provides good-quality infrastructure and the rules of the road, but it is ultimately up to citizens themselves to qualify as drivers and to stick to the rules. That works, and a similar situation is what is needed for the internet.

It was also noted that developments are moving so fast that legislation is having trouble keeping up. The use of other policy instruments is therefore needed.

3.2.2.2 Certification

Many of the interviewees stated that cyber security should be included in the manufacturing process at a much earlier stage, such as during the design phase. The public sector – the government, for example, or certification bodies or trade associations – could give a lead through certification and standards and by setting requirements that systems should meet. An example could be the setting up of a quality mark with different levels based on security in relation to vulnerability and impact of the risk, or by making it compulsory in the case of work equipment to make certain non-essential activities impossible (for instance by removing or blocking USB ports if they are not needed for operational processes).

[21] Similar legislation took effect on 1 January 2016.

Several specific proposals for adding to existing standards were offered during the interviews, such as introducing the human factor in IEC 62443 (formerly ISA 99)[22]. This concerns the use of safe IACS (Industrial Automation and Control Systems). People are often the weakest link in the system but this aspect is not yet taking into account in the standard develomentss. Account needs to be taken of different national cultures, however, and the training required to work with systems of this kind should also be firmly incorporated. ISO 55000[23] was also mentioned as a starting point for expanding on cyber security issues.
The interviewees stated that they adhere to the prescribed standards. However, there were doubts as to the degree to which certification could help. If a client does not manage installations or software correctly, e.g., by connecting an insecure laptop, then cyber security can no longer be guaranteed. In addition, care should be taken not to rely solely on being compliant. A company may be fully compliant with all the rules and certification requirements, but that does not necessarily mean it has eliminated every risk. Could the time spent being fully compliant not be better used on actual risk management?

3.2.2.3 Frameworks of standards

One of the interviewees mentioned a third aspect that could be managed by the public sector – frameworks of standards. An important feature of a framework of standards is that it involves a dynamic process. The idea should not be to think in terms of introducing a one-off concrete solution to a problem; instead, the framework of standards should be continually modified and adapted in order to keep up with societal and technological developments.
The banking sector is given as an example of how a framework of standards should develop. The banks have become aware that, in addition to the market and credit risks that they face, there are also operational risks – that is, that if process errors are made, there are consequences. A framework of standards is said to have been created over the space of fifteen years that entails a ‘thou shalt limit thy operational risks’ approach to which banks adhere.
It is important that a framework of standards is set up that is specific to the context of a particular sector. See section 3.2.1.2.

[22] http://isa99.isa.org/ISA99%20Wiki/Home.aspx
[23] http://www.iso55000.nl/

3.2.3 Private sector

3.2.3.1 Sharing information

The interviewees stated that we are actually still in the process of mapping out the problem of cyber security; we do not yet know how large the iceberg is, as there is no obligation to report cyber incidents. Cyber security is often organized on a need-to-know basis, while incidents are frequently not shared because of privacy considerations and possible reputational damage. However, cyber situational awareness would improve if information about incidents were to be shared. Companies could rank themselves based on best practices, with the aim of challenging each other. It is only when it is known what can go wrong, or what has gone wrong in the past, that lessons can be learned from it.

The interviewees stated that there is a role here for industry (branch) and employee organizations. They could help draw up 'proof of practice' and benchmarks that companies could comply with, and that they could use to compare each other's performance. Information Sharing and Analysis Centres (ISACs) were also mentioned as relevant parties for the critical infrastructure sectors. There are twelve such sectors in the Netherlands.[24] ISACs are a form of institutionalizing the exchange of cyber security-related information. If this leads to a better understanding that everyone is faced with the same problems, this will lower the reluctance to share cyber security-related information. The Dutch National Cyber Security Centre (NCSC) coordinates these ISACs, but could push for cross-sector collaboration, for example by allowing ISACs to come together at national level. The resulting threat landscapes would then be of greater value than the current insights of the individual ISACs.

3.2.3.2 Training courses

The interviewees acknowledged the fact that the current generation of operators and employees require new skills. Operators are often no longer managers of work equipment, but rather supervisors, remotely in many cases, of automated processes. There was therefore frequent reference to the importance of training and courses. This should ideally start in primary schools, with awareness of new technologies and how they work, but it will take years before the effect is visible at the shop floor.

Additional training is therefore also important in order to enable current employees (such as those aged forty and above) to work with the new tools. 'Field labs' should also be set up for people in this group in which they could learn in an industrial setting, with the help of tutors and individual supervisors, and to create new curricula. At present, nobody is taking any responsibility for this. According to the interviewees, the Dutch Ministry of Education, Culture and Science is focusing primarily on those entering the labour market for the first time.

