UNIVERSITY OF CAMBRIDGE

OK Computer?

The safety and security dimensions of Industry 4.0

A report prepared by Policy Links (Institute for Manufacturing, University of Cambridge) for the Global Manufacturing & Industrialisation Summit (GMIS) and Lloyd's Register Foundation (LRF)

Lloyd's Register Foundation

GMIS Global Manufacturing & Industrialisation Summit

Authors

David Leal-Ayala
Jennifer Castañeda-Navarrete
Carlos López-Gómez

Contributors

Kieron Swift
Ella Whellams

This report was commissioned by the Global Manufacturing & Industrialisation Summit (GMIS) and Lloyd's Register Foundation (LRF). It has been produced without formal GMIS or LRF editing and the views expressed here do not imply the expression of any opinion on the part of GMIS or LRF. Mention of firm names or commercial products does not constitute an endorsement by the authors, GMIS or LRF.

GMIS | Global Manufacturing & Industrialisation Summit

The Global Manufacturing and Industrialisation Summit (GMIS) was established in 2015 as an industry association to build bridges between manufacturers, governments & NGOs, technologists, and investors in harnessing the Fourth Industrial Revolution's transformation of manufacturing to the regeneration of the global economy. A joint initiative by the United Arab Emirates and the United Nations Industrial Development Organization (UNIDO), GMIS is a platform that presents the manufacturing sector with an opportunity to contribute towards global good, working to the benefit of all.

LR Lloyd's Register Foundation

The Lloyd's Register Foundation is a UK charity established in 2012. With our mission to protect the safety of life and property, and to advance transport and engineering education and research, the Foundation has an important role to play in meeting the challenges of today and the future. Our vision is to be known worldwide as a leading supporter of engineering-related research, training and education that makes a real difference in improving the safety of the critical infrastructure on which modern society relies. In support of this, we promote scientific excellence and act as a catalyst working with others to achieve maximum impact.

Key messages

Manufacturing is changing. Industry 4.0 is leading to a sharp increase in the number of machines, components, sensors, actuators and products connected among themselves and to the Internet. New forms of work organisation are arising that involve a sharp rise in software content; an exponential increase in the connectedness of machines, processes and firms; and new forms of work organisation involving more intensive interactions among humans and machines.

However, knowledge gaps around the safety and security dimensions of Industry 4.0 are prevalent among manufacturers. In order to realise the full benefits deriving from Industry 4.0, manufacturers will need to more proactively understand and address new safety and security implications arising from the adoption of 4IR technologies. Yet published work addressing the safety and security dimensions of Industry 4.0 remains scarce in spite of its importance.

New safety risks are emerging.[1] Safety risks include: new sources of physical risks and hazards; long-term health risks from exposure to new hazardous substances; and psychosocial risks from new sources of work-related stress. In order to address these, new requirements for ensuring safe manufacturing operations include: design for safety methodologies; development of new standards and certifications; risk assessment and management methodologies; and new skills for risk prevention.

Similarly, Industry 4.0 is exposing manufacturers to new security risks. Security risks include: loss of data; intellectual property theft; business interruptions; fraud; reputational damage; cyber extortion; physical asset damage; and others. In order to address these risks, new requirements for ensuring secure manufacturing operations include: solutions to address the technical vulnerabilities of legacy systems; the sharing of cyber security best practices; new regulatory frameworks and standards; risk transfer mechanisms; and addressing new skills and training needs.

A range of international responses are emerging across key enabling action areas. These aim to tackle emerging safety and security risks and facilitate compliance with new requirements for the adoption of 4IR technologies. They include initiatives that are focused on: new frameworks, regulations and standards development; awareness-raising and information-sharing; skills development; anticipation of 4IR risks; 4IR safety and security research and development; and funding of co-innovation efforts. While a number of efforts are already in place, open themes remain that could form the basis of an agenda for future actions between industry, academia and policy-makers.

An integrated approach to safety and security is required for the successful deployment of 4IR technologies. Separate expert communities have traditionally addressed safety and security. Safety has focused on redundancy as a method to prevent harm, but with little attention to data and system integrity (i.e. accuracy/completeness of data and correct operation of services). Security efforts have

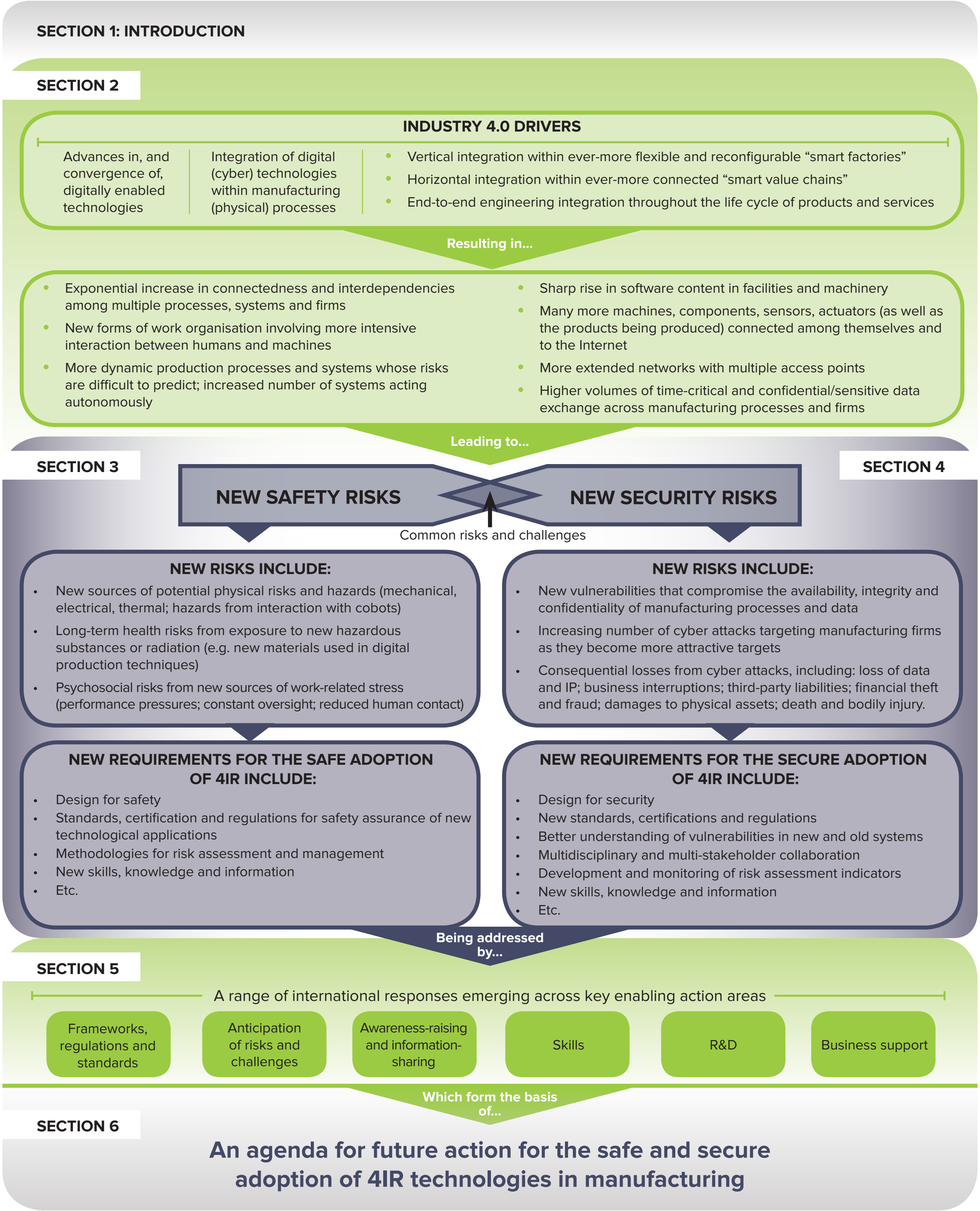
[1] In the context of 4IR safety and security, “risks” are defined as situations involving exposure to danger, while “requirements” refer to necessary conditions that need to be met to guarantee safety and security.

primarily focused on threats to confidentiality and virtual harm such as data breaches, but little attention has been paid to asset damage and physical harm. A new paradigm must emerge whereby safety and security systems do not allow unsafe operations, but safety systems can guarantee their integrity and not be abused into a method of bypassing security or causing greater harm than they should prevent.

Areas of future work that could be the basis of pilot projects (to bridge the safety and security knowledge gaps in 4IR deployment) include:

- Building a unified global knowledge database on 4IR safety and security (through publicly accessible online platforms).
- Developing a unified vision of future safety and security risks and requirements (e.g. through foresight and scenario-planning).
- Creating interest groups (for the mapping, sharing and adoption of best practices).
- Creating industrial safety and security guidelines to inform the development of standards (through collaboration with standards bodies).
- Developing a 4IR-ready workforce (integrating safety and security skill requirements).

Figure 1 - The safety and security dimensions of Industry 4.0 – key themes and structure of the report



SECTION 1: INTRODUCTION

SECTION 2

INDUSTRY 4.0 DRIVERS

Advances in, and convergence of, digitally enabled technologies

Integration of digital (cyber) technologies within manufacturing (physical) processes

- Vertical integration within ever-more flexible and reconfigurable "smart factories"
- Horizontal integration within ever-more connected "smart value chains"
- End-to-end engineering integration throughout the life cycle of products and services

Resulting in...

- Exponential increase in connectedness and interdependencies among multiple processes, systems and firms
- New forms of work organisation involving more intensive interaction between humans and machines
- More dynamic production processes and systems whose risks are difficult to predict; increased number of systems acting autonomously
- Sharp rise in software content in facilities and machinery
- Many more machines, components, sensors, actuators (as well as the products being produced) connected among themselves and to the Internet
- More extended networks with multiple access points
- Higher volumes of time-critical and confidential/sensitive data exchange across manufacturing processes and firms

Leading to...

SECTION 3

NEW SAFETY RISKS

SECTION 4

NEW SECURITY RISKS

Common risks and challenges

NEW RISKS INCLUDE:

- New sources of potential physical risks and hazards (mechanical, electrical, thermal; hazards from interaction with cobots)
- Long-term health risks from exposure to new hazardous substances or radiation (e.g. new materials used in digital production techniques)
- Psychosocial risks from new sources of work-related stress (performance pressures; constant oversight; reduced human contact)

NEW RISKS INCLUDE:

- New vulnerabilities that compromise the availability, integrity and confidentiality of manufacturing processes and data
- Increasing number of cyber attacks targeting manufacturing firms as they become more attractive targets
- Consequential losses from cyber attacks, including: loss of data and IP; business interruptions; third-party liabilities; financial theft and fraud; damages to physical assets; death and bodily injury.

NEW REQUIREMENTS FOR THE SAFE ADOPTION OF 4IR INCLUDE:

- Design for safety
- Standards, certification and regulations for safety assurance of new technological applications
- Methodologies for risk assessment and management
- New skills, knowledge and information
- Etc.

NEW REQUIREMENTS FOR THE SECURE ADOPTION OF 4IR INCLUDE:

- Design for security
- New standards, certifications and regulations
- Better understanding of vulnerabilities in new and old systems
- Multidisciplinary and multi-stakeholder collaboration
- Development and monitoring of risk assessment indicators
- New skills, knowledge and information
- Etc.

Being addressed by...

SECTION 5

A range of international responses emerging across key enabling action areas

Frameworks, regulations and standards

Anticipation of risks and challenges

Awareness-raising and information-sharing

Skills

R&D

Business support

Which form the basis of...

SECTION 6

An agenda for future action for the safe and secure adoption of 4IR technologies in manufacturing

Contents

1. Introduction

Manufacturing is changing. The emergence of the Fourth Industrial Revolution (4IR), or “Industry 4.0”, is radically changing the ways in which firms manufacture products, the business models they adopt and even how they innovate. In order to realise the full benefits deriving from Industry 4.0, manufacturers will need to more proactively understand and address new safety and security risks and requirements arising from the adoption of 4IR technologies.

Many industry stakeholders are willing to undertake the organisational and operational transformation necessary to adopt 4IR technologies in manufacturing. In order to do so, they will need to be able to assess the risks entailed in the application of these technologies, from business, environmental and social perspectives – including the impact on future workforce safety and operational security.

Although a large number of academic, industrial and policy documents have been published in recent years on the topic of Industry 4.0, the focus has generally been on the technological aspects. Published work addressing the safety and security implications of Industry 4.0 remains scarce in spite of its importance.

Against this backdrop, the Global Manufacturing and Industrialisation Summit (GMIS), on behalf of the Lloyd’s Register Foundation (LRF), has commissioned Policy Links, IfM Education and Consultancy Services (IfM ECS), of the University of Cambridge, to explore the safety and security implications of 4IR technologies based on a review of the latest international evidence.

This review constitutes the first stage within an open, multi-stakeholder project by GMIS and LRF that aims to bridge the safety and security knowledge gaps in the deployment of 4IR technologies in manufacturing. The end goal is to promote better knowledge of the safety and security risks and requirements deriving from 4IR in order to design concrete implementation plans for industry stakeholders to adopt 4IR technologies confidently through pilot studies.

> This review constitutes the first stage within an open, multi-stakeholder project by GMIS that aims to bridge the safety and security knowledge gaps in the deployment of Fourth Industrial Revolution (4IR) technologies in manufacturing.

The objectives of this report are to:

a. Summarise the emerging safety and security risks and requirements for manufacturing, in the context of 4IR, based on a review of the international evidence;

b. Offer insights into strategies and practical steps adopted by national governments and industry stakeholders to address emerging risks and requirements;

c. Indicate priority areas for future work suggested across the literature.

As described in Figure 1, the structure of this report is as follows:

- **Section 2** reviews some of the key drivers behind Industry 4.0 and its practical implications for safety and security within manufacturing;
- **Section 3** focuses on the safety risks arising from Industry 4.0 and the new requirements that these confer on manufacturers and policy-makers;
- **Section 4** focuses on the security risks arising from Industry 4.0 and the new requirements that these confer on manufacturers and policy-makers;
- **Section 5** discusses priority action areas identified internationally, providing examples of specific initiatives identified in selected countries that aim to tackle emerging risks and facilitate compliance with new requirements;
- **Section 6** proposes an agenda for future action to enable the safe and secure adoption of 4IR technologies in manufacturing.

This report is published in conjunction with two supporting briefing papers that provide deeper insights into key aspects of 4IR safety and security:

- **"Safety assurance of autonomy to support the Fourth Industrial Revolution"**, by Richard Hawkins and John McDermid from the Assuring Autonomy International Programme at the University of York.
- **"Managing cyber risk in the Fourth Industrial Revolution"**, by Jennifer Copic and Éireann Leverett from the Cambridge Centre for Risk Studies at the University of Cambridge.

2. Industry 4.0 drivers and the safety and security implications

With the advent of Industry 4.0, a number of additional safety and security requirements are set to arise. It will only be possible to fully implement Industry 4.0 and get people to accept it if the full scale and nature of these requirements are properly understood and appropriately addressed. In this section we conceptualise the safety and security dimensions of Industry 4.0 based on a review of the relevant literature.

2.1 What is Industry 4.0?

Industry 4.0 refers to an anticipated Fourth Industrial Revolution (4IR), whereby a number of digitally enabled technologies come together to more effectively connect, integrate and optimise production processes, factories and entire value chains. Made popular by Germany's "New High-Tech Strategy", a strategic initiative of the federal government, the term Industry 4.0 is now widely used by government, academia and industry around the world.

Internationally, variations exist in terminology and emphases related to Industry 4.0, reflecting differences in stakeholder perspectives and industrial contexts. A range of related terms used in different countries include: "digital manufacturing", "smart manufacturing", "industrial Internet", "smart factories", "cloud manufacturing" and "cyber-physical production systems". These terms do not necessarily have a one-to-one correspondence and they are not necessarily defined or used consistently.

