Lloyd's Register
Foundation

Foresight review of cyber security for the Industrial IoT

Enabling safer more resilient infrastructures

July 2020

Lloyd's Register Foundation
Report Series: No.2020.1

About Lloyd’s Register Foundation

Our vision

Our vision is to be known worldwide as a leading supporter of engineering-related research, training and education, which 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.

Lloyd’s Register Foundation charitable mission

- To secure for the benefit of the community high technical standards of design, manufacture, construction, maintenance, operation and performance for the purpose of enhancing the safety of life and property at sea, on land and in the air.
- The advancement of public education including within the transportation industries and any other engineering and technological disciplines.

About the Lloyd’s Register Foundation Report Series

The aim of this Report Series is to openly disseminate information about the work that is being supported by Lloyd’s Register Foundation. It is hoped that these reports will provide insights for research, policy and business communities and inform wider debate in society about the engineering safety-related challenges being investigated by the Foundation.

Lloyd’s Register Foundation is a Registered Charity (Reg. no. 1145988) and
limited company (Reg. no. 7905861) registered in England and Wales,
and owner of Lloyd’s Register Group Limited.
Registered office: 71 Fenchurch Street, London EC3M 4BS, UK

T +44 20 7709 9166
E info@lrfoundation.org.uk
www.lrfoundation.org.uk

Contents

Executive summary 1

Foreword 4

Background 6

Report authors 7

Introduction to the Industrial Internet of Things 8

How industry is using the IoT 11

Drivers and possible IIoT futures 15

- Driver 1: Improving operational processes 15
- Driver 2: Green agenda 16
- Driver 3: Data markets 17
- Driver 4: Convenience and customer experience 18
- Emerging characteristics of the IIoT 18

The IIoT cyber-risk landscape 19

- Context 19
- Categories of risk in the IIoT 23

Current approaches to operational security and risk management 29

Operational cyber security for the IIoT: Capability gaps 33

- Risk assessment approaches 36
- Operational defence processes 36
- Human-centred recovery processes 37
- Defensive technologies 37
- Widening gaps in skills and awareness 38
- Interdependence of risk controls 39

Cyber security practice: Challenges for mindset, regulation and insurance 40

Mindset 40

Regulation 41

Cyber insurance 42

Strategic findings and recommendations 43

Looking ahead 44

Practical next steps for users of the IIoT 45

Further research and investigation 47

Call to action 51

Appendix A: References 52

Appendix B: Contributors 55

Appendix C: Glossary 57

Words underlined in the text are included in the glossary

Executive summary

The Internet of Things (IoT) is set to benefit society through a range of smart platforms and has been undergoing huge expansion; estimates vary but it is in the order of tens of billions of devices and growing rapidly. The focus of this review is the Industrial IoT (IIoT). IoT-enabled industrial control systems (ICS) are becoming a significant proportion of current and future critical infrastructures, with high uptake in areas like energy, transport, the built environment and manufacturing facilities. The consequences of failure can be high in these environments and so it is essential to understand how to deliver secure and resilient infrastructures. The IIoT exacerbates security challenges that already exist and poses new ones of its own. It is essential to prioritise action by identifying key emerging risks and gaps in capability.

The IoT is set to benefit society through a range of smart platforms and has been undergoing huge expansion

From a security standpoint, this review considers the IIoT to be comprised of three key parts: physical devices (especially including sensors), communications networks, and information and data, including associated software and hardware technologies for delivering processing and analytics.

Smart technologies facilitate new areas of innovation and new forms of control, enabling organisations to predict and manage the behaviours of their systems and environments. This review identifies four key forces driving adoption of IIoT technologies:

- Improving operational processes for safety, productivity, monitoring, efficiency, adaptability, risk management or other outcomes.
- The green agenda: optimised energy efficiency, proof of energy consumption, etc, whether in support of internal priorities or for external compliance.
- Data markets: whether to monetise proprietary data on open markets, or to create or expand internal processes and services.
- Convenience and customer experience: providing data-based customisation and external windows into real-time status will become increasingly valuable.

Together, these drivers contribute to emerging characteristics of the IIoT which, it is anticipated, will continue into the future:

- The scale of IIoT devices, networks and data is growing rapidly.
- IIoT systems within and across organisations and industries are becoming increasingly connected to each other.
- Industry and society are developing a critical reliance on IIoT systems and their smart functionality.
- Faster and more reliable communications between components of the IIoT are enabling new functionalities and interoperability.
- The dynamism and agility of systems and networks is increasing as a result of automation and software-definition.

As the IIoT advances, there will be greater potential for cyber harm, which will be more severe and potentially systemic as mission-critical systems are connected and automated. These challenges are particularly acute for industry and infrastructure providers, where there are strong economic and safety imperatives to keep core systems operational in all circumstances. In the IIoT future:

- Traditional cyber security risks evolve and scale up as the IIoT scales up.
- Interconnectedness creates shared and systemic risks.
- Risks may arise directly from data created by the IIoT.
- Emerging technologies, such as artificial intelligence (AI) and quantum computing, may create new risks.
- Industry-specific risks include likelihood of safety risk, unanticipated interaction between legacy systems, risk of contagion due to the small number of IIoT manufacturers, and risks related to the necessary evolution of training and culture to include IIoT.