3.2.3.3 Maintenance and management of software and hardware

Mention was made in the interviews that the well-known doctrine, 'if it ain't broke, don't fix it', does not hold true for cyber security. Constant updates are needed in order to keep security at the best-possible level. In other words, a greater emphasis on preventive maintenance is required. It emerged from the interviews that responsibility for this rests with the end users. It is currently the case that suppliers

[24] https://www.ncsc.nl/samenwerking/publiek-private-samenwerking/isacs.html

and system integrators should supply products that meet all cyber security requirements, but it is then the responsibility of the end users to make sure they stay that way (see section 3.1.1).

4 Workshop results

During the workshop, the participants were able to write ideas on Post-It notes and attach them to particular locations on a large sheet of paper. In two parallel sessions, they identified threats and vulnerabilities, as well as identified possible control measures based on the product life cycle (section 2.1.2). They also drew up a list of actors for whom security and safety awareness raising and the provision of information about these topics is important, and how the provisioning of such information can be supported. Figure 2 gives an example of the resulting overview. The results below are a direct representation of the Post-Its as they were created during the sessions.

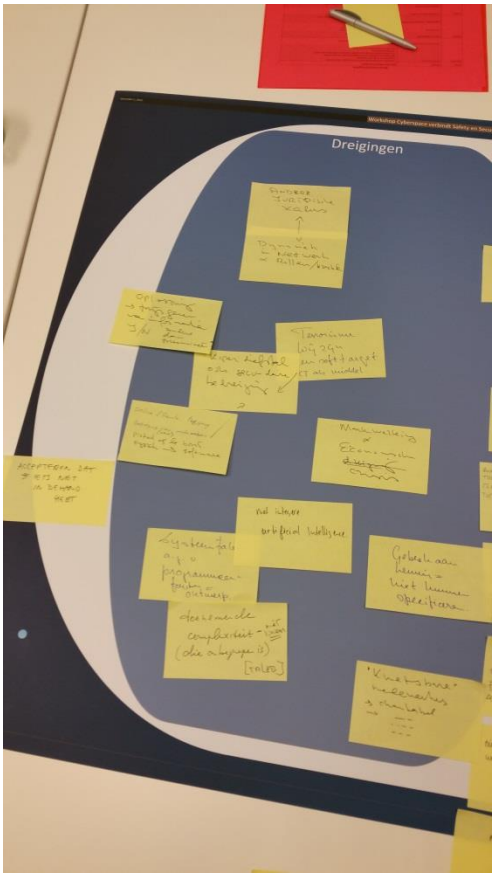

Figure 2. Example of how the results from the workshops were displayed.

4.1 Risks, threats, and vulnerabilities

Accept that you do not have something completely under control.

4.1.1 Threats

- Different legal framework applies
- Dynamics in network and in the roles/strength
- Terrorism

    - We (industry) are a soft target for terrorists who wish to make a physical impact or sow fear using ICT.
- For example – copper theft, a secondary threat (safety is affected, control is lost)
- Online/remote access is a threat to employees.
    - Knife to the throat
    - Local physical access versus remote access using software
- Market forces and economic crisis
- Fragmented artificial intelligence
- System failure as a result of programming error / design
- Increasing complexity (non-linear), which is not understood (Taleb[25])
  Vulnerable employees
    - Susceptible to blackmail, for example.

4.1.2 Vulnerabilities

- Communication
    - Managers and engineers do not speak the same language
- Partly as a result of this, there is a lack of a sense of urgency in board rooms /among management
- Partly as a result of this: no funds available for good security (low urgency)
- Security of ICS and SCADA is not included in new functionality recruitment process
- Organizational structure (mini-kingdoms, lack of integrated approach)
- Risk management not integrated in the business (compulsory)
    - No business value
- World usually viewed from multiple paradigms
    - Conflict
- Paradigm shift needed (diagram)
    - Out of the box thinking
    - Letting go of old paradigms
- Lack of integrated approach (people, processes, physical security, IT security)
- From separate boxes (design, development, manufacture, etc.)
    - to one integrated responsible team (or separated but closely connected to common aim/knowledge)
- System integrity (knowledge of whole system)
- Renewable components. New risks to the same component because of a new but different context (response to fire safety of aircraft versus fire safety of train; should be tested according to how they are used (engine switched off or not))
- Awareness raising versus responsibility
    - Responsibility leads to decisions and action
    - Awareness raising must take place at the top levels of companies, politics, and hospitals.
    - Awareness raising through risk management / BCM / etc.

[25] Taleb is the author of books such as ‘Black Swans’ and ‘Anti-Fragile’, in which he advocates a greater focus on outliers, in other words, beyond 10-6 in the Gauss curve. He also advocates (like Snowden, with his Cynefyn model) a greater focus on the fact that systems are not linear.