A common aspect across Industry 4.0 definitions is the use of a number of digital technologies (see Table 1), data and applications to deliver improvements in manufacturing-related operations (including the broader value chain of manufacturing activities), and to enhance the performance of manufactured products and related services in both established and emerging sectors.

Potential improvements enabled by Industry 4.0 include, among others:

- Greater product personalisation (the production of small series and customised products) through more automated and reconfigurable production systems;
- Greater productivity through increased process connectivity and automation;
- Improved energy and resource efficiency through better process monitoring and control;
- Shorter product-development lead times through to stronger links between design and production;
- Production localisation through, for example, distributed 3D printing facilities.

In order to achieve these benefits, however, industry stakeholders will need to better understand the new safety and security risks and requirements emerging from the adoption of 4IR technologies in manufacturing.

2.2 4IR technologies

Table 1 introduces some of the key technologies commonly described under the umbrella of Industry 4.0, including: cyber-physical systems (CPS); the Internet of Things (IoT); cloud computing; big data; machine learning; artificial intelligence (AI); and advanced production technologies such as 3D printing.

The impacts of each of these technologies are expected to be important in their own right, but it is their convergence and integration with manufacturing technologies that makes them so disruptive (Figure 2).

Table 1 - Key technologies underpinning Industry 4.0

Cyber-physical systems (CPS)	• Systems formed of electronic hardware (including sensors and actuators) and software (including computer interfaces and control algorithms) designed to sense and interact with the physical world (including human users). • By providing a rich variety of real-time data from production processes, cyber-physical systems can be used to improve the adaptability, flexibility and customisation of manufacturing operations.
Internet of Things (IoT)	• The Internet of Things refers to networks of physical objects (devices, vehicles, buildings, equipment, etc.) connected to the Internet. • In the IoT, cyber-physical systems generate and capture data from the physical world and transmit it through the network infrastructure for it to be analysed and employed by distinct applications.
Big data	• The large-scale deployment of cyber-physical systems, together with improvements in industrial networking, have led to the exponential growth of data volume and traffic. • These large data sets, whose size means that it is beyond the capability of typical database software tools to capture, store and analyse them, are commonly known as "big data".
Artificial intelligence (AI)	• Artificial intelligence refers to the use of data to take decisions or perform certain tasks that are normally considered to require human knowledge, intelligence, learning and understanding. • Such tasks include: visual perception, speech recognition and decision-making.
Machine learning (ML)	• Machine learning is considered to be an enabler of artificial intelligence. In its most basic form, machine learning refers to the use of algorithms to analyse data, learn from it and then make decisions about specific tasks. • Rather than writing a specific set of software code to instruct a machine to do a particular job, machine-learning algorithms give it the ability to learn how to perform a task by training the system using large amounts of data or big data.
Advanced production technologies, including 3D printing	• Advances on digitally enabled production technologies are driving changes, not only in terms of how goods are produced but also in the way that manufacturing value chains are organised. • 3D printing, or additive manufacturing (AM), has received significant attention worldwide. 3D printing encompasses multiple techniques used to build solid parts by adding material in layers. This stands in contrast to typical manufacturing processes in which material is removed or formed. While 3D printing has been in use since the mid-1980s, recent advances in accuracy and repeatability are broadening its application areas.
Other	• Other technologies typically described under the umbrella of Industry 4.0 include advanced robotics and automation technologies; hybrid production systems (which combine various technologies within one production process); virtual reality (VR); and augmented reality (AR).

Adapted from: UNIDO and Policy Links (2017). Emerging trends in global advanced manufacturing: challenges, opportunities and policy responses. Report for the United Nations Industrial Development Organisation, Vienna.

2.3 Convergence of digital (cyber) and manufacturing (physical) systems

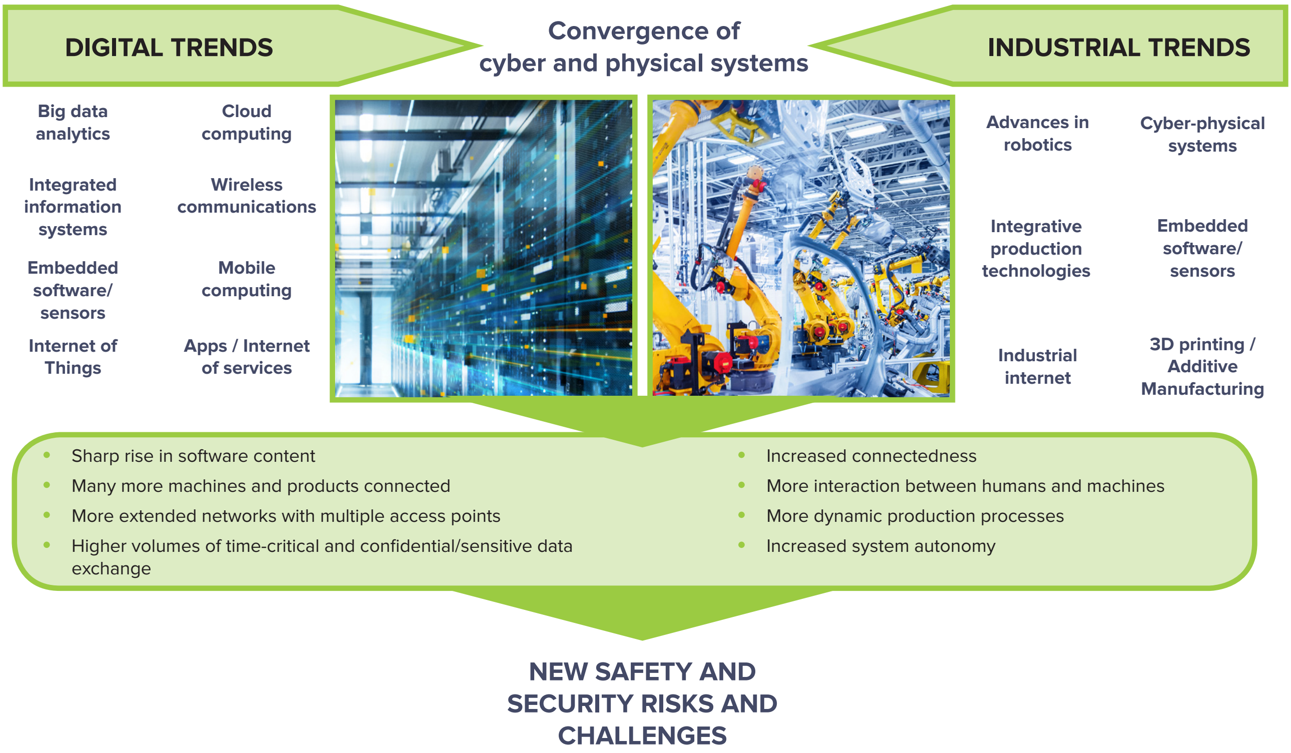
Industry 4.0 is characterised by the convergence of the digital (cyber) and manufacturing (physical) environments. Cyber-physical systems are designed to sense and interact with the physical world (including human users) and provide this data for “smarter” analysis and decision-making within cyber applications.

Enabled by cyber-physical systems, the convergence of digital and manufacturing systems in Industry 4.0 is happening in a number of “dimensions”:

- The vertical integration of flexible and reconfigurable manufacturing systems within businesses (“smart factories”/”smart enterprises”);
- The horizontal integration of inter-company value chains and networks (“smart supply chains”);
- The product life-cycle integration of digital end-to-end engineering activities across the entire value chain of both the product and the associated manufacturing system.

As shown in Figure 2, convergence in Industry 4.0 is resulting in significant transformations to manufacturing systems. This, in turn, is leading to new safety and security risks and requirements, which are discussed in the following sections.

Figure 2: The convergence of cyber and physical systems in Industry 4.0


DIGITAL TRENDS
Convergence of cyber and physical systems
INDUSTRIAL TRENDS
Big data analytics
Cloud computing
Integrated information systems
Wireless communications
Embedded software/ sensors
Mobile computing
Internet of Things
Apps / Internet of services
Advances in robotics
Cyber-physical systems
Integrative production technologies
Embedded software/ sensors
Industrial internet
3D printing / Additive Manufacturing

- Sharp rise in software content
- Many more machines and products connected
- More extended networks with multiple access points
- Higher volumes of time-critical and confidential/sensitive data exchange
- Increased connectedness
- More interaction between humans and machines
- More dynamic production processes
- Increased system autonomy

NEW SAFETY AND SECURITY RISKS AND CHALLENGES

2.4 Safety and security in Industry 4.0

Significant knowledge gaps still exist regarding the safety and security implications of the deployment of 4IR technologies in manufacturing. While some of these implications are becoming apparent, their full scale and nature are still being explored and will further emerge as these technologies are applied in production.

2.4.1 Safety

The safety of people in working environments is studied under the field of occupational health and safety (OHS), which focuses on the safety, health and welfare of workers. Ensuring safety has traditionally been a major concern and area of work in manufacturing OHS, with injury rates decreasing over time.[2]

However, there are growing concerns that the implementation of new Industry 4.0 technologies in the working environment could lead to significant changes in existing methods of work. New objects and complex and autonomous systems are increasingly being used, bringing about new challenges for work processes and safety.[3] Traditionally static production processes allowing a relatively accurate prediction of hazards and risks in the working environment are expected to change to more dynamic and changing environments, potentially rendering existing laws and formalised practices to OSH risk assessment invalid. As such, new protective and preventive safety measures are required.[4]

The convergence of technologies such as robotics, artificial intelligence and the Internet of Things could result in fundamental changes to the way work is organised and carried out in manufacturing environments. For example, traditionally caged robots could now become more intelligent and autonomous, becoming uncaged, mobile and working in closer collaboration with humans through improved speech and image recognition.[5] Interactions between workers and digital technologies are expected to increase, involving new human–machine interfaces based on voice or visual commands that could transform the way workers communicate with machines.

Industry 4.0 therefore opens up the possibility for the emergence of new safety risks resulting from changes introduced by, for example:[6]

- New work equipment and tools (including new machine behaviour such as self-learning autonomy);
- New ways in which work is organised and managed (including new behaviours of people);
- Varying characteristics of the workforce (including new skills, knowledge and information requirements);
- Unclear responsibilities for managing safety.

[2] EHS Today (2018). “Cause to Celebrate: Workplace Injuries Continue to Decline”. Available online: <https://www.ehstoday.com/safety/cause-celebrate-workplace-injuries-continue-decline>.

[3] Podgórski et al. (2017). Towards a conceptual framework of OSH risk management in smart working environments based on smart PPE, ambient intelligence and the Internet of Things technologies. International Journal of Occupational Safety and Ergonomics, Vol. 23, No. 1, 1–20.

[4] Ibid.

[5] Stacey et al. (2018). Foresight on new and emerging occupational safety and health risks associated with digitalisation by 2025. European Agency for Safety and Health at Work (EU-OSHA).

[6] Ibid.

2.4.2 Security

In addition to modifying existing methods of work, the introduction of new Industry 4.0 technologies is expected to involve the exchange of high-volume time-critical data and information between technological systems, originating from an increasing number of stakeholders across value chains.[7]

As computers and communications become embedded in manufacturing systems and products, software will play an ever-greater role,[8] which opens the door to the introduction of a range of IT security hazards caused by software and network vulnerabilities.

Beyond the intrinsic security risks existing within information technology (IT) systems present in any organisation, manufacturing involves particular security challenges as a result of the unique nature of cyber-physical systems (CPS), which include operations technology (OT) such as industrial control systems (ICS), supervisory control and data acquisition (SCADA) systems, and networked machines, sensors, data and software.[9]

This additional layer of complexity, unique to the manufacturing sector, introduces the potential for cyber-physical consequences (e.g. damage to assets or products) that could translate into safety incidents. This is the point where the safety and security worlds overlap.

Unlike the study of Industry 4.0 safety, which is a topic still in its infancy, security for Industry 4.0 is a relatively better understood phenomenon. The Industry 4.0 security dimension is already showing visible signs of disruption for some manufacturers. For example, a 2018 survey of UK-based manufacturers highlights that 48 per cent of respondents have at some time been subject to a cyber security incident, while 91 per cent of businesses surveyed said they are investing in digital technologies in readiness for the Fourth Industrial Revolution, but 35 per cent of those consider that cyber vulnerability is inhibiting them from doing so fully.[10]

2.5 Critical manufacturing

Although safety and security are important concepts for all manufacturing sectors, the consequences of potential incidents become particularly acute in the so-called “critical manufacturing” sectors. These are defined as those that, together with both physical and virtual infrastructures, are considered necessary for a country to function and are vital for the security, economic prosperity, national public health and safety of a country.[11]

[7] ACATECH (2013). Recommendations for implementing the strategic initiative INDUSTRIE 4.0. Germany’s National Academy of Science and Engineering.

[8] Leverett et al. (2017). Standardisation and Certification of Safety, Security and Privacy in the “Internet of Things”. European Commission, Joint Research Centre technical reports.

[9] MFORESIGHT (2017). Cybersecurity for manufacturers: securing the digitized and connected factory. MForesight: Alliance for Manufacturing Foresight.

[10] MakeUK (2018). Cyber security for manufacturing.

[11] CISA (2019). Critical Infrastructure Sectors. The Cybersecurity and Infrastructure Security Agency (CISA), US Department of Homeland Security; CPNI (2019). Critical National Infrastructure. UK Centre for the Protection of National Infrastructure.

Example critical manufacturing sectors, as defined by the United States Department of Homeland Security, include:

- Primary metals manufacturing;
- Machinery manufacturing;
- Electrical equipment, appliance and component manufacturing;
- Transportation equipment manufacturing.

Industry 4.0 systems are likely to generate more safety and security questions as they become more complex. Research, policy and practice all have a role to play in ensuring that emerging digital technologies can deliver on their promise to unlock new value-capture opportunities for the manufacturing sector by addressing key safety and security concerns in the coming years.

In this new landscape, vendors, system integrators, regulators and the industrial community as a whole have to start collaborating to better characterise Industry 4.0 safety and security risks and to develop appropriate measures to address emerging requirements.

3. The safety dimension of Industry 4.0

Although a great number of studies have been published in recent years about Industry 4.0, there is still no standardised way to classify the emerging safety risks and requirements. Under the new anticipated Industry 4.0 landscape, the occupational health and safety (OHS) community, together with vendors, system integrators and regulators, will have to start collaborating to better characterise safety risks and meet key requirements for the safe adoption of 4IR technologies. This section outlines an initial taxonomy of safety risks and requirements, based on the existing literature, which could be used as a first step to inform policy needs for the future.

3.1 Safety for industry 4.0 – definition

Safety in the context of industrial and technological systems refers to the fact that the operation of machines, production facilities and products should not pose a danger to either people or the environment.[12] Additional relevant safety dimensions for Industry 4.0 have been highlighted by Germany's National Academy of Science and Engineering, which states that:

> *"Safety requires both operational safety and a high degree of reliability. Operational safety refers to the aspects of safety that are dependent on the correct operation of the system or that are provided by the system itself. The elements required to deliver operational safety include low fault rates, high fault tolerance (i.e. the ability to keep operating correctly even when faults occur) and robustness (the ability to guarantee basic functionality in the event of a fault). Reliability refers to the probability of a (technological) system operating correctly for a given period of time in a given environment."*

ACATECH (2013) – Germany's National Academy of Science and Engineering

3.2 Emerging 4IR safety risks

As summarised in Table 2, safety risks arising from new 4IR technologies and systems can be classified into three main categories: new sources of potential physical risks and hazards; long-term health risks from exposure to new hazardous substances or radiation; and psychosocial risks from emerging sources of work-related stress. Unlike security risks, which are currently better studied and understood, the full scale and nature of safety risks can only currently be predicted based on our existing understanding of long-term developments. In this regard, Table 2 highlights some of the key emerging risks discussed in a range of foresight exercises found in the literature. Further work is required to better characterise these risks in the future.