The current pace of change in operational security capabilities will not match the fast emergence of new security risks in IIoT environments. At a conceptual level, existing security standards and guidelines are still relevant for the IIoT. At a practical level, however, the ability to deliver these capabilities, and the ways in which they must be delivered, are altered in the IIoT. Often capabilities do not scale, are not interoperable, are not technically feasible, do not exist yet, or are not tested. As an added complication, gaps in some key capabilities have consequences for other risk controls. There are widening gaps in skills and awareness. We are at a tipping point for recovery, as manual fall-back becomes infeasible for complicated systems-of-systems and mesh environments: the approach to recovery will need to change. There are also challenges for mindset, regulation and insurance, as we seek to promote improved security practice.

The analysis for this review indicates a need to adopt a set of guiding principles to increase the pace of operational cyber security change sufficiently. These seek to harden positions in the following ways: to "assume failure" as a basis for risk scenario planning, architecture and security strategy development; to "assume insider threat" within systems and supply chains; to "assume potential for systemic risk" and seek ways to identify and test for where it might manifest, and methods for limiting harm propagation.

This review identifies seven practical next steps for organisations using IIoT today. These are measures that should be considered when developing products and services for the near and far term: generally, organisations should seek to move from compliance- to outcomes-based risk management.

The review identifies an urgent need for further research and investigation aimed at understanding and evidencing risk control performance; study into liability models, practicalities and implications for IoT markets; and exploration of potential international cooperation to develop trust in the supply chain for IIoT devices and software. The report ends with a call to action to seek to support understanding of systemic risk potential in the IIoT, as this could have significant consequence for public safety and global economic wellbeing, and proof-of-concept cyber security demonstrators for emerging IIoT environments to ensure proliferation of best practice and capacity building around the globe.

Foreword

Today's industrial landscape would be unrecognisable to the safety experts who founded Lloyd's Register. Our highly interconnected and globalised industrial systems demand new safety approaches and those who design, operate and govern our new industrial landscapes must keep safety as a primary objective as we rapidly adopt new technologies.

While organisations have suffered cyber security breaches, we have not yet experienced wholesale devastation across cyberspace. No attack has resulted in a large-scale systemic failure, involving fundamental breakdown of technology and services, or complete loss of trust in infrastructure. Some believe this demonstrates inherent resilience across cyberspace: while there may be individual losers or victims (at every scale), our approaches to managing cyber risk are sufficient. This belief is unlikely to hold true in the future as we develop the Internet of Things (IoT). We will face significant challenges to delivering cyber security due to the difference in systems that the IoT will create.

Foresight in the field of cyber security is difficult because we must not only consider the relevant advances in technology, but also how they will potentially be used and attacked. This is especially true of the IoT, where the applications are growing exponentially, creating new digital ecosystems that might bring with them new types of possible attacks.

This report focuses on IoT-enabled industrial control systems that are aimed at a significant proportion of our future critical infrastructures, specifically energy, transport, the built environment and manufacturing facilities. The scope of IoT considered includes the technical components, as well as people and processes, that underpin the critical infrastructures on which society depends. The report’s observations and recommendations are generalisable across all nations regardless of wealth and likely to hold true for all Industrial IoT (IIoT) applications, to enable safer, more secure and more resilient infrastructures

The IoT is evolving rapidly and current cyber security approaches to attack prevention, detection and response are not fully translatable into this domain. This foresight review delineates the major challenges for operational cyber security in the IIoT context and suggests options for addressing capability gaps. The findings of this review are a call to action in support of the Lloyd's Register Foundation mission to engineer a safer world.