- Insufficient knowledge/skills among risk management officers in order to be able to make clear their added value to the business.
- Security and risk are flawed terms for non-experts.
    - Unclear terminology
- Lack of knowledge. Unconsciously unskilled regarding content, processes, systems and organizations. Should ensure reaching unconsciously skilled.
- Learn to learn about known, known unknown and unknown unknown
- Not one safe situation but several; is determined by the context (based on content, processes, systems, and organizations)
- Carry out impact analysis to see what is important
- Backdoor via 'tele networks' gives a risk of unauthorized manipulation or changes to the system.
- Non-resilient managing.
    - Instead of static risk management – the ability to anticipate and to adapt
    - Learn the weakness of threats
- Accessible for drone (Wi-Fi)
- Attaching plasters instead of devising fundamental solutions
- The non-user-friendly design; invites bad (that is, unsafe) behaviour.
- Non-redundant implementation of systems.
- Lack of lines of defences for cyber risks (no layer of protection analysis, LOPA)
- Many different users
- Fast-changing environment
- Same information stored at different locations.
    - Redundant (for example, access information)
- Naivety among users of connected work equipment or systems
- Knowledge on need-to-know basis. The wheel has to be repeatedly invented, without your knowing it.
- Fail to limit losses.
- Human factors
    - Remember access procedures / keys
- Not complying with joint basic conditions, but facing the same direction.
- Finding solutions based on outdated traditional paradigms for risk management.

4.2 Control measures

- Knowledge development about the shape and impact of combinations of new technologies/risks
- We do not understand it, ICT moves forward so quickly. What is the social responsibility?
- "If it goes wrong, I will get to hear about it" (director)

In the case of an order

- Where are the phase of demand definition and the formulation of the order?
- Corporate Security Concept/ Corporate Security architecture

- Guidelines / terms of reference with orders. Scope of order (including cyber security)
- Architecture development as a whole
- Classification of risk level
- Risk? Authorization? Responsibility! Guarantee!

Put in feedback loops between the various life cycle stages

4.2.1 Design and engineering

- Cyber security rules of conduct
- Screening of designers (knowledge/skills, malicious?)
- Cyber security design specifications in the order, including detection and forensic.
- Record of design phase (units and interaction)
- Usability
- Structuring the development process (including responsibility and authorization duties). Disclosure of milestones and proplanning
- Design: Manufacturer must make an inventory of the risks and ensure that they are eliminated as much as possible. Manufacturer must state how any remaining risks are to be managed.
- Risk inventory
    - Access analysis (internet)
    - Network (every level)
    - Risk inventory
    - Hardware (removing wire)
    - Software
    - Physically protect (Faraday cage)
    - White list (software/processes).

- Equip PLC with anti-virus/malware security
- Design: intrinsically safe
    - No opportunities for connecting to the outside world. So no connections to the internet. No opportunities for access via information carriers.
    - To integrated risk management that connects the S, such as SafetySec HAZOP?
- Design: Must take account of the life cycle of product and components and raw materials.
- Apply more system engineering.
- Introduce new risk scenarios
    - Cross-domain learning
    - Analogies: car-machine system
- Involve ICT specialists with risk sessions (safety cases, TRAs, RI&Es)

4.2.2 Production, supply and installation

- Entry control (specifications)
- Distribute TVBs
- MoC
- Record of ‘completion phase’

- Sound programme environment, without back doors
- Cyber security test phase
- Structure project (TVBs, milestones, planning and disclosure)
- Whatever cannot be organized at work equipment level. This requires application of technical or organizational measures in the usage phase.
- Places a heavy strain on behaviour and culture
    - Behaviour of individuals
    - Culture of company or parts of it
- Allow friendly hackers to carry out a stress test aimed at machine safety.
- Total clarity about who is responsible.
    - Manager
    - Service supplier (maintenance service)
- Test protocols, regression tests.
- Correct learning schedule
- Use correct clearance
- Check redundant execution of systems that check each other.
- Expand production guidelines and installation manuals with new risks
    - Page 1: security settings (EMC standards to the back)
    - Secure out-of-the-box
- Also have MoC look at cyber risks.
- How work equipment is to be installed safely is to be explained by the manufacturer. What to do next in the case of joint construction. Introduces new risks. Role for manufacturer here too.
- System integrators
    - Making complex systems from ‘safe’ (or otherwise) components.
- Include traditional security with a view to machine safety.