[12] ACATECH (2013). Op. cit.

Table 2 - Overview of selected emerging Industry 4.0 safety risks

NEW SOURCES OF POTENTIAL PHYSICAL RISKS AND HAZARDS

New mechanical, electrical, thermal hazards

- New systems, such as autonomous robots, vehicles and drones, collaborative robots or exoskeletons, could generate mechanical, electrical or thermal hazards that lead to harm through trapping, entanglement, impact, noise, vibration or electric shock for users.
- Safety risks could also be generated by peripheral equipment used by robots (e.g. lasers, welding electrodes).
- Autonomous robots, guided vehicles and exoskeletons must be physically stable enough to work on slopes or uneven ground to avoid falling over.

New sources of engineering and human errors

- The increasing complexity of new systems could lead to design, installation and/or operational errors such as loose connections, faulty electronics or errors in the programming and interfacing of peripheral equipment, leading to physical injuries of workers.

Reduced safety situational awareness in workers

- Reliance on digital systems to alert about safety hazards could create workers with lower situational awareness unable to prevent safety incidents themselves or respond to incidents when safety systems fail.

Serial failure from high system integration and interdependence

- High levels of system interconnectivity and integration could help propagate failures that could trigger safety hazards for workers interacting with said systems. This complexity also increases the difficulty of risk assessments.

Lack of AI algorithm transparency and understanding

- The behaviour of AI-based systems could become difficult to predict because of a lack of transparency, increasing the complexity of assessing safety risks, recognising when behaviour is not normal and responding in case of failure.

Physical risks from over-reliance on cobots or exoskeletons for manual handling

- Over-reliance on cobots or exoskeletons for manual handling could have implications for workers' physical fitness. This could result in a loss of muscle/bone density or joint flexibility. Workers could tempt them to take greater risks.

Risk of command loss or misinterpretation in new human–machine interfaces (e.g. voice, gesture, eye tracking)

- Gesture, voice or eye tracking commands could be misinterpreted or sent to the wrong machine, leading to potential safety incidents, especially if safety-critical commands do not require validation/confirmation.

New ergonomic risks for technology users

- New workstations that include the use of handheld or portable devices might generate ergonomic risks (e.g. injury to the upper limbs, neck and back) if used for long periods of time. Legislation must adapt to these changes.

LONG-TERM HEALTH RISKS FROM EXPOSURE TO NEW HAZARDOUS SUBSTANCES OR RADIATION

- Metal powders employed in additive manufacturing (3D printing) represent a known health risk for workers exposed to airborne particles. Safety measures are required to avoid long-term exposure to these materials.
- Furthermore, new 3D printing and bio-printing technologies involve the use of new materials and substances whose health consequences might not yet be fully understood. Exposure to these might be exacerbated by a lack of regulations on safe handling procedures.

PSYCHOSOCIAL RISKS FROM EMERGING SOURCES OF WORK-RELATED STRESS

Increased work performance pressure

- Digital devices used to supervise workers' productivity could increase work performance pressure and lead to negative stress-related health impacts if workers feel that they have to meet challenging performance targets that require increased cognitive demands that are beyond their capabilities.

Stress related to increased oversight and privacy invasion

- Constant oversight enabled by new digital technologies can generate stress and anxiety, particularly if they reduce workers' human/social interaction and independence within the limits of the working place. This can also generate an atmosphere of privacy invasion, particularly if workers have no access to the data collected about them.

Worsening workplace atmosphere, worker involvement and peer support

- New digital technologies could enhance independent work, leading to reduced contact between employees, co-workers and supervisors. Less social workplaces could induce loneliness related to stress and anxiety.

Work–life balance

- Digitally enabled mobility and remote access would allow employees to work away from traditional locations, including in their homes. This could translate into worsening stress induced by their individual work–life balance.

Sources: Stacey et al. (2018). Foresight on new and emerging occupational safety and health risks associated with digitalisation by 2025. European Agency for Safety and Health at Work (EU-OSHA); Leso et al. (2018). The occupational health and safety dimension of Industry 4.0, Med Lav, 109, 5: 327–338; EU-OSHA (2016). Discussion paper: 3D printing and additive manufacturing – The implications for OSH; Knowledge at Work (2017). The future of safety in the digital age; Steijn et al. (2016). Emergent risk to workplace safety as a result of the use of robots in the work place, TNO Report R11488, TNO (Netherlands Organisation for Applied Scientific Research); Boagey, R. (2016). Hand in hand, Institution of Mechanical Engineers; Abdlkader et al. (2015). Brain computer interfacing: Applications and challenges, Egyptian Informative Journal 16, 2: 213–230; Suh, A. and Lee, J. (2017). Understanding teleworkers' technostress and its influence on job satisfaction. Internet Research 27, 1: 140–159; Celik, N. and Oztürk, F. (2017). The upcoming issues of industry 4.0 on occupational health and safety specialized on Turkey example. Int. J. Econ. Bus. Manag., 1: 236–256; EU-OSHA (2017). Monitoring technology: the 21st century's pursuit of well-being? European Agency for Safety and Health at Work.

3.3 Key safety requirements arising from industry 4.0

The path to assuring the safety of new 4IR technologies and/or managing key safety risks is, however, complex. As suggested by Hawkins and McDermid in the briefing paper accompanying this report, at the most fundamental level, assuring the safety of new 4IR technologies and systems requires the relevant actors to:[13]

- Provide a clear and unambiguous definition of how the system must behave in all situations it might encounter during operation in order to be considered safe;
- Implement the system such that it provides the required behaviour, and generate evidence to demonstrate this;
- Gain a detailed understanding of things that might go wrong when the system is operating, identify if these might affect safety and demonstrate that sufficient mitigation has been put in place for those things.

Each of these steps is challenging in its own right and completing them requires addressing a number of requirements in future efforts to prevent and control key Industry 4.0 safety hazards. Table 3 classifies some of these key requirements into four main categories, as gathered from the published literature: managing the integration of new and old legacy systems (i.e. the transition from Industry 3.0 to Industry 4.0); ensuring risk prevention at distinct stages of the technology life cycle; developing new skills for risk prevention; and establishing clear safety liabilities and responsibilities within an Industry 4.0 context. Section 5 discusses existing international efforts developed to address these requirements, while Section 6 examines open themes where future work is still needed.

[13] Hawkins, R. and McDermid, J. (2019). Safety assurance of autonomy to support the Fourth Industrial Revolution. Assuring Autonomy International Programme, University of York.

Table 3 - Requirements for addressing Industry 4.0 safety risks

INDUSTRY 3.0–4.0 TRANSITION

Managing OHS risks arising from the integration of new and old legacy systems

- The long life expectancy of existing operation technologies (OT) means that there will be a transition period in which both old and new technologies are in service. This interaction represents an OHS challenge for a number of reasons: technical integration is not always straightforward; infrastructure designed for old technology might not work properly for new applications; and workers might struggle to switch between old and new systems and their respective operational procedures. All of these represent sources of unforeseen OHS risks that need to be addressed.

RISK PREVENTION AT DIFFERENT STAGES

Developing new and/or improved "design for safety" methodologies

- Embedding safety in the design process of new applications appears to be the most suitable approach to reduce safety risks within the current context, where safety regulations and standards for Industry 4.0 are still not mature. However, further work is required to develop design methodologies that include new safety risks as a key design variable. Once in operation, feedback from users could provide essential input for next-generation designs.

Creating suitable certifications and standards to ensure minimum levels of safety

- Establishing risk profiles of Industry 4.0 workplaces and developing appropriate international standards to protect workers from emerging risks remain pending tasks. Further investigation is required to develop workplace safety standards for new technological applications, particularly those that involve close interaction with humans.

Developing risk assessment, monitoring and management methodologies for factories with changing risk profiles

- Identifying, preventing and managing safety risks become challenging tasks under an Industry 4.0 context in which production processes are no longer static, adding complexity to the accurate prediction of hazards and risks in the working environment. This context is likely to require adequate OHS assessment and management procedures able to be continuously changed, evaluated and improved as factory risk profiles are modified. Developing such risk assessments, monitoring and management methods remains a pending task.

NEW SKILL REQUIREMENTS FOR RISK PREVENTION

Keeping pace with fast technology development rates

- Quick technological change under Industry 4.0 could have OHS implications if risk prevention and management methods struggle to catch up. In addition, workers' skills need to keep pace with changes to avoid new sources of human error, while OHS research and regulations may also struggle to keep up.

Addressing new skills and training needs

- In addition to learning how to use new technologies, Industry 4.0 workers are likely to require skills to adapt to the new ways of working introduced by said technologies, including how to manage their own OHS. New varieties of worker-centred approaches to OHS are likely to emerge, some of which may have unforeseen consequences and make regulation and enforcement difficult. Further research is required to evaluate the relative merits of distinct OHS training strategies (e.g. in-house versus distance learning, general versus vocational education).

Supporting lifelong learning models

- The continuous technological change introduced by Industry 4.0 makes lifelong learning a requirement for employability. This might represent a challenge for an existing workforce not used to continuous education, particularly workers not familiarised with digital technologies, and for existing short-focused training approaches.

Creating flexible self-learning methods and approaches

- New skills training could be facilitated by digital learning platforms that allow learning at workers' own pace, tailored to their own needs and learning styles, rather than current occasional training schemes based on group and not individual needs. Developing such programmes and certifying their effectiveness remains a pending task.

Workforce de-skilling

- Over-reliance on new technology could lead to workers becoming less able to solve issues and make decisions, including how to prevent and respond to OHS events. The challenge is how to ensure that workers' skills do not become out of date to the point that they no longer have the experience to prevent OHS risks.

SAFETY LIABILITIES AND RESPONSIBILITIES

Need for new regulatory framework

- A key requirement for the successful implementation of Industry 4.0 is related to the clarification of OHS liabilities and responsibilities for new systems and methods of work. A multi-stakeholder approach is required to develop an appropriate regulatory framework that clarifies responsibilities between vendors, system integrators and users.

Sources: Leso et al. (2018). The occupational health and safety dimension of Industry 4.0, Med Lav, 109, 5: 327–338; Stacey et al. (2018). Foresight on new and emerging occupational safety and health risks associated with digitalisation by 2025. European Agency for Safety and Health at Work (EU-OSHA); Brettel et al. (2014). How Virtualization, Decentralization and Network Building Change the Manufacturing Landscape: An Industry 4.0 Perspective. International Journal of Information and Communication Engineering, 8: 37–44; ERPS (2015). Industry 4.0 – Digitalisation for productivity and growth. European Parliamentary Research Service; Celik, N. and Oztürk, F. (2017). The upcoming issues of industry 4.0 on occupational health and safety specialized on Turkey example. Int. J. Econ. Bus. Manag., 1: 236–256; WEF (2016). The future of jobs: Employment, skills and workforce strategy for the fourth industrial revolution — Global Challenge Insight Report. World Economic Forum; Zhou, K. et al. (2015). Industry 4.0: Towards future industrial opportunities and challenges. 12th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD); HSE (2017). Tackling work-related stress using the Management Standards approach: A step-by-step workbook. Health and Safety Executive; NIOSH (2014). The state of the national initiative on prevention through design. US National Institute for Occupational Safety and Health, Publication No. 2014–123; Tupa, J. et al. (2017). Aspects of risk management implementation for Industry 4.0. 27th International Conference on Flexible Automation and Intelligent Manufacturing, 27–30; Jilcha, K. and Kitaw, D. (2017). Industrial occupational safety and health innovation for sustainable Development. Eng. Sci. Technol. Int. J., 20: 372–380.

4. The security dimension of Industry 4.0

Industry 4.0 security risks could potentially translate into very tangible and sizeable losses for manufacturers if not prevented. Unlike the study of Industry 4.0 safety, which is a topic still in its infancy, security for Industry 4.0 is a relatively better understood phenomenon. However, no standardised taxonomies of emerging risks and requirements exist. This section introduces practical classifications based on selected academic and policy literature, which can be employed as a starting point to understand some of the key dimensions of Industry 4.0 security and implications for manufacturers.

4.1 Security for Industry 4.0 – definition

In the context of Industry 4.0, "security"[14] refers to the fact that IT and OT systems need to be protected against misuse and unauthorised access (e.g. access protection, security against attacks, data and information security).[15] Relevant features of security for Industry 4.0 have been highlighted by Germany's National Academy of Science and Engineering, which states that:

> *"The goals of security measures are to increase confidentiality (the restriction of access to data and services to specific machines/human users), integrity (accuracy/completeness of data and correct operation of services) and availability (a means of measuring a system's ability to perform a function in a particular time). Depending on the technological system in question and the data and services that it incorporates, security provides the basis for information privacy, i.e. the protection of individuals against infringements of their personal data rights. It also enables know-how protection, i.e. protection of intellectual property rights."*

ACATECH (2013) – Germany's National Academy of Science and Engineering

4.2 Emerging Industry 4.0 security risks origins and consequences

As outlined in Figure 3, Industry 4.0 security risks originate from cyber security threats targeting specific vulnerabilities within information technology (IT) and operation technology (OT) systems.[16] In order to prevent these risks, it is first necessary to understand three main cyber security components: adversarial attack

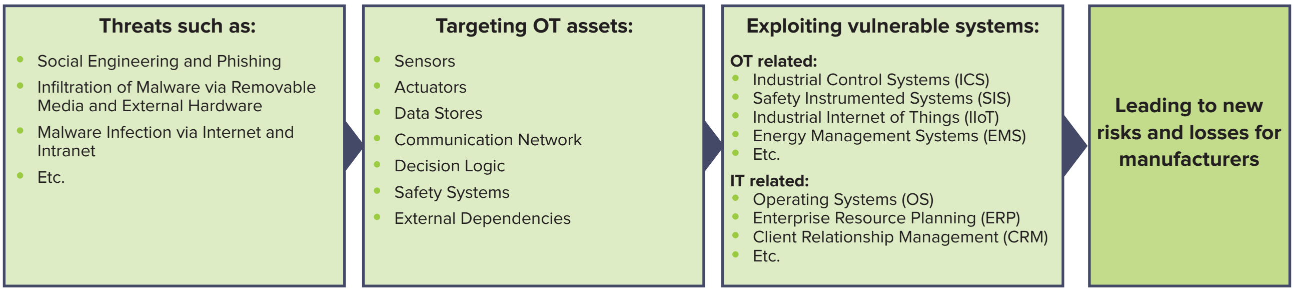
[14] Also known as "IT security" and cyber security.

[15] ACATECH (2013). Op. cit.

[16] IT systems refer to traditional PCs, servers, cloud storage, enterprise networks, smartphones and tablets, among others; OT systems include, for example, industrial controls systems (ICS), safety instrumented systems (SIS), the Industrial Internet of Things (IIoT) and energy management systems (EMS). Extracted from: Copic, J. and Leverett, E. (2019). Managing cyber risk in the Fourth Industrial Revolution. University of Cambridge.

techniques, target OT assets and vulnerable systems.[17]

Security threats can include malware and efforts to corrupt data, steal intellectual property (IP), sabotage equipment, commit extortion and disable networks.[18] As suggested by Copic and Leverett in the accompanying briefing paper, adversaries employ several techniques in order to compromise a system and achieve their end goal. These techniques are used to target key assets within an industrial environment such as sensors, actuators, data stores, communication networks, decision logic, safety systems and external dependencies. They do so by targeting key vulnerabilities in IT or OT systems.[19]



Threats such as:

- Social Engineering and Phishing
- Infiltration of Malware via Removable Media and External Hardware
- Malware Infection via Internet and Intranet
- Etc.

Targeting OT assets:

- Sensors
- Actuators
- Data Stores
- Communication Network
- Decision Logic
- Safety Systems
- External Dependencies

Exploiting vulnerable systems:

OT related:
- Industrial Control Systems (ICS)
- Safety Instrumented Systems (SIS)
- Industrial Internet of Things (IIoT)
- Energy Management Systems (EMS)
- Etc.