Sadie Creese
Professor of Cybersecurity
University of Oxford

Robert Hannigan
Chairman, BlueVoyant International

Professor Richard Clegg
Foundation Chief Executive
Lloyd’s Register Foundation

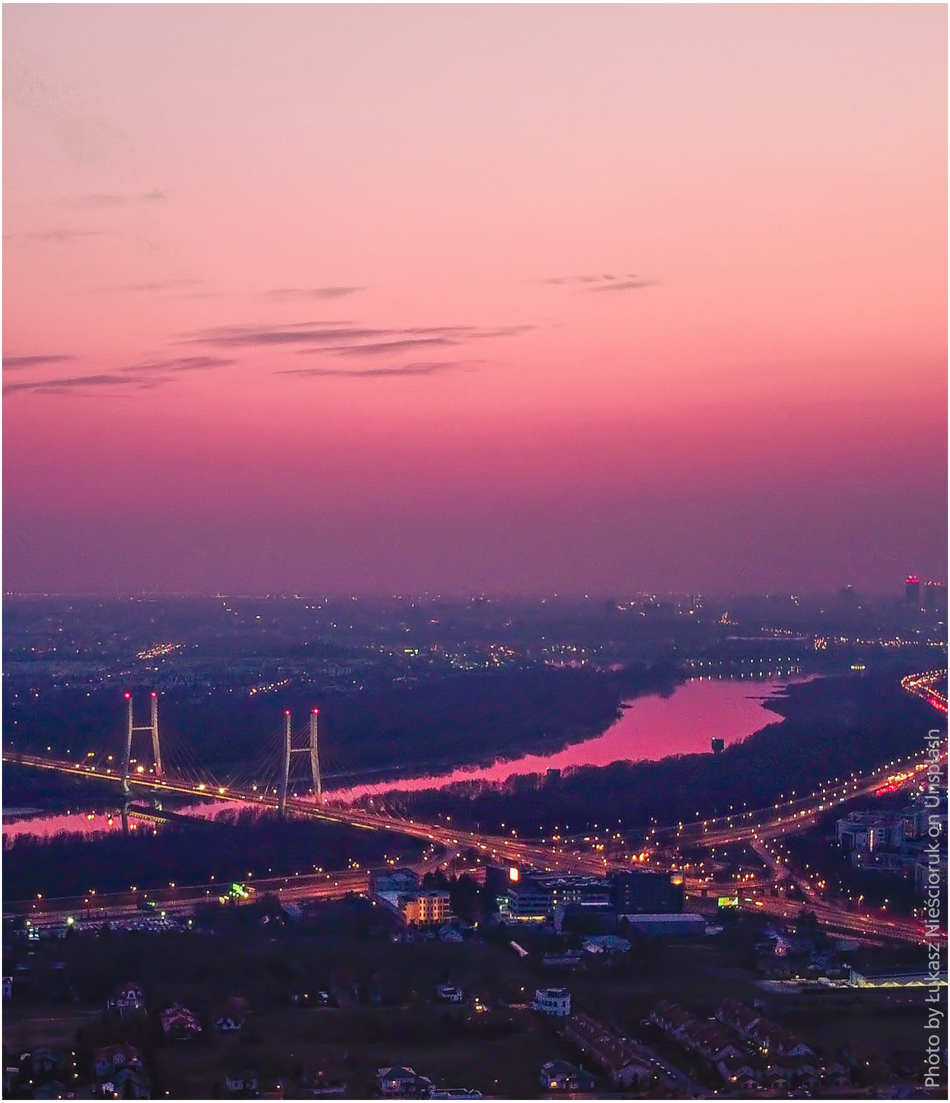


Photo by Łukasz Nieścioruk on Unsplash

Background

The purpose of this foresight review is to disseminate information, provide insight for decision-makers and researchers and inform wider debate, particularly focusing on the question: will current operational change in cyber security be enough? It presents both a long-term vision for key challenges, that the research and development communities will need to address, and also a view on the broader practical next steps that should be taken today to prepare for the immediate adoption of IoT technologies by industry.

Complexity will grow as key systems increasingly depend on smart or connected approaches to controlling work; exposing industrial processes, and the people who work with them, to greater risk. Therefore, the cyber security requirements of the Industrial Internet of Things must be identified now so that we better understand their vulnerabilities and are better educated and equipped to manage the associated risks. The review encompasses the technologies and socio-technical systems underlying the critical systems on which life depends, identifying requirements and response options to enable safer, more resilient infrastructures and enable safe and more secure innovation.

This review illustrates this by focusing on four sectors: energy, transport, the built environment and manufacturing facilities.

The findings and recommendations are built on a series of conversations and workshops, and literature review, from which key themes and issues were synthesised and considered for inclusion. Workshops were held in Singapore on 3 October 2019*, Oxford (UK) on 13 January 2020, and San Francisco (USA) on 25 February 2020. This process involved more than 110 contributors. Those who wished to be recognised are listed alphabetically in Appendix B. The authors thank all those listed and those opting not to be named in the report for their energy and thoughtful contributions to the production of the review. The authors are grateful for the support from the Cyber Security Agency of Singapore, Singapore Standards Council, Enterprise Singapore and Singapore Manufacturing Federation – Standards Development Organisation, and AXIS Capital in facilitating these workshops.

*The workshop was a sub-session of a Cyber Security Awareness and Standards workshop organised by the Singapore Manufacturing Federation – Standards Development Organisation, held as part of Singapore International Cyber Week 2019 (SICW 2019).

Report authors

Sadie Creese
Professor of Cybersecurity, Department of Computer Science, University of Oxford

Robert Hannigan
Chairman, BlueVoyant International; Director of GCHQ 2014-17

Ali El Kaafarani
Founder & CEO, PQShield

Louise Axon
Post-Doctoral Research Associate, Department of Computer Science, University of Oxford

Katherine Fletcher
Project Manager, and Coordinator of the Cyber Security Oxford network, University of Oxford

Eva Nagyfejeo
Research Fellow, Global Cyber Security Capacity Centre, University of Oxford

Arianna Schuler Scott
Doctoral Researcher, Centre for Doctoral Training in Cyber Security, University of Oxford

Marcel Stolz
Doctoral Researcher, Centre for Doctoral Training in Cyber Security, University of Oxford

Contributing rapporteurs

Mary Bispham
Matthew Rogers
Centre for Doctoral Training in Cyber Security, University of Oxford

Introduction to the Industrial Internet of Things

The Internet of Things (IoT*) is the network of technologies which interface and compute across the internet, largely without human intervention: it is often (but not always) a collection of small, low-powered devices designed to function as part of a coordinated system for data collection and analysis. It represents a massive instrumentisation of the world where computing devices, large and small, are pervasive and embedded throughout a wide variety of environments. This is not limited to the creation of new technologies, but also involves adding computing hardware and software to objects that previously did not have digital components. Importantly, to be part of the IoT, the digital components must connect to the internet. Often this adds a cyber element to something physical, resulting in a cyber-physical system. The functionality of the internet is already ubiquitous throughout work and social lives, and the IoT will bring about a closer coupling, where relationships between devices, software and people will vary greatly in density, time, space and automation.