4.2.3 Use

- Good logging / audit trail
- User certified and screened
- No connections with outside world (stand-alone)
- TVBs
- Planning (updates/physical/software)
- Periodically testing
- MoC
- Keep register up to date
- Back up
- Detection and forensic
- Temporary password generator
- Cyber security rules of conduct
- Monitoring / inspection
- Prevent employees from installing software themselves (such as games) on ICS or other internal systems.
- Role-based access and separation of functions
- Integrated G&S management
    - …[26]

[26] Illegible

    - Multidisciplinary incident management.
    - Integrated crisis management.
- Use in accordance with the manufacturer's specifications.
- Procedures relating to access control and key procedures.
- Regulated transfer/training between installer and user.
    - Safety steps
    - Installer visits user

- Access control and passwords
- Training /additional training for skilled persons
- Disconnecting work equipment from external networks like the internet.
- Screening of internal employees (background checks)
- Invite a group of hackers to attack your system (or at least to identify the security leaks).
- Protocol for the use of USB sticks, external hard disk, and the Cloud.
- Limit plugging in opportunities
- Carefully monitor visitors and temporary users such as those on work placements.
- Introduce barriers against /links between connected physical systems in order to prevent a cascade effect elsewhere in the system.
- Inform employees and third parties about possible cyber security risks

4.2.4 Maintenance

- Work equipment goes to safe mode in the event of a disruption
- Need to know! Maintenance and users → consciously safe
- Destruction of data and passwords
- Local maintenance, not remote
- Certified employees
- Good logging / audit trail
- Actively involve direct users
- Structure SLAs (service providers) on the basis of cyber security risks
- Make agreements on results based on desired/non-desired effects.
    - Relevance of management based on performance and execution
- Maintenance roles logically separated from user roles
- Screening personnel from installation firms that carry out software updates on process control systems or work equipment
- Maintenance (patching) on small (manageable) scale (pilots)
- Adhere to at least the security level specified by the manufacturer.
- Carry out updates safely, do not introduce any new risks
- Have your system tested periodically for security leaks, during maintenance checks.
- Automate back-up systems
- Keep HRM employee registration system up to date. Be aware of former employees who could have access to systems.

4.2.5 Innovation

- Learning/ feedback loops at every stage
    - Improvement cycle

- "See design and production/delivery"
- References and verification
- Regularly on contract basis
- Locally modernized
- No remote system
- Repairs also? Repairing is replacing defective components with components of equal value.
- Adapt to the latest scientific, technological, and technical position.

4.2.6 Disassembly and disposal

- Use certified parties
- By specialist firms
- Check that material is not dumped in developing countries
- Disassemble in a manner that is demonstrably safe
- Destroy information carriers prior to disposal
    - Including information in embedded systems, components, and network components
- Put old computers and data beyond use.

4.2.7 Final thoughts

- Where is the end of the system? I.e. scope of the governance
- Time horizon: shifting interests
    - Can you tackle this with a framework?
- Look at overall management system
    - Monitoring by manufacturer as an example and online adaptation of safety parameters
    - Information security problems regarding components is much more extensive than components in machine guideline

4.3 Actors

Is governance important or not?

4.3.1 Public sector

- European platforms
- ISSA[27]/ ?/ Bilbao (EU agency for health and workplace safety/ Focal Points
- NCSC (National Cyber Security Centre)
- Rathenau Institute
- Social and Economic Council of the Netherlands (SER)
- Confederation of Netherlands Industry and Employers
- WRN

4.3.2 Private industry

- Universities (for example, Tilburg Institute for Law, Technology, and Society; TU Delft; Eindhoven University of Technology; University of Twente)

[27] http://issa.int

- Pieter van Gelder network
- WIB
    - Process control
    - High end
- ISACs (Information Sharing and Analysis Centre)
    - that is, a new actor is appearing in the field of industry
- FME
- NEN / standards committees (CIEs)
- COB (knowledge centre for underground construction and lack of space underground)
- VLR (Dutch association for lift and escalator technology)
- Medical sector (IC technology system integration)
- Cyber Security Academy (CSA)
- Training courses
    - Professional training courses
- Vital infrastructure (see the Ministry of Economic Affairs)
- DEVOPS teams (development and operation teams)
- VNCI (Association of the Dutch Chemical Industry)
- SmartIndustry.nl agenda
- Wide range of production companies
- Manufacturer / approval / certification / use / monitoring
- Trade association
    - NVVK (Dutch association for safety expertise)
    - SEC
- KPMG / accountant/ risk management (Annual Accounts Act places requirement on the signature in relation to the security of ICT resources; unfortunately ICS ‘not my problem’ (and tailor-made)’)
- DITCM
    - Round-table meetings (including mobility)
- Organization of management / inspection services
- Branch of software developers
- Conference circuit (but not just about process safety)
- Systems of water authorities (see RAAK project HHS, TNO, Unie van Waterschappen, NCSC)

5 Discussion

In reflecting on the results achieved by the workshop participants, the interviewees, and TNO experts, the following additions have been noted, based on the results from the interviews and the workshop.