IT related:
- Operating Systems (OS)
- Enterprise Resource Planning (ERP)
- Client Relationship Management (CRM)
- Etc.

Leading to new risks and losses for manufacturers

Figure 3 - Sources of security risks for manufacturers (source: Ibid. Modified by authors)

A study by Germany's Federal Office for Information Security (BSI) compiled a list of the top ten cyber security threats faced by manufacturers in 2016. Among the conditions that enable these threats, insufficient organisational policies, a lack of knowledge at all levels of the organisation (including management and board levels) and human errors are key factors that not only favour attacks but also impede the detection and restoration of systems after a successful attack.[20] The top ten threats identified by BSI are:

- **Social engineering and phishing**
  Social engineering is a method used to gain unauthorised access to information or IT systems by exploiting human traits such as curiosity, helpfulness or fear. Typical examples are fraudulent phishing emails tempting employees to open attachments containing malware.

- **Infiltration of malware via removable media and external hardware**
  Removable media such as USB flash drives are widely used in IT and OT networks. These can become infected with malware when used outside the company.

- **Malware infection via Internet and intranet**
  Malware can be introduced to a company intranet through vulnerabilities present in standard components connected to the Internet in enterprise networks. These include operating systems, web servers, databases, browsers or email clients.

- **Intrusion via remote access**
  External access for maintenance purposes is very common in OT installations. Poorly secured access via default passwords or even hardcoded passwords is a widespread issue. External access via virtual private networks (VPN) sometimes allows access to additional systems that should not be accessed externally.

[17] Copic, J. and Leverett, E. (2019). Op. Cit.

[18] MFORESIGHT (2017). Op. Cit.

[19] Copic, J. and Leverett, E. (2019). Op. Cit.

[20] BSI (2016). Industrial Control System Security – Top 10 Threats and Countermeasures 2016. Germany's Federal Office for Information Security (BSI).

- **Human error and sabotage**
  Privileged access given to staff working in OT environments represents a risk if this is not accompanied by strict organisational regulations that prevent error and sabotage.

- **Control components connected to the Internet**
  OT assets such as programmable logic controllers are often connected directly to the Internet without featuring sufficient security levels. In addition, installation of patches is not possible for these controls if a vulnerability is discovered, so implementing additional security mechanisms is urgently required.

- **Technical malfunctions and force majeure**
  It is impossible to exclude software errors in security-specific components and OT components that may lead to unexpected malfunction, as well as potential hardware defects and network failures.

- **Compromising of extranet and cloud components**
  Cloud solutions lead to the asset owner having very limited control over the security of these components, while they may still be connected directly to local production.

- **Distributed denial of service attacks (DDoS)**
  Purposely interrupting communications between OT components, leading to control data no longer being transmitted, or overloading components with a very high number of queries, thereby making it impossible to deliver a timely answer, is known as a distributed denial of service (DDoS). These attacks have the aim of deliberately causing a malfunction.

- **Compromising of smartphones in the production environment**
  The use of smartphones or tablets in OT environments and components constitutes a special case of remote maintenance access adding additional attack vectors.

Manufacturers are therefore exposed to a high number of security threats that can translate into very tangible and sizeable risks for their businesses. Although no standardised risk taxonomies exist, Table 4 introduces a useful classification developed by the Cambridge Centre for Risk Studies. In this classification, 19 common potential consequences of cyber security incidents are listed and explained. Further details can be found in the accompanying briefing paper by Copic and Leverett.

Table 4 - Overview of emerging Industry 4.0 security risks for manufacturers

SECURITY RISKS	DESCRIPTION
Breach of privacy event	The cost of responding to an event involving the release of information that causes a privacy breach, including notification, compensation, credit-watch services and other third-party liabilities to affected data subjects, IT forensics, external services, internal response costs and legal costs.
Data and software loss	The cost of reconstituting data or software that has been deleted or corrupted.
Network service failure liabilities	Third-party liabilities arising from security events occurring within the organisation's IT network or passing through it in order to attack a third party.
Business interruption	Lost profits or extra expenses incurred as a result of the unavailability of IT systems or data resulting from cyber attacks or other non-malicious IT failures.
Contingent business interruption	Business interruption resulting from the IT failure of a third party, such as a supplier, critical vendor, utility or external IT service provider.
Incident response costs	Direct costs incurred to investigate and close the incident to minimise post-incident losses. Applies to all the other categories/events.
Regulatory and defence costs	Costs related to the legal, technical or forensic services necessary to assist the policy-holder in responding to governmental inquiries relating to a cyber attack, including fines, penalties, defence costs, investigations or other regulatory actions in violation of privacy law, and other costs of compliance with regulators and industry associations.
Liability – product and operations	Third-party liabilities arising in relation to product liability and defective operations.
Liability – technology errors and omissions	Third-party claims relating to a failure to provide adequate technical service or technical products, including legal costs and expenses of allegations resulting from a cyber attack or IT failure.
Liability – professional services errors and omissions	Third-party claims relating to a failure to provide adequate professional services or products (excluding technical services and products), including legal costs and expenses for allegations resulting from a cyber attack or IT failure.
Liability – directors and officers	Cost of compensation claims made against the individual officers of the business, including for breach of trust or breach of duty resulting from cyber-related incidents, and can result from alleged misconduct or failure to act in the best interests of the company, its employees and shareholders.
Multimedia liabilities (defamation and disparagement)	Cost of investigation, defence cost and civil damages arising from defamation, libel, slander, copyright/ trademark infringement, negligence in publication of any content in electronic or print media, as well as infringement of the intellectual property of a third party.
Financial theft and fraud	The direct financial loss suffered by an organisation arising from the use of computers to commit fraud or theft of money, securities or other property.
Reputational damage	Loss of revenue arising from an increase in customer churn or reduced transaction volumes, which can be directly attributed to the publication of a defined security breach event.
Cyber extortion	The cost of expert handling for an extortion incident, combined with the amount of the ransom payment.
Intellectual property (IP) theft	Loss of value of an IP asset, expressed in terms of loss of revenue as a result of reduced market share.
Environmental damage	Costs of clean-up, recovery and liabilities associated with a cyber-induced environmental spill or release.
Physical asset damage	First-party loss due to the destruction of physical property resulting from cyber attacks.
Death and bodily injury	Third-party liability for death and bodily injuries resulting from cyber attacks.

Source: The table has been reprinted from the Cambridge Centre for Risk Studies (2016). Cyber Exposure Data Schema. Cyber Accumulation Risk Management.

Box 4-1: Physical asset damage – case studies

Safety system attacks at petrochemical facilities (2017)

- In late 2017 a destructive malware, termed Triton or Trisis, targeted a single petrochemical facility. Triton was designed to undermine ICS safety instrumented systems (SIS) and under the right circumstances could result in physical destruction.
- The malware enabled attackers to remotely control the SIS targeting the Triconex safety controller by Schneider Electric. Reports indicate that the plant shut down initially in June 2017 and again in August 2017, and it is believed that the attackers were in the system long before the shut-down.
- Schneider Electric has released a patch to address the zero-day vulnerability used in the attack. This is the first known incident of a cyber attack violating safety instrumented systems, and it provides us with a key example of why we must focus on integrity. If it were easier to verify the integrity of the firmware of the SIS, it might have been quicker to detect and thwart these attacks.

Sources: B. Johnson et al. (2017). Attackers Deploy New ICS Attack Framework 'TRITON' and Cause Operational Disruption to Critical Infrastructure. FireEye.; Dragos (2017). TRISIS Malware - Analysis of the Safety System Targeted Malware. TLP: White.

Physical asset damage from malware at candy manufacturer (2017)

- A candy manufacturer reported $187.6 million in losses from NotPetya as a result of damage caused to its hardware and operational software systems, affecting sales, distribution and other financial systems. It lost 1,700 servers and 24,000 laptops because of the malware. The manufacturer is claiming physical asset damage as the result of a clause in its property insurance that states: "Physical loss or damage to electronic data, programs, or software, including physical loss or damage caused by the malicious introduction of a machine code or instruction." The losses experienced fall into the following categories: Physical Asset Damage, Business Interruption and Incident Response Costs.

Sources: E. Rosen (2018). Manufacturers Remain Slow to Recognize Cybersecurity Risks. The New York Times, sec. Business; K. McCarthy (2019). Cyber-Insurance Shock: Zurich Refuses to Foot NotPetya Ransomware Clean-up Bill – and Claims It's 'an Act of War'. The Register; R. Armstrong and O. Ralph (2019). Mondelez Sues Zurich in Test for Cyber Hack Insurance. Financial Times.

4.3 Key requirements for Industry 4.0 security

Preventing security risks is, however, a challenging task. A number of key requirements need to be met to prevent and/or manage security risks in manufacturing, which go beyond the technical space and touch upon legal, regulatory and educational factors, among others. Table 5 presents an overview of the key technical requirements for ensuring Industry 4.0 security at company level, while Table 6 introduces a non-comprehensive list of non-technical requirements needed to prevent global cyber security threats in the manufacturing sector from a policy and regulatory perspective, as found in the literature. Overall, requirements are classified into the following list of categories:

- Addressing IT/OT technical vulnerabilities;
- Awareness-raising and effective sharing of best practices and tools, including security by design;
- Creating new regulatory frameworks and standards;
- Developing industry-specific cyber security policies;
- Clarifying security liability and responsibility issues;
- Creating effective risk transfer mechanisms;
- Addressing emerging skills and training needs;
- Achieving international cross-border multi-stakeholder cooperation.

Table 5 - Technical requirements for addressing Industry 4.0 security risks

ADDRESSING IT/OT TECHNICAL VULNERABILITIES	
ICS lifetime versus IT system lifetime • Engineering systems are generally designed to last five times longer than IT systems. Continual verification of the device's integrity over a long lifespan is crucial and challenging for legacy systems.	**Third-party vendor access** • Outside vendors are often employed to aid in various engineering support activities such as system improvement or training. This poses a risk should the vendor not adhere to cyber security standards.
Poor patching cadence • It is challenging to patch operating systems and software to ensure functionality. Not only is patching cadence within an organisation a concern but patch releases from vendors are also subject to delays.	**Enterprise management systems** • These systems are a potential entry point for attackers who are trying to pivot (move from one network segment to another) from a corporate environment to the control system.
Poor password security and unencrypted protocols • Default passwords on ICS devices are not regularly changed and the Internet of Things ("IoT") is usually sold with easily hackable passwords and employs unencrypted protocols.	**Network architecture** • Use of firewalls, intrusion detection systems and user privileges can increase or decrease an OT system's security depending on how they are deployed. It is necessary to verify network integrity/access control.
Increasing use of IIoT • Insecure remote connectivity of smart devices and IIoT enables unrestricted outbound Internet access. Exposure to the Internet compromises the integrity of IIoT devices.	**Testing costs** • Many OT products are under-examined because there is too little impetus on independent security testing, and equipment is expensive or cumbersome for a researcher to acquire for testing purposes.

Source: The items above have been extracted from Copic, J. and Leverett, E. (2019). Managing cyber risk in the Fourth Industrial Revolution. University of Cambridge. Adapted and significantly expanded from the original version published in S. Ruffle et al. (2018). Submission to UK Parliamentary Joint Committee on the National Security Strategy: Cyber Security: Critical National Infrastructure Inquiry. Cambridge Centre for Risk Studies.

Table 6 - Non-technical requirements for addressing Industry 4.0 security risks

POLICY AND REGULATORY REQUIREMENTS
Achieving international cross-border multi-stakeholder cooperation • Cyber security is inherently multi-disciplinary and spans private- and public-sector interests. Security challenges are global, with networks, services and attacks rarely confined to a single jurisdiction. Collaboration between governments, industry and academia, although necessary, can be challenging because of the sheer number of actors. The issue of cross-border interdependencies is rarely addressed at strategic level in national strategies.
Awareness-raising and effective sharing of best practices and tools (e.g. security by design) • Awareness of cyber security risks, assessment methods and appropriate mitigation strategies remains a challenge, particularly among SMEs without the necessary skills and expertise to assess their risk profiles. Security by design can help minimise system vulnerabilities, but this is not yet common practice. Tools and guidelines on best practices to foster the cyber security of IT and OT systems are not readily or widely shared among industrial users.
Creating new regulatory frameworks and standards • Most cyber security standards and regulations are not tailored to the needs of the manufacturing sector and are no longer fit for purpose as systems evolve and the threat level changes. A market-based approach to the promotion of cyber security has not produced the required pace and scale of change, and therefore a new regulatory framework accompanied by new standards could incentivise change more directly.
Developing industry-specific cyber security policies • Most national cyber security strategies do not sufficiently address industry-specific cyber security risks such as those relevant to manufacturing. Further efforts are required in this area.
Clarifying security liability and responsibility issues • The risk of security incidents raises questions about how to assign liability between technology providers, system integrators and users of ICTs. The issue is exacerbated by data ownership issues, which involves complex assignments of different rights across different stakeholders.
Creating effective risk transfer mechanisms • Insurance for cyber risks is a complex issue. Cyber risks are usually covered as part of general business insurance, traditionally focused on losses rather than the actual vulnerabilities exploited. Transparency of breach and vulnerability reporting can thus be of real value to drive a change in the security culture, particularly for OT systems.
Addressing emerging skills and training needs • In businesses, many staff members are not cyber security aware and do not understand their responsibilities in this regard, partially due to a lack of formal training. A multi-stakeholder approach might be required to address skills bottlenecks, partnering government, academia and the private sector to develop programmes focused on cyber security education, training and workforce development.

Sources: Royal Society (2016). Progress and research in cyber security: Supporting a resilient and trustworthy system for the UK; LRF (2016). Foresight review of robotics and autonomous systems. Lloyd’s Register Foundation; BIS (2013). UK cyber security standards. Department for Business, Innovation and Skills; Leverett et al. (2017). Standardisation and Certification of Safety, Security and Privacy in the “Internet of Things”. European Commission, Joint Research Centre technical reports; RAENG (2018). Cyber safety and resilience – Strengthening the digital systems that support the modern economy. Royal Academy of Engineering; HM Government (2016). National cyber security strategy 2016–2021; OECD (2017). The Next Production Revolution: Implications for Governments and Business; OECD (2012). Cybersecurity Policy Making at a Turning Point: Analysing A New Generation of National Cybersecurity Strategies for The Internet Economy; DIN/DKE (2016). German standardization roadmap – Industry 4.0, Version 2. DIN/DKE – Roadmap.

5. International responses to the safety and security risks of Industry 4.0

The safety and security dimensions of 4IR technologies in advanced manufacturing are increasingly included in national and international policy, academic and business agendas. The review of international efforts reveals, however, a focus on security, with less attention being paid to the safety dimension. One of the main reasons for this is the lack of information and uncertainty surrounding the possible impacts of new human–machine interactions and their potential physical and psychosocial hazards for workers and users of new technology. This section discusses priority areas of action identified internationally to support the safe and secure adoption of 4IR technologies.

This section is based on the review of selected public- and private-sector studies and initiatives, at national and international levels, addressing the safety and security dimensions of Industry 4.0. These include studies and policy documents produced by national innovation agencies, strategies of national initiatives, reports by industry associations and academic studies. It is important to note that the majority of initiatives analysed focus entirely on security aspects, and only a smaller number focus on safety. An even smaller proportion consider safety and security aspects in conjunction.

Six key interrelated priority areas of action emerged from the review: i) the development of new frameworks, regulations and standards; ii) awareness-raising and sharing of information; iii) skills development; iv) anticipation of risks and needs; v) research and development; and vi) funding of co-innovation efforts. Table 7 provides a broad overview of the emphasis of the initiatives analysed across these priority action areas, which are discussed later in this section. As observed from the table, initiatives addressing the safety dimension of 4IR technologies are less numerous than those addressing the security dimension. The exception are the initiatives designed to anticipate risks, which tend to focus on safety aspects.