The IoT is set to benefit society through a range of smart platforms and has been undergoing huge expansion; estimates vary but always the numbers of devices are large (tens of billions and growing rapidly). This review focuses on the Industrial IoT (IIoT); that is, the industrial applications of IoT technologies. Internet-enabled industrial control systems (ICS), which by nature tend to be physically larger than "traditional" IoT, as well as smaller devices (sometimes including consumer-grade IoT devices) are becoming a significant proportion of current and future critical infrastructures. IIoT often creates new bridges between information technology (IT) and operational technology (OT) – two areas which have traditionally been managed and regulated separately[1,2].

This report focuses on the IIoT because safety is critical in these environments and it is essential to understand how to deliver secure and resilient infrastructures. The 2020 World Economic Forum Global Risks Report put the short-term risk of cyber attack on infrastructure at over 76%[3].

This report focuses on the IIoT because safety is critical in these environments

The IIoT exacerbates security challenges that already exist and poses its own new challenges. It is essential to prioritise action by identifying key emerging risks and gaps in capability for which the current pace of change in operational cyber security (ie, the set of cyber security risk management processes) will not be sufficient.

To help pinpoint where risks emerge, this report conceptually divides the IIoT into three key parts, illustrated in figure 1 overleaf.

- Physical devices include sensors, which collect data from the physical world, and control components, which take actions in the physical world based on information communicated to them and computations they make.
- Communications networks which connect the devices to the internet and each other. These networks carry data for processing and analytics, and the information and control instructions that result. New communications technologies, in particular, the new 5G standard for cellular communications but also peer-to-peer technologies, are set to drastically improve mobile communications; the speed of communications and the volume of devices that can be connected will continue to grow sharply. It is anticipated that this will be a key advance in facilitating the scale-up of the IIoT.
- Information and data and the associated software and hardware technologies for delivering processing and analytics, both in cloud service environments and increasingly at edge-computing sites. Data is the main source of value in IIoT: key questions usually revolve around how and where data is collected and sent, and what insights or improvements can be gained by processing and learning from it. Therefore, other key technologies include AI/machine learning and big data analytics – new techniques in computer and data science which enable organisations to make sense of the vast quantities of data they are able to collect.

* This report is aimed at a non-specialist audience and important terms are defined as they are introduced but readers may find the glossary in Appendix C helpful for unfamiliar terms. All terms appearing in the glossary are underlined where they first appear in the report text.