5.1 Integral risk management

5.1.1 Risk management

Basically, cyber security is linked to security management and the risk evaluation is carried out not just in terms of financial impact but also the effect on image of an organization. Also, strict compliance is no guarantee that total security has been achieved.

It has been emphasized regularly that ICT and security departments should be more aware of the workplace safety related problems. For example, during a crisis management situation often major decisions are taken, but it is questionable as to whether the decision-takers are able to oversee the entire process. Therefore, it is important that the parties and stakeholders are brought together.

Security management should extend across the entire system life cycle. The aim should actually be to internalize the problems, involving all the actors in the product life cycle, and to move from unconsciously unskilled to consciously skilled.

In the context of risk management, an examination could be made of which standard methods and techniques could be expanded to cover cyber security. Even integrated analysis methods could be developed. One possibility is the explicit inclusion in HAZOPS of the role of software and the role of people. The aim here does not necessarily have to be to remove people 'by design', but to actually strengthen their role in robustly coping with threats and disruptions.

5.1.2 Education

Education is one way of making experts and other specialists who are involved with workplace safety and cyber security aware. Experts in other relevant workforces should also enhance their knowledge and insights through additional training or by following courses. ICS is often hidden in networked functionality and the process owner is not aware of the cyber risk. [28] He or she is not educated in that field and does not recognize the challenges.

The need for additional training holds true for various types of organization: maintenance/service, production, supplier. Sectors can initiate awareness in companies and in their networks as well as their supply chains.

5.1.3 Technology

An important area for attention is the becoming accustomed to familiar life cycles; for example, replacing your computer or laptop every three years, your landline phone every fifteen years (perhaps for the last time), and lifts every thirty years. In the case of machines with a long life cycle, new replacement modules with ICT functionality can be embedded during maintenance or the resolution of problems. In

[28] Luiijf, E., & te Paske, B.J. (2015). *Cyber Security of Industrial Control Systems*: https://www.tno.nl/ics-security/

the process, however, it is possible to overlook the fact that safe basic settings have to be adjusted, that no transfer of ownership takes place, or that consultations should be held with the ICT department! An example that comes to mind is the consequence of a data subscription for a mobile device that, say, a lift uses to communicate with the outside world. A department that is traditionally linked to mechanical engineering may bring in or modernize existing functionalities (such as work equipment) without realizing that the modernization is ICT-based. The company's own ICT department does not know this has taken place. In many cases, installations are carried out by an external company that makes sure that everything works. The cyber security aspect of the installation often falls outside the scope of the operation, meaning that no cyber security instructions are provided, for example, and that organization procedures are not applied accordingly.
For buying new equipment, too, it is important to take cyber security into account when making acquisitions. This aspect is often perceived – erroneously – as extra baggage.
All in all, therefore, it is not just about the ICT but also about the method of working and the structure of the organization. It starts with the design specifications, but also involves being alert to 'function creep', for example. Over a period of many years, a system can grow and become more complex without anyone realizing that things are getting critical as far as cyber security is concerned. This is the case not just with individual items of work equipment, but also with system integrators that supply an insecure product or functionality. Product and process alike must be delivered in a cyber secure way.

5.2 Complexity

The increasing linking of systems in networks is making the cyber security problems even more complicated. We simply do not know how certain software interacts with other software. Think of a building automation system, for example. Another example is that of cars, where more than fifty PLCs from different manufacturers work together with the risk of an electronic handbrake that engages itself while the car is on the motorway. Engineering is no longer capable of resolving all of this. The reverse also requires attention: namely, the lack of stable connectivity. If it a certain communication platform (such as the internet or 4G) is disrupted, but not by malice or the work equipment itself, this could mean that something goes wrong with the way in which that equipment works. This could endanger safety, even though no conscious actor is behind it.

5.3 Learning organization

It is clear from the interviews that knowledge of sources where information can be found, is limited. Sources like ICS-CERT in the United States, the SCADASEC mailing list, the SCADA/ICS fact sheets from the Dutch National Cyber Security Centre[29], the trend analyses in the annual *Cyber Security Beeld Nederland* (CSBN),

[29] https://www.ncsc.nl/actueel/dossiers/ics-scada.html

and sector-based Information Sharing and Analysis Centres (ISACS)[30] could be given greater prominence.
Much research in other fields, into the motives of hackers for example, can also be used for assessing cyber security risks to workplace safety.
Cross-field learning yields important information. Currently, though, there is a tendency to say, "*nothing will happen here".* However, if you wait until something happens, the costs in financial and image terms, and the loss of time, will be greater than if you start to consider risks in a structured and integral manner now. An attitude of this kind also ensures that incidents are swept under the carpet and only come to light when something serious happens. In the safety-related world, this means risks to life and limb.
You can learn from other mistakes, such as the disruption at Vodafone or T-Mobile where a fire in one device knocked out the network across the whole country. Because there was no agreement with other providers to use their networks, the damage in terms of financial cost, time, and image was considerable.