Table 7 - Emphasis of international initiatives addressing the safety and security aspects of 4IR technologies

Priority action areas	**Initiatives addressing the safety dimension**			**Initiatives addressing the security dimension**		
	Minor emphasis	Some emphasis	Primary emphasis	Minor emphasis	Some emphasis	Primary emphasis
I. New frameworks, regulations and standards		●				●
II. Awareness-raising and sharing of information	●					●
III. Skills development	●					●
IV. Anticipation of risks			●		●	
V. Research and development		●				●
VI. Funding of co-innovation efforts	●				●	

A key lesson from the review is how these six priority areas are connected to, and depend on, one another. For example, foresight studies represent a key input for informing research needs, while research and development activities inform the elaboration of standards. Awareness campaigns and skills-development activities, in turn, are required for the implementation of standards and novel technologies. Finally, business support facilitates access to, and increases the rate and pace of, the adoption of safety and security technologies, particularly in the case of SMEs, which would otherwise not be able to afford these tools. The need for collaboration between stakeholders across the value chain was identified as a common theme across the different initiatives.

5.1 New frameworks, regulations and standards

The vertical, horizontal and "product life cycle" integration underpinning Industry 4.0 requires the use of common approaches and common terminology within industrial value chains and networks. The development of regulatory frameworks and standards is essential to achieve this. Regulatory frameworks provide benchmarks for the development of standards, which in turn guide companies in their journey from Industry 3.0 to Industry 4.0.

New regulations for cyber security have emerged in recent years, addressing issues related to the security of IT systems and data privacy. Examples of these are the Budapest Convention on Cybercrime, the EU General Data Protection Regulation (GDPR), as well as a host of Cyber Security Acts around the world. However, these norms tend to pay little attention to the security of OT systems. In terms of standards, the ISO/IEC 27000 series of information security standards are the most widely followed. An example of guidelines is the document "A Security Approach for Protecting Converged IT and OT",[21] published by the company Fortinet. It contains five best practices to minimise OT risks: i) increase network visibility; ii) segment networks; iii) analyse traffic for threats; iv) enforce identity and access management; and v) secure both wired and wireless access.

> Regulatory frameworks provide benchmarks for the development of standards, which in turn guide companies in their journey from Industry 3.0 to Industry 4.0.

The fast pace of technology change in manufacturing makes it necessary to update safety and health regulations. The "EU Machinery Directive 2006/42/EC" is a benchmark example of the minimum safety requirements needed in manufacturing. The "Guidance on the application of the essential health and safety requirements on ergonomics", a document derived from the EU Machinery Directive, provides specific guidance in ergonomics. In addition, the International Organization for Standardization (ISO) recently developed the world's first international standard for occupational health and safety management systems, ISO 45001. This standard provides a framework to improve occupational health and safety, eliminate hazards and minimise occupational health and safety risks.[22] Although these documents provide valuable guidance on safety requirements for manufacturing, none of them address the specific risks of 4IR technologies adopted in manufacturing. Some standards that have emerged in response to this need

[21] Fortinet (2019). A Security Approach for Protecting Converged IT and OT.

[22] ISO (2018). ISO 45001:2018. Occupational health and safety management systems – Requirements with guidance for use.

are the ISO 10218 and the ISO/TS 15066, which set benchmarks for safety requirements for industrial robots and collaborative industrial robotic systems. The standards database ErgoNoRA also provides useful guidance in ergonomic-related good practices. ErgoNoRA was developed by KAN, the German Commission for Occupational Health and Safety and Standardization, and DIN Software. The database is updated monthly and contains standards on working conditions, human characteristics (anthropometrics, biomechanics, sensory performance, mental performance, physiology), human–machine interface and human–environment interface.[23] Regarding the psychological aspects of safety, as part of the standards series 45000, the ISO is developing guidelines for psychological health and safety in the workplace (45003).[24]

In order to strengthen security in critical infrastructure and critical manufacturing, the US National Institute of Standards and Technology (NIST) has worked on making existing standards, best practices and regulations easily available to companies. NIST developed the "Framework for Improving Critical Infrastructure Cybersecurity",[25] which presents in an organised structure different standards and guidelines on the cyber security of IT and OT systems in critical infrastructure sectors. Specific guidelines for the critical manufacturing sector were derived from this framework. Although the emphasis of these documents is on security issues, they also address some safety standards. The framework and guidelines are supplemented by the "Critical Infrastructure Cyber Community C^3 Voluntary Program", which is designed to provide support for the adoption of NIST's framework.

Initiatives addressing safety and security best practices in an integrated manner are still incipient. Some of the most significant efforts are the reference documents produced by the International Society of Automation (ISA) and the "Architecture Model Industrie 4.0" (RAMI 4.0).[26] Standards, best practices and technical reports developed by the ISA include areas such as: Industrial Automation and Control Systems Security, Wireless Systems for Automation, and Instrumented Systems to Achieve Functional Safety in the Process Industries. In addition, a series of standards are being developed under the theme of human–machine interfaces.

At the international level, examples of best practice guidelines on IT and OT security aspects include the OECD's Recommendation on the Protection of Critical Information Infrastructures and the reference documentation published by the European Union Agency for Network and Information Security (ENISA), such as: "Good Practices for Security of Internet of Things in the context of Smart Manufacturing"[27] and "Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures". [28]

From a safety perspective, the International Labour Organisation (ILO) provides guidelines on OSH regulations. The most recent are The Promotional Framework for Occupational Safety and Health Convention, 2006 (No. 187) and its Recommendation (No. 197).[29]

Collaborative initiatives between public and private actors were identified to be helping in the adoption of standards and best practices by industry. Examples of these are the Cyber Essentials certification backed by the UK government; the ISASecure certification adopted by the Japanese government as part of its

[23] Kommission Arbeitsschutz und Normung (KAN) – DIN Software GmbH (2019). NoRA OH&S standards search tool.

[24] ISO (2019) ISO/AWI 45003. Occupational health and safety management – Psychological Health and Safety in the Workplace – Guidelines.

[25] National Institute of Standards and Technology (NIST) (2018). Framework for Improving Critical Infrastructure Cybersecurity. US.

[26] Platform Industrie 4.0. (2018). Reference Architecture Model Industrie 4.0 (RAMI 4.0).

[27] ENISA (2018). Good Practices for Security of Internet of Things in the context of Smart Manufacturing.

[28] ENISA (2017). Baseline Security Recommendations for IoT.

[29] International Labour Organisation (ILO) (2019). Safety and health at the heart of the future of work. Building on 100 years of experience. ILO. Geneva.

critical infrastructure protection; and the Charter of Trust, a collaboration effort between the private sector, government organisations and academia for setting baseline cyber security requirements. Cooperation between countries has also led to the establishment of standards and best practices. For instance, the Common Criteria (CC), also known as the standard ISO/IEC 15408, is the result of collaboration between national security and standards organisations in Singapore, Canada, France, Germany, the Netherlands, the United Kingdom and the United States. This standard follows a security-by-design approach to ensure the security of IT products.[30] Another example of a collaborative initiative is the coordination of efforts between Germany, the US, Italy, France and China for the harmonisation of RAMI 4.0.[31]

As explained in Box 5-1, the Cyber Essentials certification was derived from the self-assessment tool "10 steps to cyber security", developed by the UK National Cyber Security Centre. Two other self-assessment initiatives are CheckMe, a simulation tool developed by Check Point, and the reference document "Capabilities assessment for securing manufacturing industrial control systems. Cybersecurity for Manufacturing", published by the US NIST.

Market-based incentives, such as cyber security insurance schemes, also contribute to the adoption of best practices. Examples of initiatives in this field are the Cyber Exposure Data Schema, developed by the Cambridge Centre for Risk Studies in collaboration with insurance industry organisations,[32] and the "Industrial Internet of Things: Safety and Security Protocol", published by the World Economic Forum.[33]

Box 5-1: Cyber Essentials certification scheme (United Kingdom)

Need

- After the UK National Cyber Security Centre (NCSC) published the "10 Steps to Cyber Security", companies approached them asking for some additional detailed guidance. In response to this request, the NCSC launched the Cyber Essentials scheme in 2014.

Response

- Cyber Essentials is a certification scheme, backed by the government of the United Kingdom, against the most common cyber attacks. The scheme was developed through risk-scenario techniques, selecting five controls that were considered the minimum standard required to protect organisations' systems.
- The scheme is flexible, targeted at companies of all sizes, which can decide how much help they require from the certification bodies.
- Cyber Essentials has three levels of operation:
  - First level. Certification bodies (more than 170) carry out the assessment and are approved to issue certificates.
  - Second level. Five accreditation bodies that oversee the certification bodies.
  - Third level. The NCSC oversees the accreditation bodies and runs the overall scheme.
- The Cyber Essentials standard is mandatory for some public-sector contracts.

Lessons learned

- Although having five accreditation bodies has promoted competition and innovation, it has also created inconsistencies and made management of the scheme more challenging.

Sources: National Cyber Security Centre. Cyber Essentials.

[30] CSA (2019). Singapore Common Criteria Scheme.

[31] ISASecure (n.d.). ISASecure™ certifications; Platform Industrie 4.0 2018 Op. cit.

[32] Cambridge Centre for Risk Studies. Cyber Insurance Exposure Data Schema V1.0.

[33] WEF (2018). Industrial Internet of Things Safety and Security Protocol.

5.2 Awareness-raising and iformation-sharing

Raising awareness of the different risks associated with 4IR technologies is necessary for a proactive approach to addressing safety and security risks. Within the reviewed national agendas, cyber security awareness campaigns tend to target SMEs, as well as the general public. Examples include the security awareness campaigns "Information Security Awareness Month" in Japan and the "Go Safe Online" campaign in Singapore. In 2011 the government of Japan designated February the "Information Security Awareness Month". This campaign included a kick-off symposium, public talks and diffusion of information security measures through the website of the National Centre of Incident Readiness and Strategy for Cybersecurity (NISC).[34] "Go Safe Online" is a campaign led by the Cyber Security Awareness Alliance, a public–private partnership. As part of this awareness campaign, they provide several resources for companies to improve their information security, such as the Employee Cyber Security Kit, which is a digital toolkit that allows companies to perform a basic assessment of their cyber security readiness.[35]

Though there are several initiatives designed to raise awareness of occupational safety and health risks in manufacturing, very few of them focus on the emerging risks related to increasing automation. Those that address these issues are conferences, seminars and workshops targeted at more specialised audiences, such as health and safety professionals, robot system integrators and researchers. For example, the US Robotics Industries Association organises the International Robot Safety Conference, which centres on robot safety and provides a comprehensive overview of industry trends and standards. The United Nations Industrial Development Organization (UNIDO) recently organised the International Conference "Ensuring Industrial Safety: the role of government, regulations, standards and new technologies". At the European level, the European Agency for Safety and Health at Work (EU-OSHA) publishes on its website information on OSH events in Europe. Some events that can be found on the website, with a focus on 4IR technologies, are the European Conference on standardization, testing and certification in the field of occupational safety and health organised by the European Occupational Safety and Health Network; and the International Conference on the Prevention of Accidents at Work, organised by the Austrian Workers' Compensation Board (AUVA).

A lack of cyber security incident data is a broadly recognised challenge for risk assessment.[36] This need is being addressed through regulation, partnership initiatives and data-collection efforts. For instance, the General Data Protection Regulation (GDPR) in the European Union introduced the duty to report some types of data breach. In the UK, the Information Sharing Partnership (CiSP) is a joint industry and government initiative for sharing cyber threat information "in real time, in a secure, confidential and dynamic environment".

The collection and sharing of data on occupational health and safety has a much longer tradition. Examples of data-collection efforts include ILOSTAT and national labour force surveys.[37] Nonetheless, these databases may need to be adjusted to capture the emerging issues from 4IR technologies. The European Survey of Enterprises on New and Emerging Risks (ESENER) is a recent effort collecting more detailed information. This survey collects data on occupational safety, health and psychosocial risks, including information on the

[34] NISC (2011). Information Security Awareness Month.

[35] CSA (2018). Employee Cyber Security Kit.

[36] European Union Agency for Network and Information Security (ENISA) (2016). Cyber Insurance: Recent Advances, Good Practices and Challenges Heraklion, Greece; OECD (2012). Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy, OECD Digital Economy Papers, No. 211, OECD Publishing, Paris.

[37] Lloyd's Register Foundation (2018). Foresight review on global safety evidence. Towards a global safety outlook. London.

risk of accidents with machines and OSH management. The third round of the survey is being conducted in 2019, covering more than 40,000 businesses in 33 European countries.[38] There exist several national, regional and international OSH networks that act as forums for sharing information and best practices. Box 5-2 presents information on the ASEAN-OSHNET, an example of these networks within the ASEAN region.

Box 5-2: ASEAN-OSHNET

Need

- The ASEAN Occupational Safety and Health Network (ASEAN-OSHNET) arose in response to the need to raise awareness on OSH issues, to share best practices and to harmonise OSH standards and guidelines within the ASEAN region.

Response

- The ASEAN-OSHNET includes the 10 country members of the Association of South East Asian Nations (ASEAN).
- The activities of the network comprise 7 main areas: information; research and development; standards; training; inspection; national OSH framework; and SMEs and informal economy.
- Examples of the information shared through the network include government and private-sector good practices ("ASEAN-OSHNET Good Occupational Safety and Health Practices 2008/2009") and guidelines on OSH management systems for small and medium enterprises ("ASEAN Guidelines for Occupational Safety and Health").

Sources: ASEAN-OSHNET (2019) Website http://www.asean-osh.net/

5.3 Skills development

Increasing the quality and quantity of safety and security specialists is necessary for the adoption of best practices among industry. Current skills-development initiatives are heavily focused on cyber security. For example, Computer Emergency Response Team (CERT) centres have been established in several countries to strengthen the security of both governments and companies.

Although most of these are focused on critical infrastructures, they have developed useful learning material and capabilities that can be applied in other sectors within manufacturing.[39] An example of this is the ICS-CERT Virtual Learning Portal (VLP) managed by the US National Cybersecurity and Communications Integration Center (NCCIC).[40] It contains online course and learning plans on cyber security for industrial control systems.

Numerous training courses and learning material websites on cyber security were identified. For instance, from the private sector, the Cisco Learning Network offers several training courses, certifications and self-study resources in this field. The Mexican company TIC Defence provides customised training in cyber security. From academia, CyBOK (Cyber Security Body of Knowledge) is a "knowledgebase" online platform that offers education and professional training materials. It is managed by the University of Bristol. Its knowledge areas are: malware; security operations and

[38] EU-OSHA (2019). European Survey of Enterprises on New and Emerging Risks (ESENER).

[39] ENISA (2019). CSIRTs by Country – Interactive Map.

[40] ICS-CERT Virtual Learning Portal (VLP).

incident management; network security; and cryptography and software security.[41]

At the national level, the Cyber Security Agency of Singapore (CSA) offers a Cybersecurity Career Mentoring Programme and the Cyber Security Associates and Technologists Programme. Singapore also addresses the need for lifelong learning through the SkillsFuture initiative, which provides career advice, training courses and study awards and credits. Through the SkillsFuture series programme, the Singaporean government offers courses in cyber security and advanced manufacturing.[42]

In terms of safety training, TÜV SÜD, a global company with a comprehensive offer of testing, certification, auditing and advisory services, offers training courses on industrial safety standards. In addition, the company is integrating security and safety standards in its training courses offer. The US Robotics Industries Association also offers public and in-house training on robot safety, collaborative robot safety and robot risk assessment (see Box 5-3).