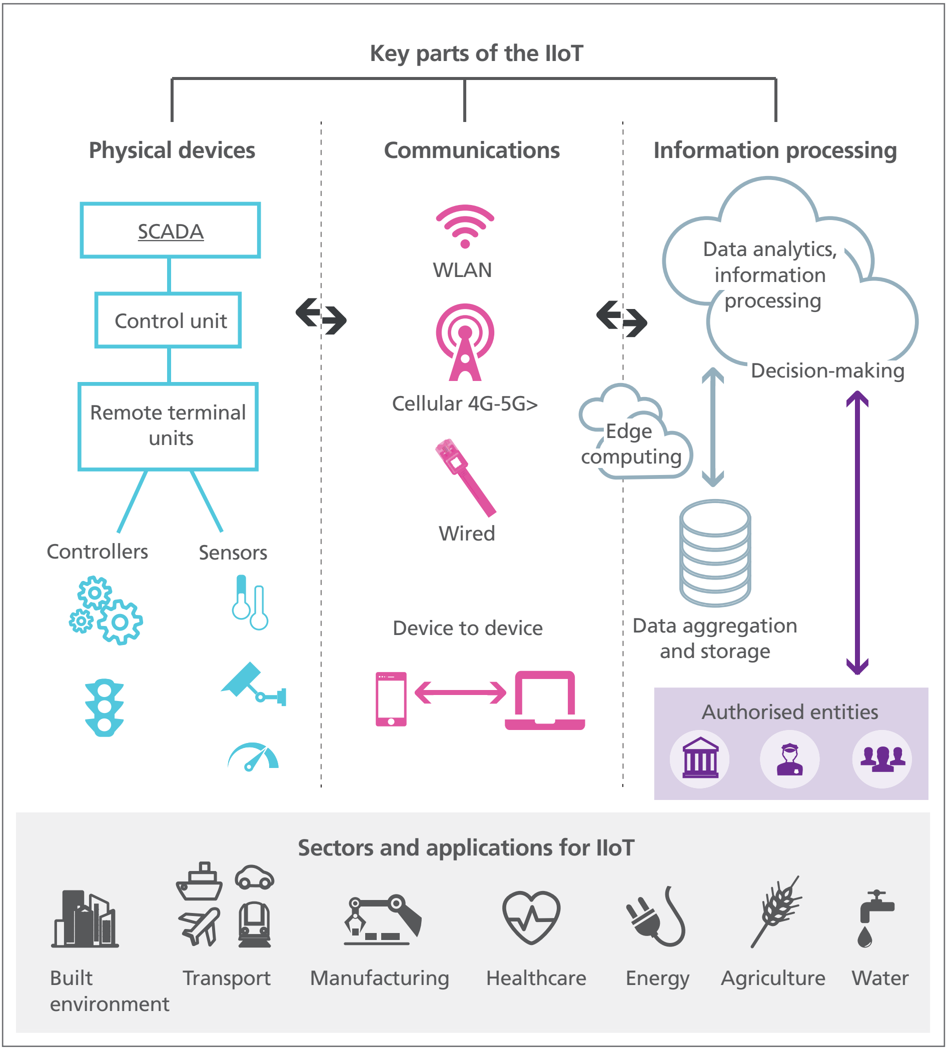


Figure 1: The three key parts of the IIoT in context

How industry is using the IoT

The addition of IoT enabled technology to industrial environments can help improve efficiency and safety in many ways; for example, through monitoring the state of equipment or processes, improved situational awareness, and minimising the need for humans in dangerous environments. IIoT technologies are being adopted in organisations and sectors across the economy. This review focuses on four sectors (transport, energy, the built environment and manufacturing facilities) for three reasons:

- There are many organisations within these sectors exploring IIoT use, so there is a wide variety of data to draw on.
- They provide a representative cross-section of challenges with widely applicable lessons.
- The sectors are relatively well-defined, with known key players, so focused efforts should make tangible progress.

Transport

The transport sector covers interconnected systems that allow people and goods to travel. Recent technology that enables this to happen includes autonomous or partially autonomous vehicles, human-controlled vehicles and the infrastructure supporting these vehicles. Increasingly this technology is connected to the internet through the IoT. Consider a smart port: gathering data about water and salt levels, wind, visibility and current can provide information that will help optimise mobility and improve safety of ships within the port and its environs, and eventually will also enable autonomous ships, cranes and lorries to load and unload cargo based on container contents, as illustrated in figure 2. Real-time location updates, tilt, temperature, humidity and other data can provide better visibility throughout the supply chain, potentially improving security, auditability, scheduling and safety.

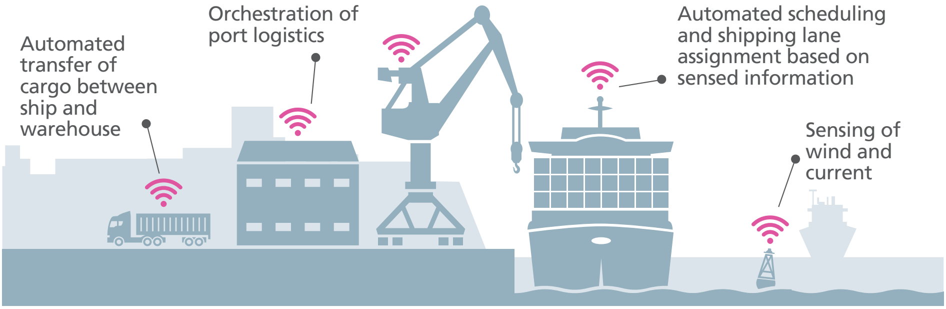

Automated transfer of cargo between ship and warehouse
Orchestration of port logistics
Automated scheduling and shipping lane assignment based on sensed information
Sensing of wind and current

Figure 2: IoT for a smart port

Energy

The energy sector covers interconnected systems that create, refine, manage, transport and deliver power. Smart grids (figure 3) are a key example of IIoT integration: they can manage energy distribution by collecting data and self-diagnosing issues, which establishes a baseline of operation that allows utility companies to continually assess and respond to network behaviour. The smart grid is a collection of technologies that perform several important roles: helping dynamically balance load and maintain continuous supply, while integrating unreliable renewable energy sources, supporting accurate billing and forecasting for system users and owners, and potentially enabling predictive maintenance or re-routing to maintain resilience of safety-critical electricity supply. By collecting data about how people use power, the smart grid enables more efficient energy distribution and planning.

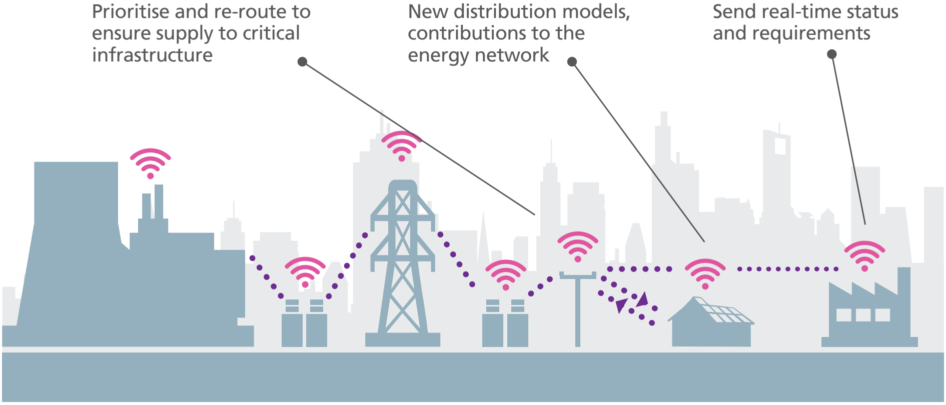

Prioritise and re-route to ensure supply to critical infrastructure
New distribution models, contributions to the energy network
Send real-time status and requirements