5.4 Culture and behaviour

Finally, as well as the structure and learning approach, there is also the culture approach, which is covered here. It will be necessary to highlight the desired organizational culture partly through a combination of cyber security and workplace safety. It is how this is expressed in terms of behaviour that provides evidence of a safe and secure culture.
The increasing linking of work equipment to the internet entails new types of behaviour, which itself can lead, consciously and unconsciously, to risks:

- The 'bring your own device' policy in the business environment is leading to new vulnerabilities.
- Phishing and other forms of attack using the private and work channels have been identified. [31]
- The greater connectivity also gives disgruntled employees new ways of causing significant damage, although the phenomenon itself is nothing new.

[30] See www.ncsc.nl and elsewhere
[31] See Luiijf, H.A.M., & te Paske, B.J. (2015). Cyber Security of Industrial Control Systems: https://www.tno.nl/ics-security/ for an overview.

6 Synthesis and recommendations

It became clear during this project that, although this is an important subject, it has not been looked at in a structured manner yet, neither in the Netherlands nor internationally. In that respect, this report is the first of its kind. Now, of all times, there is an important window of opportunity. The Internet of things (IoT) movement is gaining momentum, a development that still can be influenced. It emerged from many of the interviews that we are frontrunners. Little is done so far and little thought is being given to this subject. Below is our synthesis of the information we have gathered on this project, together with our recommendations for organizations. It cannot be denied that the introduction of new ICT and the connections between work equipment through the internet or telecommunications has enabled industry to make great strides in terms of efficiency. Nonetheless, it was obvious from the interviews and the workshop that these developments also entail many new threats and vulnerabilities. We propose the following as a general definition: *the possibility that one or more individuals may gain unauthorized access to systems monitoring and controlling workplace equipment of companies and disrupting them to the extent that a situation could arise that poses a danger to workplace safety.* This definition is all-encompassing – it can refer to access for malicious hackers or malware, as well as unintended acts on the part of a maintenance engineer.

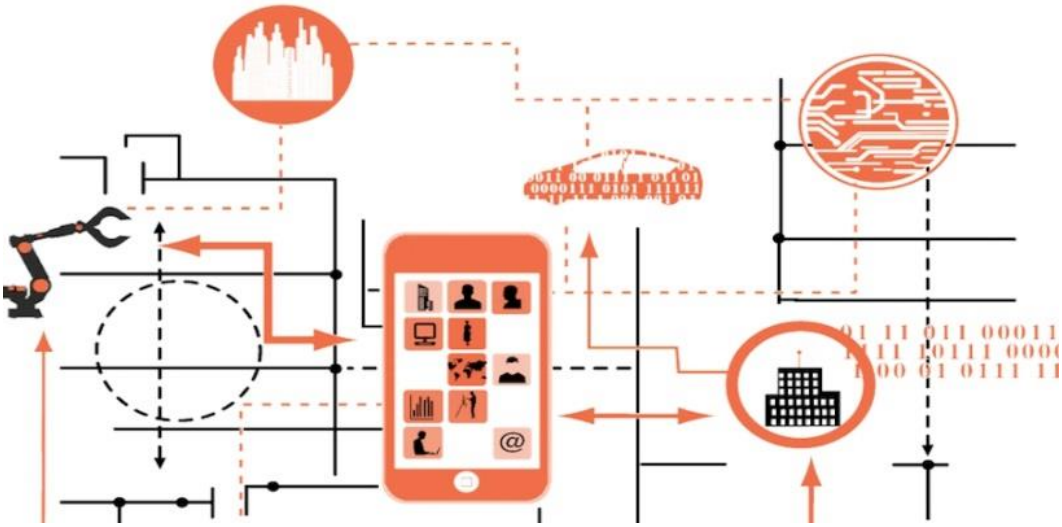

Figure 3.The Internet of Things is creating complex connectivity between systems and processes.[32]

An important underlying factor that strengthens this risk is the ever-greater complexity resulting from the IoT - that is, that everything is connected to everything else via networks (Figure 1). The scale on which this happens is not always appreciated, because the underlying ICS are not always visible. It is presented in terms of functions and possibilities, without any direct realization that this also

[32] Bloem, van Doorn, Duivestein, van Manen, van Ommeren (2013). Things: Internet of Business Opportunities. *VINT research report 1 of 4. http://www.fr.sogeti.com/globalassets/global/downloads/reports/vint-research-1-things-internet-of-business-opportunities.pdf*

creates back door for external parties (hackers)[33]. System processes can suddenly be approached on a scale. Below, we present the most significant risks, vulnerabilities, and control measures that have emerged from the project, the most important actors and sources of information for businesses seeking to work on prevention, and several concrete steps for tackling the risk from a company perspective. This information is summarized in Appendix A in the form of a knowledge chart.