Collaboration between the public sector, academia and industry is essential for the development of new programmes that respond to the rapid changes in companies' needs. Examples of skills development initiatives based on this type of partnership are: the competition Cyber Security Challenge UK; the US Initiative for Cybersecurity Education; and the Master of Science Program in Cyber-Physical and Embedded Systems, as part of a collaboration between IBM Research, the Università della Svizzera Italiana, the Swiss Federal Institute of Technology in Zurich (ETHZ) and the Politecnico di Milano (Italy).[43]

Box 5-3: Collaborative Robot Safety training

Need

- The Robotic Industries Association (RIA) helps the robotics industry to assess and assure the safety of robotic applications. As part of their efforts, the RIA provides different sources for training on risk assessment and standards compliance: webinars, one-day training seminars and in-house training services.

Response

- The seminar on Collaborative Robot Safety covers: standard safety requirements (ANSI/RIA R15.06-2012), collaborative safety requirements (ISO/TS 15066), safeguarding, risk assessment and applications of the safety standards in daily operations. These applications include pressure and speed measurements, layout and design elements, mitigation, awareness measures and validation.

Sources: RIA (2019). Robot Safety Resources.

5.4 Anticipation of risks

There is broad consensus internationally about the need to anticipate insufficiently understood safety and security risks in Industry 4.0. Foresight studies and assessment tools are among the most common approaches to address this need. Studies focused on future security issues are mainly being produced by the private sector, while projections of safety risks and opportunities are being

[41] CyBOK (2019). Knowledgebase.

[42] Government of Singapore (2019). SkillsFuture.

[43] IBM Research-Zurich (2017). IBM Research Teams up with Swiss University to Launch Degree in Cyber-Physical and Embedded Systems.

conducted by a more diverse group of actors, including international organisations, charities, national organisations and research institutes.

Studies published by the European Agency for Safety and Health at Work (EU-OSHA), the Lloyd's Register Foundation, the German Federal Institute for Occupational Safety and Health (BAuA) and the Czech Occupational Safety Research Institute (VÚBP) are examples of the latter.

Assessment tools include the Smart Industry Readiness Index launched by the Singapore Economic Development Board (EDB) in partnership with TÜV SÜD.[44] It allows companies to assess and guide their adoption of Industry 4.0 technologies. Simulation applications are a nascent approach to addressing safety risks.

The French Agency for the Improvement of Working Conditions (Anact) has explored the application of a virtual reality platform and 3D software to simulate the impacts of transformations in working conditions.[45] CheckMe, a security assessment tool developed by the company Check Point, is also based on simulation technologies.[46] It evaluates companies' security status in four targets: network, endpoint,[47] cloud and mobile. For example, six vulnerabilities are tested for endpoint evaluations: malware infection; command and control communication; zero day; browser exploit; and ransomware and persistent malware.

Stress-test scenarios are another methodology used to anticipate risks. Copic and Leverett, in the accompanying briefing paper, "Managing cyber risk in the Fourth Industrial Revolution", describe the application of stress-test scenarios in cyber security (also summarised in Section 6).

Box 5-4: SIMUL&CEPTION, simulation for improving working conditions

Need

- Ensure the success of companies' physical investments, such as equipment renewal and expansions, while protecting workers' safety and reducing production disruptions to the minimum.

Response

- The Normandy offices of the French Agency for the Improvement of Working Conditions (Anact) tested a 3D simulation tool in 7 SMEs, involving a total of 130 participants. This process involved recording operators' movements and input flows, following a participatory approach. These data allowed the design of scenarios to predict the possible impacts of the new investments. Some impacts of the project were improved comfort of workers and increases in productivity.

Sources: Anact (2012). Simuler les situations de travail avec un logiciel 3D

[44] EDB- TÜV SÜD (2017). Smart Industry Readiness Index. Singapore.

[45] Anact (n.d.). Outils.

[46] Check Point (2019). CheckMe.

[47] For example, PCs, laptops, tablets, machines.

5.5 Research and development

Research and development is a priority area in national policy agendas to address the knowledge gaps on the risks and opportunities involved in the adoption of 4IR technologies. A variety of research projects and programmes addressing these gaps were identified from this review. Figure 4 presents five trending topics in safety and security R&D for Industry 4.0.

Figure 4 - R&D trending topics in safety and security for Industry 4.0

Five trending R&D topics in Safety for Industry 4.0	Five trending R&D topics in Security for Industry 4.0
❯ Human–machine interaction ❯ Safety design of systems ❯ Sensors/ wearable safety technology ❯ Ambient intelligence (AmI) ❯ Implications of 3D printing for health and safety	❯ Cyber threat simulation and analytics ❯ Malware detection ❯ Encryption technologies ❯ Information security automation ❯ Reference designs and architectures

Source: Policy Links

Emerging research topics and areas for further research are presented in Section 6. Those areas are based on the review of different country strategies, research and international organisations' reports. For example, in Germany the Industrie 4.0 Working Group identified as a priority for future research "the investigation and development of fully describable, manageable, context-sensitive and controllable or self-regulating manufacturing systems".[48]

In order to address this research gap, they focus on five main research themes:

- Horizontal integration through value networks;
- End-to-end engineering across the entire value chain;
- Vertical integration and networked manufacturing systems;
- New social infrastructures in the workplace;
- Cyber-physical systems technology.

In the US, the Networking and Information Technology Research and Development (NITRD) Program funds advanced information technologies in computing, networking and software. NITRD comprises 21 agencies, which focus their R&D activities in 12 areas:

- Artificial intelligence;
- Big data;
- Cyber-physical systems;

[48] ACATECH (2013). Op. cit.

- Cyber security and information assurance;
- High confidence software and systems;
- Health information technology research and development;
- High-end computing;
- Intelligent robotics and autonomous systems;
- Large-scale networking;
- Privacy research and development;
- Software productivity, sustainability and quality;
- Wireless spectrum research and development.

Besides setting priorities related to 4IR technologies in their research agendas, different countries have established public and private cyber security research centres. Examples of these are the UK Academic Centres of Excellence in Cyber Security Research, the Honeywell Industrial Cyber Security Lab and the Siemens China Cyber Defense Center.

Box 5-5 presents a case study from the Fraunhofer Institute of Optronics, System Technologies and Image Exploitation (IOSB) in Karlsruhe, Germany, where an IT laboratory has been equipped with a model factory to simulate network attacks.

An example of an R&D programme that addresses specific safety risks from 4IR technologies is the Assuring Autonomy International Programme. Through this programme, Lloyd's Register Foundation and the University of York support research demonstration projects to facilitate the safe, assured and regulated adoption of robotics and autonomous systems. Box 5-6 presents examples of these demonstrator projects.

Box 5-5: IT security laboratory for production and automation technology (Germany)

Need

- Industry 4.0 involves the networking of production facilities and components along the value chain, exposing production plants to new threats. In order to address the specific needs of Industry 4.0 in terms of protective measures, network technology and testing methods, the Fraunhofer Institute of Optronics, System Technologies and Image Exploitation (IOSB) in Karlsruhe, Germany, equipped an IT laboratory with a model factory.

Response

- The IT laboratory includes real automation components that control a simulated production facility. All network levels of a factory are equipped with typical components, including firewalls, circuits and components for wireless parts. A private cloud makes it possible for IOSB experts to flexibly arrange various configurations and set up the model factory for a variety of scenarios.
- The laboratory is available for companies' consultation on the planning and operational launch of secure industrial network structures. IOSB researchers are also exploring the possibility of opening the laboratory as an education and learning platform.

Sources: Fraunhofer-Gesellschaft (2015). Safe production in Industry 4.0.

Box 5-6: Demonstrator projects for safe, assured and regulated adoption of robotics and autonomous systems

Need

- Lloyd's Register Foundation and the University of York fund the Assuring Autonomy International Programme, which aims to undertake and support research activities that will influence industrial practice and the development and adoption of robotics and autonomous systems.

Response

- As part of the Assuring Autonomy International Programme, demonstrator projects are funded every year. Some examples of these are:
  - Assistive Robots in Healthcare by Bristol Robotics Laboratory (University of West England) and Designability.
  - Safety Assurance of Autonomous Intravenous Medication Management Systems (SAM) by Human Reliability Associates Ltd, NHS Digital and Derby Teaching Hospitals NHS Foundation.
  - Safety Assurance of Cooperating Construction Equipment in Semi-Automated Sites (SUCCESS) by Malardalen University, Sweden, Volvo Construction Equipment and Safety Integrity AB.
  - Safety of Reconfigurable Collaborative Robots for Flexible Manufacturing Systems (RECOLL) by Machining Centers Manufacturing SpA, University of York, National Research Council of Italy and the Institute for Intelligent Industrial Systems and Technologies for Advanced Manufacturing.
  - Towards Identifying and Closing Gaps in Assurance of Autonomous Road Vehicles (TIGARS) by Adelard LLP, City, University of London, Kanagawa University, Nagoya University, and Witz Corporation.

Sources: University of York. Assuring Autonomy International Programme.

5.6 Funding of co-innovation efforts

New technology know-how is not always available to manufacturers, especially SMEs that do not have the time and resources to embark on innovation. To address this problem, a number of international initiatives provide funds aimed at supporting the adoption of technologies and co-innovation between public and private partners.

The Australian Cyber Security Small Business Program illustrates how governments can support small businesses to gain access to certified cyber security health checks.[49] Through this programme the Australian government provides grants of up to AUD 2,100 to cover the costs of certified cyber security health checks. The Dutch FARBO regulation is an example of a business support programme that aims to encourage companies to purchase equipment that reduces exposure to OSH risks, and which prevents harm to or improves the health and safety of employees using the equipment. It involves a reimbursement of 10 per cent of the purchased equipment up to a maximum of EUR 25,000 per item

[49] The Australian Government (2019). Cyber Security Small Business Program.

of equipment/year.[50] In Italy the Workers' Compensation Authority provides financial support to SMEs for compliance with OSH regulations. The programme supports investment in facilities, machinery and equipment; implementation of safety management systems; and training. The support is in the form of credits of up to EUR 155,000 with subsidised interest rates.[51]

Collaboration between academia, public and private actors to achieve cutting-edge security research is the basis of the UK CyberInvest partnership. This programme promotes the direct investment of companies of all sizes in universities that "best meet" their needs. Investments range from GBP 10k for micro-companies (fewer than 10 employees) to GBP 500k for large companies (more than 250 employees). "In-kind" contributions, such as equipment and staff time, are also considered in the scheme.[52] The Singaporean Co-innovation and Development Proof-of-Concept Funding Scheme presented in Box 5-7 is another example of how collaboration between solution-providers and cyber security end-users can be promoted through funding support. A similar approach, but with a focus on health and safety, the UK Digital Catapult Centre, is hosting workshops to promote co-innovation between AI start-ups and manufacturers.[53]

Box 5-7: Co-innovation and Development Funding Scheme (Singapore)

Need

- The increasing sophistication of cyber attacks demands a faster pace in the development of prevention, detection, mitigation and recovery of cyber threats. The Cyber Security Agency of Singapore (CSA) launched the Co-innovation and Development Proof-of-Concept Funding Scheme with the aim of catalysing the development of cyber security solutions that "would meet national cyber security and strategic needs, with potential for commercial application".

Response

- Through the scheme, the CSA provides funding support of up to a maximum of SGD 500,000 for a period of up to 12 months.
- Solution-providers must target their solution to meet the new and emerging demands of at least one cyber security end-user.

Sources: Cyber Security Agency of Singapore (2018). Co-Innovation and Development Proof-of-Concept Funding Scheme.

[50] EU-OSHA (2010). Economic incentives to improve occupational safety and health: a review from the European perspective. European Union: Luxemburg.

[51] EU-OSHA (2010). Economic incentives to improve occupational safety and health: a review from the European perspective. European Union: Luxemburg.

[52] NCSC 2016. CyberInvest.

[53] Digital Catapult (2019). Powered by AI: Health & safety for the manufacturing sector.

6. An agenda for future action

Although several public- and private-sector initiatives aimed at addressing safety and security requirements have been identified, many of these are incipient and leave numerous themes open for further action. Opportunity areas and recommendations identified by the international evidence can inform the development of an agenda for future action involving industrial, academic, and government stakeholders. Future efforts need to consider safety and security requirements in an integrated manner. Pilot studies and activities represent a promising mechanism to help bridge some of the key safety and security knowledge gaps in the deployment of 4IR technologies in manufacturing.

6.1 Safety and security: towards an integrated approach

Safety and security are important dimensions in their own right. As a result, they have traditionally been addressed by separate expert communities. However, Industry 4.0 increases the risk of security vulnerabilities being exploited to generate safety impacts through cyber-physical systems. In particular, security vulnerabilities can play a key role in generating safety hazards or undermining safety controls.

Safety and security have similar objectives. Both are concerned with understanding and controlling the negative impact of system weaknesses, and there are shared concerns related to system integrity.[54] Safety compliance tends to be rule-based, while the essence of security threats consists in abusing established rules. In the same manner that safety progresses with the study of each accident, security progresses with the study of every adversarial exploit. As safety starts to require security, compliance needs to be supplemented with adversarial thinking.[55]

Security engineers usually possess specific expertise in security or privacy testing, but they often lack experience of developing or certifying against safety standards. Similarly, safety engineers often have safety compliance and conformance testing experience, but little knowledge of adversarial approaches.[56] A key implication of Industry 4.0 is the need to “unify” safety and security over the coming years for successful implementation. This will have to be done in the context of quick dynamic change that contrasts with the relatively static nature of safety up to date, traditionally based on pre-market testing according to standards that change slowly.

[54] Hawkins, R. and McDermid, J. (2019). Op. Cit.

[55] Leverett, et al. (2017). Op. cit.

[56] Ibid.

6.2 Key areas of future work - suggestions from international evidence

Table 8 summarises key opportunity areas for future work gathered from international evidence, emphasising themes where safety and security overlaps can be addressed in conjunction. Opportunity areas are classified under the same priority areas of action that emerged from the analysis shown in Section 5. Key highlights are outlined below:

1. Regulation frameworks, standards and best practices

Updating the OHS legislation represents an urgent area of action to prevent safety risks. In addition, progress is needed to include new liability issues in regulatory frameworks, from both safety and security perspectives. The literature review also pointed to the need to continue efforts to develop standards that incorporate the emerging challenges and to share best practices.

2. Awareness-raising and sharing of information

Awareness-raising campaigns have focused on IT security issues, as discussed in Section 5. However, efforts are needed to create and raise awareness of OT security and OHS issues. While current campaigns are targeting the public and SMEs, the review sheds light on the need for customised campaigns for manufacturing companies. Existing information-sharing initiatives are mainly focused on cyber threats and incidents. Recommendations include developing data trusts and improving digital security risk management governance.

3. Skills development

Some overlap was found between documents addressing the need for skills for safety and those with a focus on security. Recommendations for future work tend to focus on three key areas: i) interdisciplinary approaches and collaboration; ii) the use of modelling, simulations and virtual-augmented-reality applications for training; and iii) lifelong learning approaches.

4. Anticipation of 4IR safety and security risks

Recommendations on further work to anticipate risks and needs focus on: development of "prevention through design" approaches; participatory work organisation; creation of new impact and risk assessment methodologies; investment in real-world test facilities; and adoption of socio-technical approaches to work organisation.

5. Research and development

Several areas for future research were identified, with some of the most frequently mentioned themes being:

- Safety: ergonomics; sensing technology; big data applications; and psychosocial effects.
- Security: automated, robust part validation technology; automated vulnerability assessment and detection tools; methods for assuring complex systems of systems; and malware/attack prevention.
- Safety and security: reference architectures for manufacturing; modelling, simulations, virtual and augmented reality applications; data analytics to prevent risks; explainable robust AI.

6. Funding of co-innovation efforts

New sources and mechanisms of funding to support research work and the adoption of best practices by businesses are advised in the reviewed literature. Recommendations also call for interventions to coordinate R&D efforts between the government, academia and the private sector; and to translate scientific knowledge into useful applications.