Figure 3: IoT for energy: optimising energy distribution from a variety of sources, according to usage and demand

The built environment

Larger scale city buildings, like car parks, hospitals or apartment blocks, incorporate sensors that measure a huge variety of data points including changes in temperature, humidity, strain, vibration, movement of people, vehicles or items, air quality, and consumption of resources such as energy, water and data (see figure 4). These data can be used to identify emerging maintenance or safety hazards, support cyber and physical security operations, and be shared with service providers to optimise and personalise offerings. They can also be used by the building management system to optimise resource consumption for the building as a whole, to manage and automate building-wide systems such as ventilation and heating, and enable the building to be integrated into its wider built environment (city, town, country).

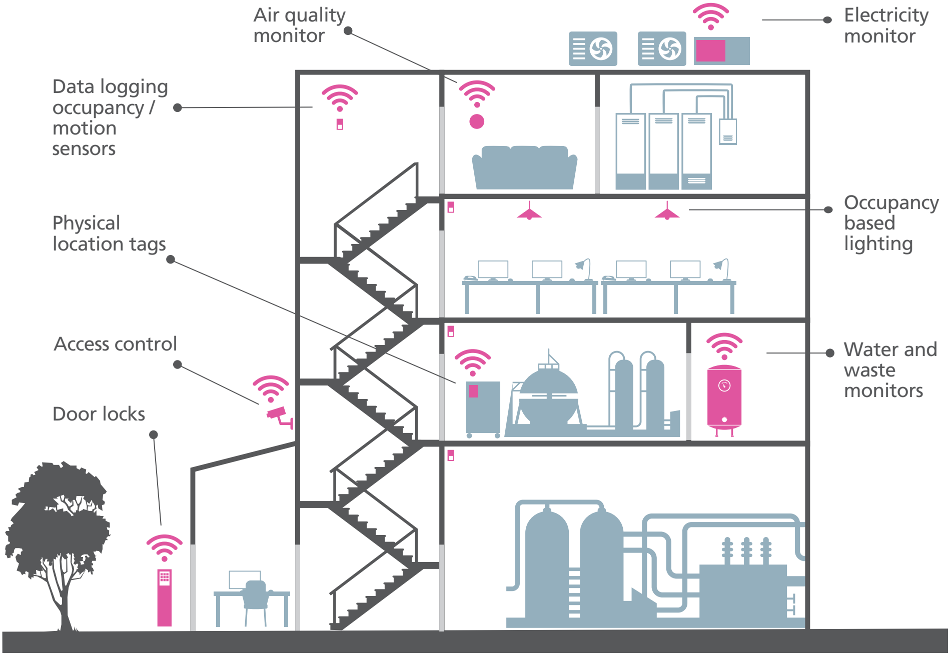


Figure 4: IoT for the built environment: sensor data can support maintenance, safety, security, ecological and other missions

Manufacturing facilities

Manufacturing environments, such as factories, use sets of interconnected systems to create products. IoT technologies are often seen as a natural evolution of existing IT- and OT-enabled processes, providing yet more detailed data on inventory, processes and equipment (see figure 5). IIoT can enable improved efficiency and safety through robotics and automation, as well as smart stock management, order processing and production cycle planning. Baseline operational data can help provide insights and allow unusual behaviour to be noticed and addressed.

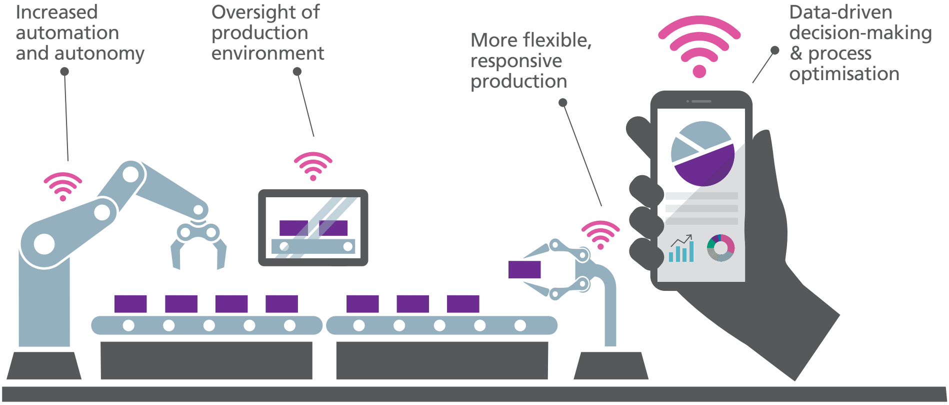

Increased automation and autonomy
Oversight of production environment
More flexible, responsive production
Data-driven decision-making & process optimisation

Figure 5: IoT for manufacturing

Drivers and possible IIoT futures

The IIoT offers the tantalising possibility of understanding and managing complex systems, both natural and human-made. Firms are motivated to invest in IIoT because smart technologies can facilitate new forms of control (enabling organisations to predict and manage the behaviours of their systems and environments, or demonstrate compliance) and new areas of innovation, in both service and product. The acceptable risks and cyber security safeguards may be different, depending on whether control or innovation is the priority, and successful use will need to take account of the main drivers of IIoT adoption since these are likely to shape how the environment evolves into the future.