6.1 Risks

- Disruptions to processes threaten the business continuity and the quality of the production.
- Employees injured or killed as a result of an unsafe work situation caused by an unintended cyber disruption or hacking, malware, or signal interruption, and the concomitant financial damage (absenteeism and sickness costs, for example).
- Access can be gained to processes and machines via blackmail (such as physical threats to employees or the creation of an access path through 'phishing').
- Harm to image resulting from incidents visible to the public (such as in cases where there are victims).

6.2 Vulnerabilities

Table 6. Overview of vulnerabilities, with explanatory notes.

Vulnerabilities	Explanation
Communication	Managers and engineers do not speak the same language. This means that any shared insights and communications, to the extent that they exist, between ICT security and operational employees or safety experts regarding cyber risks in relation to workplace safety, are often limited.
Costs of cyber security	The current competitive market means that SMEs in particular invest very little in cyber security in relation to workplace safety, focusing instead on functionality (so they prefer, for example, to have a crane that transports a container from A to B, with cyber security being of secondary importance). The same thing applies to manufacturers and system integrators. An underlying factor is that there have been very few incidents (known to the public) that have had affected the safety of employees or any other people, which could have increased the urgency of investing in cyber security.
Rapid developments	Rapid technological developments mean that software and cyber security in relation to workplace safety quickly become outdated. Moreover, the complexity of ICT controlled and operated processes (24/7) is increasing.

[33] http://link.springer.com/chapter/10.1007%2F978-3-319-24255-2_2

Vulnerabilities	Explanation
Outdated risk management[34]	Despite the ever-greater connectivity of systems and processes, risk factors are still too often viewed from different angles (maintenance versus implementation, safety versus security, staff versus management, etc.). However, this is an outdated paradigm. Integral risk management is needed. There is frequently also a lack of awareness and an overview of the interrelationship of the technical systems, as well as of the actors who play a part in providing solutions when threats occur.
Lack of cyber-situational awareness	Cyber situational awareness is still relatively low in most organizations. There is also a reluctance to share incidents with others, from which everyone could learn. A law entered into force on 1 January 2016 that compels businesses to report any data leaks.
The unconsciously unskilled	Unconsciously unskilled employees who unknowingly affect machine software and who thereby destroy control measures that have been implemented. Present-day risk analyses often do not consider this factor and assume that employees act correctly.

Control measures that have so far never been considered, and the understanding of which appears to be only very limited[35].
The complexity of the increasing connectivity of systems, processes, and the internet for example, also makes it more difficult for employees who have to work with them to retain any kind of overall view. Resulting unconsciously unskilled acts can create various unsafe situations. Examples include opening back doors for hackers via malware, or directly, by unintentionally disrupting a system in cases where not every consequence of a particular action is obvious across the whole network.

Tasks are set out for every actor in the life cycle. From the point of view of prevention, manufacturers have an important role, as far as the safe application of work equipment is concerned. It is important to give consideration to the threats and vulnerabilities described in this report as early as the design stage, as well as during the production and installation stages. Where this cannot be achieved in the technology of the work equipment in question, it is important that the owner, operator, and user of the equipment are informed about its vulnerabilities and how they can be managed. This includes ‘what if’ scenarios and how they can be managed, similar to traditional emergency situations:

- Fail safe/safe fail
- Damage tolerant
- Anticipating and fast response to suspicions of threats.

This should be factored in as early as the design stage, wherever possible.

[34] The same conclusion applies in other fields too: "Gap 7: Lack of advanced risk assessment tools Risk assessment methodologies that can deal with multiple networked stakeholders working in collaboration need to be developed. This requires a different mind-set for existing risk management approaches, which often begin by scoping a system (i.e. defining its borders) prior to a risk assessment based on the individual elements. However, in interconnected systems this clear border does not exist. To address this gap we need to redesign risk management systems/approaches so that they operate from a stakeholder perspective rather than border perspective."
https://www.enisa.europa.eu/activities/Resilience-and-CIIP/smart-infrastructures/intelligent-public-transport/good-practices-recommendations

[35] A relatively harmless example, which is nonetheless telling for the scale at which systems are linked to the internet, is that of barbecues that can be hacked:
http://news.softpedia.com/news/barbeques-are-now-hackable-thanks-to-ever-evolving-technology-497418.shtml

6.3

Table 7. Measures for minimizing the risk.