Table 8 - Key themes and opportunity areas for future work gathered from a review of international evidence on the safe and secure adoption of 4IR technologies in advanced manufacturing

	Safety	Safety and security	Security
1. Regulation frameworks, standards and best practices	• Sharing of best design for safety practices • Updating national OSH legislation	• Promoting adherence to standards • Creating systems and security reference architectures for manufacturing that define the OT and IT functions, standards and integration requirements • Improving international cooperation • Creating and updating regulatory frameworks to account for the new liability issues	• Integrating the use of encryption technologies as part of standards and best practices • Promoting the use of open technologies that facilitate standardisation initiatives • Developing best practice models on data security containing sample company agreements
2. Awareness-raising and sharing of information	• Integrating OSH into general education and vocational training programmes	• Awareness-raising campaigns targeted at the manufacturing environment	• Increasing awareness about IIoT security concerns and their consequences • Development of data trusts • Digital security risk management governance
3. Skills development	• Design for safety practice built on education and training	• Interdisciplinary approach and collaboration • Modelling, simulations, virtual and augmented reality applications for training • Development of digital learning techniques and creation of competence centres • Lifelong learning approach to facilitate skill, re-skill and upskill • Promoting mobility between vocational and academic training	• Continuing collaborative efforts to meet the market demands of the cyber security workforce
4. Anticipation of 4IR safety and security risks	• Conducting comprehensive impact assessments of new technologies, including qualitative methods • Adopting ergonomic approaches in the design and adoption of new technologies at work • Implementing a socio-technical approach to work organisation • Adopting a participative work design	• Adopting a "prevention through design" approach that integrates a user/worker-centred design approach and investing in real-world test facilities (Industry 4.0 Test Labs) • Creating guidelines for migration from Industry 3.0 to Industry 4.0 • Retrofitting of existing solutions • Leveraging learning from the historical role of insurance in confronting new risk scenarios • Creating risk-and cost-based models for decision-making	• Adopting security-by-design approaches • Developing and improving preparedness, response and recovery plans and measures

	Safety	Safety and security	Security
5. Research and development	- Areas for future research: - Testing and piloting of ergonomic and logistical arrangements of autonomous robots - Cognitive ergonomics and neuroergonomics studies - Impacts on mental health and decision-making - Big data applications to monitor the workplace - Predictive maintenance - Design of new sensing technology and of fast sensor fusion algorithms to track multiple moving targets in real time - Robust detection of contact between robots and surrounding living agents - Development of fast responsive controllers - Scalable safety concepts and theories - Health and safety apps - Connections between OSH and public health	- Areas for future research: - Safety and security reference architectures for manufacturing - Security and safety design as a socio-technical system - Development of tools to support compliance auditing - Modelling, simulations, virtual and augmented reality applications to assess and mitigate risks - Scenarios, forensics analyses and data analytics to prevent risks - Explainable robust AI - Identification and modelling of dependencies and interdependencies - Interdisciplinary research - Digital twins for safety and security scenario testing	- Areas for future research: - Open operating systems, development tools and communication infrastructure (to facilitate standardisation efforts) - Malware/attack prediction - Automated vulnerability assessment and detection tools - Automated, robust part validation technology - Decentralised self-configuring methods for trust establishment - Virtualisation technologies that enable the isolation and provision of secure execution environments - Systems of systems engineering methodologies for cyber-physical systems with designed-in cyber security and resilience - Methods for assuring complex systems of systems - Adaptation of lightweight cryptographic procedures and protocols to cyber-physical systems - Development of techniques to collect forensic information - Development of tools to audit the extent of attacks
6. Funding of co-innovation efforts	- Transferring and translating scientific knowledge into practical, accessible workplace solutions and interventions	- Promoting coordination between safety and security research projects	- Improving the coordination of cyber security R&D efforts in partnership with the private sector - Government-sponsored venture capital model to unlock cyber security innovation in SMEs

Sources: ACATECH (2013). Securing the future of German manufacturing industry. Recommendations for implementing the strategic initiative Industrie 4.0. Platform Industrie 4.0. Frankfurt.; European Cyber Security Organisation (2017). Strategic Research and Innovation Agenda. Brussels; ENISA (2012). National Cyber Security Strategies. Setting the course for national efforts to strengthen security in cyberspace; ENISA (2018). Good Practices for Security of Internet of Things in the context of Smart Manufacturing.; EU-OSHA (2015). A review on the future of work: robotics. Discussion Paper; EU-OSHA (2013). Priorities for occupational safety and health research in Europe: 2013–2020. European Agency for Safety and Health at Work; Geisberger and Broy (2015). Living in a networked world. Cyber-Physical Systems (agendaCPS). Integrated research agenda. Munich.; ILO (2019). Safety and health at the heart of the future of work. Building on 100 years of experience. ILO. Geneva; Lloyd's Register Foundation (2018). Foresight review on design for safety. Protecting lives from the start. London; Mahoney (2017). Cybersecurity for manufacturers: securing the digitized and connected factory. MForesight – Computing Community Consortium (CCC); OECD (2012). Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy, OECD Digital Economy Papers, No. 211, OECD Publishing, Paris; Perosh (2012). Sustainable workplaces of the future. European Research Challenges for occupational safety and health. Belgium; Royal Academy of Engineering (2018). Cyber safety and resilience strengthening the digital systems that support the modern economy. London; The Royal Society (2016). Progress and research in cybersecurity Supporting a resilient and trustworthy system for the UK. London; Vasic and Billard (2013). "Safety Issues in Human-Robot Interactions". IEEE International Conference on Robotics and Automation (ICRA) Karlsruhe, Germany, May 6–10, 2013.

6.3 Key areas of work - suggestions from briefing papers

The following recommendations were extracted from the two supporting briefing papers published in conjunction with this report, with the aim of providing deeper insights into key aspects of 4IR safety and security:

1) "Managing cyber risk in the Fourth Industrial Revolution", by Jennifer Copic and Éireann Leverett from the Cambridge Centre for Risk Studies at the University of Cambridge.

With the advancement of new technologies delivered through the Fourth Industrial Revolution, the manufacturing sector needs to review safer ways to adopt these technologies, focusing on cyber security. If integrity cannot be verified within a business, it will be difficult for that business to either verify third parties or justify to its customers that they are safe. Cyber risk seems simple, until you face it daily; thus, in order to truly tackle this issue, a joint effort is needed between industry, policy-makers and researchers.

- **Cyber threat and loss taxonomies**

A cyber threat taxonomy detailing the adversary techniques, OT target assets and vulnerable systems with overarching adversary goals provides a common framework for all levels within an organisation to use in order to communicate risks. This taxonomy can be used by corporates as a checklist of cyber attacks to safeguard against, allowing for interesting dialogue around threats currently without mitigation.

Furthermore, the loss taxonomy provided aids in categorising the consequences to the organisation and its balance sheet from cyber attacks, allowing for comprehensive comparisons of which scenarios impact the business most. Again, the loss taxonomy can be used as a checklist when developing internal scenarios or estimating losses from external scenarios.

- **Cyber scenario stress-test development**

The Cambridge Centre for Risk Studies will soon publish its guidelines for developing stress-test scenarios, so please watch this space. Using scenario planning can help prioritise key cyber investments, as well as better understanding the loss estimation should cyber attacks occur. This is useful both for risk management (improving the predictive power of loss estimation) and for crisis response (mapping capabilities and needs during a cyber crisis). This paper summarises how to develop stress-test scenarios and highlights macroeconomic loss estimates for various scenarios developed at the Centre. These losses range from £49 billion for a UK-based power outage, to $4.5 trillion for the systemic failure of a key relational database software used extensively by corporates.

One recommended action is to initiate an internal multi-phased scenario. Phase 1 of the project would be to ensure that your business complies with relevant external cyber scenarios and, using the loss taxonomy provided, estimate losses. Phase 2 of this project would be to develop company-specific cyber scenarios with impacts estimated. Finally, in Phase 3 you would take the most impactful scenarios and schedule a role-playing exercise within your corporation, where staff members have to go through the motions of the cyber attack from the beginning until complete resolution. This is becoming common practice at the US Pentagon, which even organised a six-day event with electricity grid operators to role play a cyber attack on the electricity grid.

2) "Safety assurance of autonomy to support the Fourth Industrial Revolution", by Richard Hawkins and John McDermid from the Assuring Autonomy International Programme at the University of York.

With the advancement of 4IR robotics, and the challenges of assurance of these systems, especially cobots, the manufacturing sector needs to investigate how to safely adopt these technologies.

- **Assurance strategies and arguments**

  A critical challenge for adopting modern robotics, using ML, is how to assure them and to gain acceptance of the systems. A three-phase project, carried out across the sector, could help to address this problem; the project would be best carried out by a working group set up with representatives from a range of manufacturing organisations, covering the spectrum from small-scale specialist developers to the operators of large facilities. The first phase should review the RECOLL project to understand how this particular application of cobots has been assured. Second, the sector should produce sector-specific arguments for the assurance of cobots, and manufacturing robotics more generally, building on the AAIP BoK and template assurance arguments produced by the Assuring Autonomy International Programme. Third, the working group should identify the appropriate forms of evidence for supporting the arguments. If appropriate, this should be documented as an industrial guideline, noting that industry can move much faster than standards bodies.

- **Industrial best practice**

  The work on assurance would focus on gaining approval for 4IR products, but it would not address the development of such products. These developments will need extensive tool support, for example, for developing and testing the control software. As with the work on assurance, a working group could seek to define and document best practice for development. Here the working group should include developers and users of 4IR technologies, but also tool suppliers, especially those working in other safety-related sectors that are already addressing some of these problems. The aim would be to gain cross-sectoral requirements on development methods and to identify requirements for tools. This would both help the developers and users of cobots and other 4IR products, and also serve to stimulate the tools suppliers to develop more relevant products, by giving clearer requirements to work to. Considering the inclusion of groups at the interface between academia and industry, such as the Advanced Manufacturing Research Centre, will enable the working group to consider best practice across different equipment manufacturers and developers, providing a wide perspective.

- **Safety and security**

  Historically, techniques and methods for assessing safety and security have evolved independently, although, as noted, there is some work to be done on drawing the techniques together, including assessing the impact of security weaknesses and vulnerabilities on system safety. The sector could work together to provide practical and focused guidelines on assessing safety and security.

A valuable perspective is how to take safety and security into account early in the development life cycle when it is possible to make trade-offs between safety and security, in the context of the system being developed. This is a little-researched area, but it is important to managing safety and security in a cost-effective manner. Some early work on this topic might provide a useful starting point for a working group. This work might usefully be merged, in time, with both the development guidelines – to help in producing safe and secure systems – and the assurance strategies and arguments, to offer a basis for providing broadly based assurance in systems.

6.4 Suggested themes for collaborative pilot studies/projects

Based on the findings of the report, a number of potential pilot studies and activities have been identified that can help to bridge some of the key safety and security knowledge gaps in the deployment of 4IR technologies in manufacturing, as shown in Table 9. The end goal of these collaborative pilot studies would be to promote multi-stakeholder collaboration in the development of better know-how of safety and security risks across the 4IR technology spectrum.

Table 9 - Suggested themes for collaborative pilot studies/projects

NO.	PROJECTS	KEY TASKS/FOCUS AREAS
1	**Build a unified global knowledge database on 4IR safety and security**	- **Online resources and knowledge platforms**. Gather and consolidate key data on safety and security (e.g. risks, hazards, standards, norms, regulations, control measures, training material, manuals, guidelines, assessment tools). This could include **cyber threat and loss taxonomies and assurance strategies and arguments**, as discussed in Section 6.3. Accessing key information at low cost could be particularly useful to SMEs. - **Industrial surveys** covering global businesses from across manufacturing sectors could be publicly accessible through online platforms. This could provide a key resource to industry, regulators, researchers, governments and other relevant stakeholders regarding the main issues faced by manufacturers. - **Safety and security use cases**. A global online repository of use cases showcasing best practices to address the most common safety and security risks could be effective as a knowledge-sharing, open innovation mechanism
2	**Develop a unified vision of future 4IR safety and security risks, requirements and their interdependence**	- **Foresight**. Carry out joint studies to anticipate future firm-specific needs and better understand key safety and security risks and requirements as 4IR technologies become more prevalent in manufacturing environments. These could be used to inform research needs and the elaboration or revision of standards. - **Development of stress-test scenarios**. Simulate plans of action to ensure that firms are prepared to prevent, manage and/or respond to various types of emerging risk. These could help to prioritise investments and better understand key safety and security requirements (see Section 6.3).
3	**Create interest groups for safety/ security cross-cutting awareness-raising and information-sharing**	- **Forums and seminars**. Interested stakeholders could join forces to create forums where industry, regulators, researchers and government agencies could exchange ideas and coordinate small collaborative projects to, for example, promote the mapping, sharing and adoption of best practices. This could also include activities, communication campaigns and seminars whereby multinational companies provide SMEs with information about safety and security best practices (value-chain collaboration). - **Industrial readiness surveys**. Interest groups could develop industrial readiness surveys and self-assessment tools (based on purposely developed risk taxonomies and archetypes) for businesses to evaluate their safety and security vulnerability and risk profiles (e.g. for SMEs).
4	**Create industrial guidelines to in-form the development or updating of standards**	- **Industrial guidelines**. Given that standards tend to lag behind the pace of technology change, industry stakeholders could mobilise to create unified safety and security guidelines **based on the best available practices** across manufacturing firms and sectors (see Section 6.3). This could be provided to standard bodies as valuable input for the development or updating of standards, and it could also aim to unify standards for safety and security.
5	**Develop a 4IR-ready workforce**	- **Competency-development courses**. These could be developed for industry (from workers and managers to company directors and board members), regulators, researchers and policy-makers, on key topics such as design for safety, standards implementation and regulation compliance, based on a practical understanding of the risks and requirements for 4IR safety and security. Expert training providers could be used. - **Business-oriented education programmes**. These could be aimed at long-term research competence-building, to develop knowledge on how to safely and securely implement digital technologies across the entire value chain.