This foresight review identifies four key drivers for adoption of IoT in industrial contexts, as set out below. Many of these drivers – or the technologies they push organisations to adopt – can also create risks, which are dealt with in the next section of this report. Here, the focus is on the motivating forces, as risk-management recommendations must account for why organisations believe they need these technologies.

Driver 1: Improving operational processes

Organisations investing in IIoT to improve operational process do so for a variety of reasons: to help maximise productivity, improve monitoring and reduce status uncertainty, reduce system and operational inefficiencies, create adaptability in the scale and scope of production (enabling resilience and risk management), de-risk supply chains, and enable predictive and remote maintenance (see figure 6 overleaf). IIoT investment can also be driven by national policy, whether to support national competitive advantage or to enable greater control and oversight of the critical national infrastructure.

These improvements are not always solely driven by the smart, automated capabilities of IoT systems, but also by the vast volumes of data, information and knowledge they create. These can support analytics which (semi or fully automatically) enable the identification of anomalies and opportunities for process improvement.

Improving safety in operational processes is a key consideration, especially in the industrial context. The IIoT offers the possibility of more effective safety monitoring, maintenance and earlier intervention (as in the use of IoT telemetry in the energy sector), auditable provenance (for example smart tags enabling inventory management and farm-to-table tracking), and the potential to reduce or replace humans in hazardous environments.

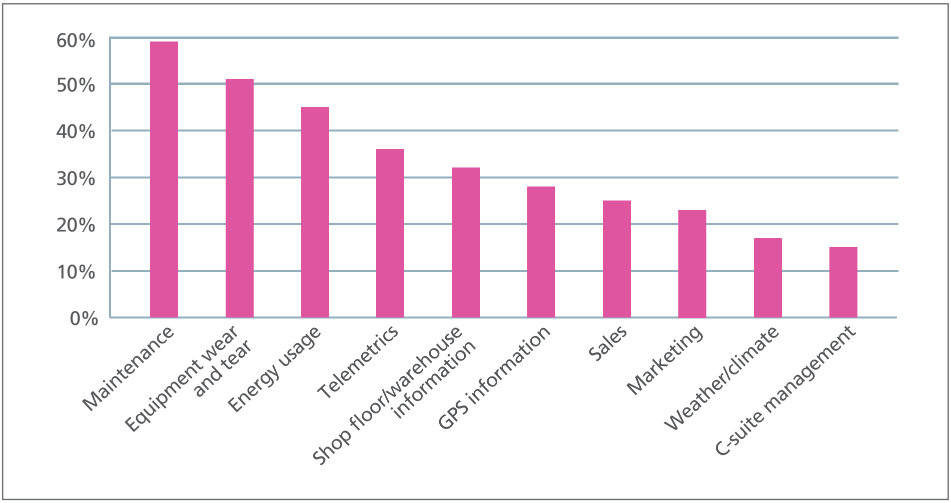


Figure 6: How firms use IIoT data[4]

Driver 2: Green agenda

With decarbonisation goals high on the global agenda and climate-action failure perceived to be a critical global risk, industry is increasingly looking to IIoT technologies to address environmental challenges. Instrumenting the physical world creates the opportunity to optimise energy efficiency and improve situational awareness of consumption. Examples of benefits include optimising transportation routes, reducing transport needs through local manufacture and remote maintenance, minimising the energy consumption and emissions of manufacturing processes, and decentralising energy generation and distribution models (where, for example, the solar panels of a household contribute to the energy network).

Many industries ask: “How will this support decarbonisation?” at every stage of the design process. Environmental responsibility is reinforced by economic pressures for companies to demonstrate “green” credentials as a competitive advantage, contractual or financing requirement. Monitoring, through smart instrumentation, also facilitates proof of energy efficiency for marketing and contractual purposes.

Driver 3: Data markets

Infrastructure providers, technology and transport companies have an opportunity to pivot towards becoming data companies. The vast amounts of data that the infrastructure produces, both as a target and by-product of IIoT activity, create data-centric economic opportunities. Infrastructure providers are likely to be in a unique position as suppliers of proprietary data streams which cannot be reverse-engineered or simulated and will have a wide range of uses in delivering more targeted products and services. Organisations may wish to learn from their data to improve and personalise products and applications, run data-driven services, or become data sellers. The value of data is magnified by the fact that the benefits and opportunities (for organisations, customers and communities) associated with the IIoT are enabled by this data: see for example Denmark's Open Data platform and The Green Button initiative run by data.gov in the United States. Overall, it is likely that organisations will pay increasing attention to the intellectual property generated by analysing IIoT data to create actionable and commercialisable information on business, processes and people.