Life cycle	Control measure
Design	✓ Intrinsically safe design (based on technical standards). ✓ Integral safety risk inventory and evaluation throughout the life cycle of the work equipment. ✓ Designs aimed at fail safe/safe fail and damage control when exposed to cybercrime.
Production, delivery, and installation	✓ Suppliers and service providers (e.g., of maintenance services) supply secure out-of-the-box products. ✓ System integrators and installers supply Industrial Control Systems (ICS) which are integrally safe. ✓ Cyber security is an integral part of the acquisition process and the test phase of products and services. ✓ Include the security of information and other systems or components in the contract with suppliers.
Use	✓ Integral and multidisciplinary risk management. ✓ Aim safety management and safety culture partly on cyber security. ✓ Add cyber security aspects to workplace safety rules of conduct and protocols that cover dealing with ICS and other internal systems. ✓ Cyber security procedures for keeping ICS and networks safe. ✓ Hardening ICS and minimizing interfaces. ✓ Informing employees (including temporary employees), suppliers, and contractors about risks and required levels of conduct. ✓ Additional training for employees on how to deal with ICS. ✓ Monitoring of ICT network anomalies (through auditing for example). ✓ Develop policy for internally and externally sharing cyber security related information. ✓ Carry out periodic penetration tests in relation to the cyber security of work equipment (by white hackers, for example). ✓ Add cyber security aspects to workplace safety rules of conduct and protocols that cover dealing with ICS and other internal systems. ✓ Screening of own employees. ✓ Integral approach to incident management (safety and security). ✓ Structure the company's emergency response organization so that it is able to anticipate and respond quickly to cybercrime threats.
Maintenance	✓ Structure maintenance activities on the basis of managing integral safety. ✓ Malware detection policy and its implementation – make sure that malware is detected quickly. ✓ Identifying attempts to breach systems during maintenance. ✓ Patch policy and its implementation – patch in good time (for example, carry out updates on a manageable scale). ✓ Monitoring access and work activities of employees and of third parties during maintenance work. ✓ Testing and preventing new security leaks as a result of the installation of new components.
Innovation	✓ Organize a management of change process based on integral security. ✓ Ensure solutions in the future: encourage research and development for the benefit of innovation to the current status of science and technology in the field of cyber security. ✓ Testing and preventing new security leaks as a result of introducing new functionalities to work equipment or new work equipment itself.
Disposal	✓ Removal of sensitive information and engaging reliable parties. ✓ Putting outdated installations and systems, or those that are no longer suitable, out of use.

6.4 Key players in knowledge sharing and awareness raising

- The parties involved with cyber security and safety in the life cycle of work equipment
- Knowledge institutes and knowledge points (such as ncsc.nl)
- Insurance companies
- Trade associations (sharing information, developing knowledge, developing guidelines)

- Government bodies and standards institutes (national and international legislation, frameworks of standards)

6.5 Recommendations for businesses and organizations

- Ensure that integral safety and cyber security are coordinated at board room level, in one portfolio, to be held, for example, by a Chief Information Officer or the CEO.
- Ensure that there is a multidisciplinary team that makes an integral evaluation of the cyber security related risk to workplace safety, with specific inclusion of the human factors, observes incidents, and which is able to take emergency measures if necessary.
- Analyse where in the here and now network connections between work equipment and 'risky' internal environments and outside worlds exist.
- Make sure that knowledge is shared, good practices are exchanged, and warn each other about incidents and threats.[36]
- Anticipate changes to work equipment and to connections between work equipment and ICS and public and other networks through integral security analyses and product requirements.
- Include safety and cyber security in designs, system integration, and supply, and when putting out orders such as for the carrying out of maintenance. In doing so, take consideration of how things are interrelated (such as system architecture and relevant actors).
- Make sure that all parties possess the necessary awareness of the importance of integral actions in relation to workplace safety and cyber security. If necessary, give people extra training (management, other employees, those carrying out the work).[37]

[36] Since 1 January 2016, there has been an obligation to report data leaks. For more information, see http://www.cip-overheid.nl/wp-content/uploads/2015/11/20151130_Meldplicht_v2_0_def01.11.pdf and elsewhere.

[37] There is another TNO report that contains more information about outdated skills. The report is here: https://www.tno.nl/media/1305/kwalificatieveroudering_in_nederland_tno_r13017.pdf