Appendix A: list of international initiatives

	INITIATIVE	ORGANISATION	TYPE OF ORGANISATION	DESCRIPTION
Frameworks, regulation and standards	**Cyber Exposure Data Schema v1.0**	Cambridge Centre for Risk Studies in collaboration with insurance industry organisations	Academia	Guidelines; cyber security insurance
	Industry 4.0 Standards / Standards Knowledge Graph	Fraunhofer IAIS	Academia	Mapping and database of key security and safety standards for Industry 4.0
	Cybersecurity Checklist when Using Outside Vendors	American Bar Association (ABA)	Industrial association	Checklist; vendor relationships
	Industrial Internet of Things: Safety and Security Protocol	World Economic Forum (WEF)	International	Framework; Internet of Things; insurance
	Recommendation on the Protection of Critical Information Infrastructures	Organisation for Economic Co-operation and Development (OECD)	International	Guidelines; national level
	A Security Approach for Protecting Converged IT and OT	Fortinet	Private	OT cyber security best practices; critical infrastrucutre
	Analysis of Semantic Specifications and Efficient generation of Requirements based Tests tool	GE	Private	Guidelines; safety critical infrastructure products
	CheckMe	Check Point	Private	Instant security assessment; simulation
	ICS Security Recommendations	SANS Institute – GE	Private	Guidelines; industrial control systems
	IoT/M2M Security Framework	Cisco	Private	Guidelines; Internet of Things
	Capabilities assessment for securing manufacturing industrial control systems. Cybersecurity for Manufacturing (First of four)	National Institute of Standards and Technology (NIST). US Department of Commerce	Public	Guidelines; anomaly detection and prevention capabilities
	CF Disclosure Guidance: Topic No. 2 (2011) Cybersecurity	US Securities and Exchange Commission	Public	Regulation; data breach notification regulation
	Common Criteria (CC) / ISO/IEC 15408	National security and standards organisations in Singapore, Canada, France, Germany, the Netherlands, the United Kingdom and the United States	Public	Security by design; IT products certification
	Critical Infrastructure Cyber Community C^3 Voluntary Program	National Institute of Standards and Technology (NIST). US Department of Commerce	Public	Support for the adoption of the NIST's Cyber Security Framework
	Critical Manufacturing Sector Cybersecurity Framework Implementation Guidance	National Institute of Standards and Technology (NIST). US Department of Commerce	Public	Guidance for the adoption of the NIST's Cyber Security Framework; critical manufacturing
	Defense Federal Acquisition Regulation Supplement (DFARS) minimum security standards & Self-assessment handbook	US Department of Defense	Public	Guidelines for public contractors

	INITIATIVE	ORGANISATION	TYPE OF ORGANISATION	DESCRIPTION
Frameworks, regulation and standards	**Framework for Improving Critical Infrastructure Cybersecurity**	National Institute of Standards and Technology (NIST). US Department of Commerce	Public	Standards, guidelines and best practices; critical infrastructure
	General Framework for Secure IoT Systems	Japanese Center of Incident Readiness and Strategy for Cybersecurity (NISC)	Public	Essential security requirements; Internet of Things
	Guide to Industrial Control Systems (ICS) Security (2015)	National Institute of Standards and Technology (NIST). US Department of Commerce	Public	Guidelines; industrial control systems
	Guidelines for Robotics Safety	US Occupational Safety and Health Administration (OSHA)	Public	Safety guidelines, robotics
	ICS Security Compendium	German Federal Office for Information Security (BSI)	Public	Compendium of standards
	Operational guidance for Cyber Security in relation to Industrial Automation and Control Systems (IACS)	UK Health and Safety Executive	Public	Guidelines; industrial automation and control systems
	OSHA Technical Manual (Chapter 4)	US Occupational Safety and Health Administration (OSHA)	Public	Safety guidelines, robotics
	Recommended practices in control systems	The US National Cybersecurity and Communications Integration Center (NCCIC)	Public	Best practices; cyber security for control systems
	Reference Architecture Model Industrie 4.0 (RAMI 4.0)	Platform Industrie 4.0	Public	Framework that facilitates the identification of relevant standards
	ErgoNoRA (Database of standards with ergonomic content)	KAN (German Commission for Occupational Health and Safety and Standardization) and DIN Software GmbH	Public–private	Database; standards with ergonomic content
	The Charter of Trust	Sixteen organisations and two government authorities, including: Siemens, IBM, Airbus, Cisco and Dell Technologies	Public–private	Baseline requirements; risk-based methodology; supply chains
	UK Government backed Cyber Essentials certification	UK National Cyber Security Centre in collaboration with Accreditation Bodies	Public–private	Public–private partnership certification; public contractors
	ARMOUR project	European Union (Horizon 2020 Programme)	Regional	Benchmarks, framework and certification; large-scale Internet of Things
	Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures	The European Union Agency for Network and Information Security (ENISA)	Regional	Guidelines; Internet of Things; critical information infrastructures
	Budapest Convention on Cybercrime	Council of Europe	Regional	Law enforcement; harmonisation of legislation
	EU Cybersecurity Act	European Parliament	Regional	Regulation framework

	INITIATIVE	ORGANISATION	TYPE OF ORGANISATION	DESCRIPTION
Frameworks, regulation and standards	**EU General Data Protection Regulation (GDPR) (2018)**	European Union	Regional	Regulation; data breach notification regulation
	Good Practices for Security of Internet of Things in the context of Smart Manufacturing	The European Union Agency for Network and Information Security (ENISA)	Regional	Good practices; Internet of Things
	Guidance on the application of the essential health and safety requirements on ergonomics	European Commission	Regional	Guidelines; EU; ergonomics
	Machinery Directive 2006/42/EC	European Commission	Regional	EU machinery legislation
	Online interactive Risk Assessment (OiRA)	The European Agency for Safety and Health at Work (EU-OSHA)	Regional	SMEs; web platform that for sectoral risk assessment
	IEC 61508 Functional Safety Standards	International Electrotechnical Commission (IEC)	Standards association	Standards; functional safety
	IEC/ISA–62443 Security for Industrial Automation and Control Systems (series)	American National Standards Institute/International Society of Automation (ANSI/ISA)	Standards association	Standards; industrial automation and control systems
	ISA-100 Wireless Systems for Automation (series)	International Society of Automation (ISA)	Standards association	Standards; wireless systems for automation
	ISA-101 Human-Machines Interfaces (in progress / series)	International Society of Automation (ISA)	Standards association	Standards; human–machine interfaces
	ISA84, Instrumented Systems to Achieve Functional Safety in the Process Industries (series)	American National Standards Institute/International Society of Automation (ANSI/ISA)	Standards association	Standards; functional safety
	ISASecure™ conformance certification program for industrial automation and control (IAC) products and systems	ISA Security Compliance Institute (ISCI)	Standards association	Private certification programme; industrial automation and control products and systems
	ISO 45000	International Organization for Standardization (ISO)	Standards association	Standard; occupational health and safety management systems
	ISO 10218	International Organization for Standardization (ISO)	Standards association	Safety requirements for industrial robots
	ISO/IEC 27001	International Organization for Standardization (ISO)	Standards association	Standard; cyber security
	ISO/TS 15066	International Organization for Standardization (ISO)	Standards association	Safety requirements for collaborative industrial robot systems

	INITIATIVE	ORGANISATION	TYPE OF ORGANISATION	DESCRIPTION
Awareness raising & sharing of information	**International Robot Safety Conference**	Robotics Industries Association	Industrial association	Conference; safety
	Go Safe Online	The Cyber Security Agency of Singapore (CSA)	Public	Cyber security awareness alliance
	Information Security Awareness Month (February 2011)	Japanese Center of Incident Readiness and Strategy for Cybersecurity (NISC)	Public	Annual information security campaign
	Information Sharing Partnership (CiSP)	UK Cyber Security Center	Public	Exchange cyber threat information; public–private partnership
	OSH events in Europe	European Agency for Safety and Health at Work (EU-OSHA)	Regional	Conference; safety
Skills development	**Robot Safety Training**	Robotics Industries Association	Industrial association	Training courses
	Customised specialised training in cyber security (TIC Defense Academy)	TIC Defense	Private	Customised training
	Memorandum of Understanding	Kaspersky Lab and Injazat Data Systems (Mubadala group)	Private	Expertise sharing; cyber security
	Siemens ProductCERT and Siemens CERT	Siemens	Private	Computer Emergency Response Team
	Training addressing safety and security industrial standards (functional safety, safety of machinery and embedded systems safety)	TÜV SÜD	Private	Training courses
	Master of Science Program in Cyber-Physical and Embedded Systems	IBM Research – Università della Svizzera italiana – Swiss Federal Institute of Technology in Zurich (ETHZ) – Politecnico di Milano (Italy)	Private–academia	Master's programme in cyber-physical and embedded systems
	Cyber Security Associates and Technologists (CSAT) Programme	The Cyber Security Agency of Singapore (CSA)	Public	Training programme
	ICS-CERT Virtual Learning Portal (VLP)	The US National Cybersecurity and Communications Integration Center's (NCCIC)	Public	Online training; industrial control systems
	SkillsFuture series	Singapore Future Economy Council	Public	Training courses with a lifelong learning approach
	US Initiative for Cybersecurity Education (NICE)	National Institute of Standards and Technology (NIST). US Department of Commerce	Public	Education, training, and workforce development; public–academia–private-sector partnership
	Cyber Security Body Of Knowledge	UK Cyber Security Center – University of Bristol	Public–academia	Skills development knowledge base
	Cyber Security Challenge UK	Cyber Security Challenge UK, not-for-profit organisation	Public–private	Competition on cyber security skills; public–private partnership
	Training for Cyber Security Specialists	European Union Agency for Network and Information Security (ENISA)	Regional	Online training material

	INITIATIVE	ORGANISATION	TYPE OF ORGANISATION	DESCRIPTION
Anticipation of risks and needs	**Potential Impacts of Industry 4.0 on Operators 3.0 and Tertiary Education in Safety Engineering (in progress)**	Occupational Safety Research Institute (VÚBP), public research institution founded by the Ministry of Labour and Social Affairs of the Czech Republic	Academia	Research in progress
	Foresight review on design for safety	Lloyd's Register Foundation	Non-profit	Foresight review
	CheckMe	Check Point	Private	Instant security assessment; simulation
	Delphi Survey: Digital Ergonomics 2025	German Federal Institute for Occupational Safety and Health (BAuA)	Public	Forecast study
	Simulation tools for the transformation in work conditions	French Agency for the Improvement of Working Conditions (Anact)	Public	Simulation tools (in French)
	Smart Industry Readiness Index	Singapore Economic Development Board (EDB) and TÜV SÜD	Public–private	Migration Industry 3.0–Industry 4.0
	CYBERSEC Brussels Leaders' Foresight 2019	European Cybersecurity Forum	Regional	High-level meeting
	European Survey of Enterprises on New and Emerging Risks (ESENER)	The European Agency for Safety and Health at Work (EU-OSHA)	Regional	Survey
	Foresight on new and emerging occupational safety and health risks associated with digitalisation by 2025	The European Agency for Safety and Health at Work (EU-OSHA)	Regional	Foresight study
	Occupational health consequences and challenges to Nordic health and safety regimes	Nordic Co-operation	Regional	Research in progress
Research and development	**Assuring Autonomy International Programme**	Lloyd's Register Foundation – University of York	Non-profit–academia	Demonstrator projects; safety; robotics and autonomous systems
	Networks attacks simulation	Fraunhofer Institute of Optronics, System Technologies and Image Exploitation (IOSB)	Academia	Simulation lab
	Academic Centres of Excellence in Cyber Security Research	UK Cyber Security Center and the Engineering and Physical Sciences Research Council (EPSRC)	Academia–public	Research centres
	AI for cybersecurity	IBM	Private	Cyber security AI technology solutions
	Honeywell Industrial Cyber Security Lab	Honeywell	Private	R&D; test and certification; training and collaboration
	IBM Employee Wellness and Safety Solution	IBM – North Star Bluescope Steel	Private	Wearable safety technology
	Industrial Security Lab (Beijing, China) and the Cyber Defense Center (Suzhou, China)	Siemens	Private	Research programme in industrial security; security monitoring and assessment services

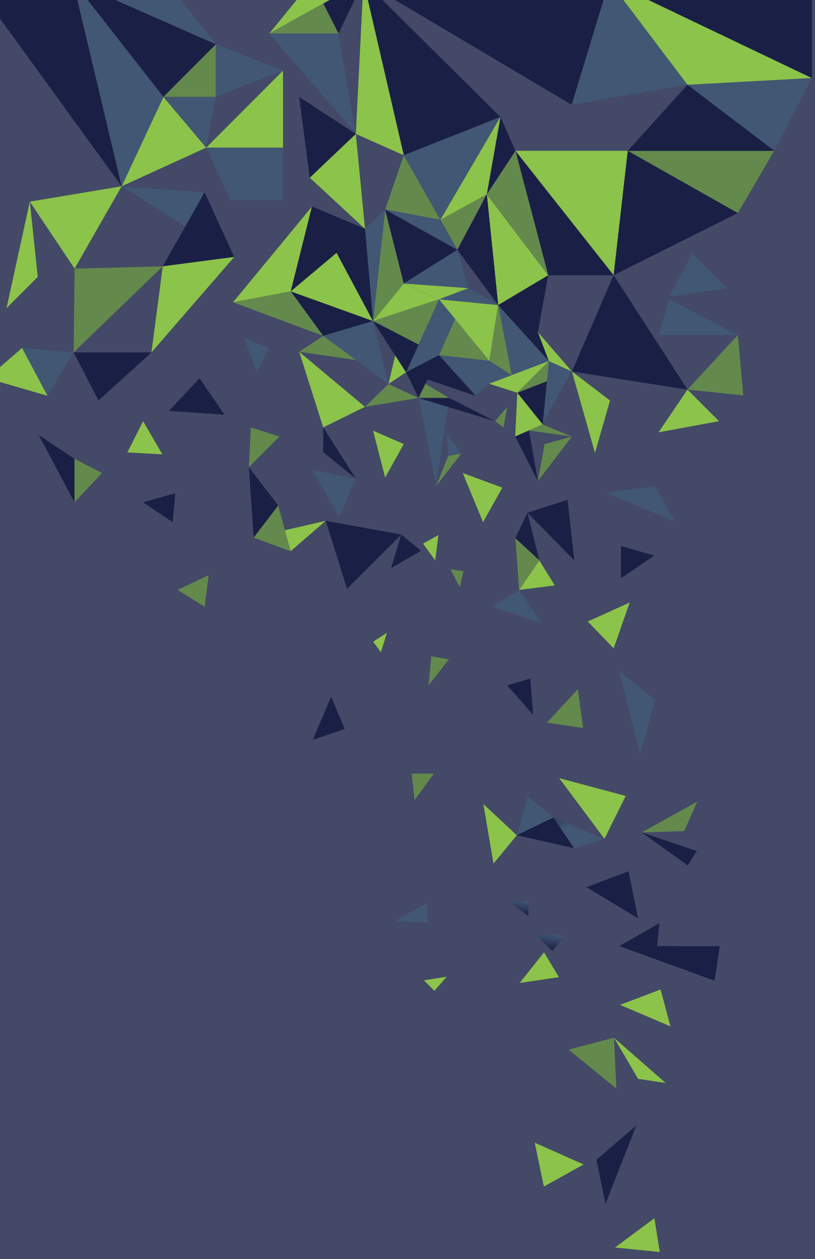
	INITIATIVE	ORGANISATION	TYPE OF ORGANISATION	DESCRIPTION
Research and development	**3D printing: Practical principles on product safety and regulatory framework (in German)**	German Federal Institute for Occupational Safety and Health (BAuA)	Public	Research (in German)
	Cyber protection technologies for critical infrastructure	GE in collaboration with the US Department of Energy and Defense Advanced Research Projects Agency (DARPA)	Public–private	Cyber security; critical infrastructure
	Risk-based automated assessment and testing for the cybersecurity certification and labelling of IoT devices	European Commission's Joint Research Centre (ARMOUR project)	Regional	Methodology proposal, IoT
Funding of co-innovation efforts	**Co-innovation and Development Proof-of-Concept Funding Scheme**	The Cyber Security Agency of Singapore (CSA)	Public	Funding for co-development of cyber security solutions between solution-providers and end-users
	Grants for advanced cybersecurity research team excellence	Spanish National Cybersecurity Institute (INCIBE)	Public	Development of researchers in cyber security
	Powered by AI: Health & safety for the manufacturing sector	UK Digital Catapult	Public	Workshop; co-innovation between start-ups and manufacturers
	The Cyber Security Small Business Program	Australian Cyber Security Centre – Council of Registered Ethical Security Testers Australia New Zealand (CREST ANZ)	Public	Funding for certified cyber security health checks; small business
	CyberInvest	UK Cyber Security Center and the Engineering and Physical Sciences Research Council (EPSRC)	Public–private–academia	Public–private partnership to invest in and support the development of cutting-edge cyber security research

About Policy Links

Policy Links is the knowledge exchange unit of the Centre for Science, Technology & Innovation Policy (CSTI), University of Cambridge. It aims to provide professional advice and education services grounded in the latest academic research to address the needs of policy officials and civil servants working in the areas of technology, manufacturing and innovation policy.

Policy Links is part of IfM ECS, a wholly owned subsidiary of the University of Cambridge. IfM ECS is embedded within the Institute for Manufacturing (IfM), a division of the University of Cambridge Engineering Department.

POLICY LINKS



Policy Links

Policy Links | IfM Education & Consultancy Services
University of Cambridge | 17 Charles Babbage Road | Cambridge CB3 0FS

+44(0)1223 766141 | www.ifm.eng.cam.ac.uk/services/policy-links

The safety and security dimensions of Industry 4.0 |

UNIVERSITY OF CAMBRIDGE

IfM Education and Consultancy Services

POLICY LINKS