Example: Open Data in Denmark

Denmark has established an Open Data platform (https://www.opendata.dk/) for municipalities to open their data, to improve transparency in administration, contribute to carbon emissions goals, and unlock collaborations and economic value. The city of Copenhagen also ran a pilot for universities, individuals and companies to share and sell a variety of data types, with plans to expand in 2020.

Driver 4: Convenience and customer experience

IIoT uptake and applications built on IIoT data are also driven by the potential to improve customer experience and convenience. For example, factories with contracts to fulfil can provide their customers information on production statistics and inventories, and offer consolidated shipping, automatic restock or other services. The convenience factor also drives the integration of IIoT into society: for example, the potential to enhance the accessibility and efficiency of travel through smart transport networks. As customers and suppliers come to expect the kinds of service and real-time information that are available with IoT instrumentisation, organisations will come under pressure to provide this information to win contracts.

Emerging characteristics of the IIoT

Together, these drivers contribute to emerging characteristics of the IIoT, which are anticipated to continue into the future:

- The scale of IIoT devices, networks and data is growing rapidly.
- IIoT systems within and across organisations and industries are becoming increasingly connected to each other.
- Industry and society are developing a critical reliance on IIoT systems and their smart functionality.
- Faster and more reliable communications between components of the IIoT are enabling new functionalities and interoperability.
- The dynamism and agility of systems is increasing as they incorporate a widening range of devices and networks can be created, grow, shrink and disappear without human intervention.

The IIoT cyber-risk landscape

Having discussed the driving forces and possible futures for industries adopting IoT technologies, the report now explores the risks. This section covers the context (what are risk, threat and harm, and how can they be determined) and a more detailed examination of various categories of risk. Some risks are related to the drivers discussed in the previous section, with new innovation creating new exposure to risk; some security threats are common to all internet-enabled devices, and these are briefly discussed. There is specific consideration of the structural features that make cyber security particularly difficult for providers of critical infrastructures.

Context

How do we define risk?

Risk is defined as being present if there is

- a threat existing in the environment (whether a human attacker or environmental factor), and
- an asset in the system with a vulnerability that can be exploited (also known as “attack surface”)

The risk is then qualified and quantified by assessing

- the likelihood that the risk will take place (whether in the form of an accident, or as the sequence of events that make up an attack), and
- the level of loss which would be experienced should the risk manifest.

Harm results from a single risk, or multiple risks, occurring.

The emerging characteristics of the IIoT, mentioned in the previous section, are altering, and will continue to alter, the cyber risk faced. They are changing the threat landscape, the attack surface, the set of risk-management approaches defenders can use, and the harms that may ensue from a cyber incident. Figure 7 overleaf illustrates how changes in each of these variables can affect risk.

The emerging characteristics of the IIoT are altering, and will continue to alter, the cyber risk faced

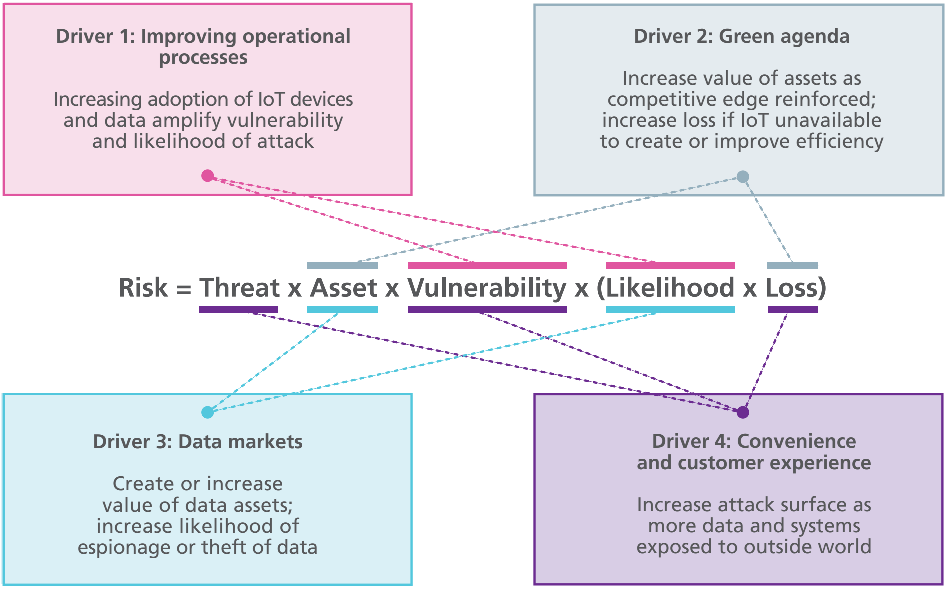

Driver 1: Improving operational processes
Increasing adoption of IoT devices and data amplify vulnerability and likelihood of attack
Driver 2: Green agenda
Increase value of assets as competitive edge reinforced; increase loss if IoT unavailable to create or improve efficiency
Risk = Threat x Asset x Vulnerability x (Likelihood x Loss)
Driver 3: Data markets
Create or increase value of data assets; increase likelihood of espionage or theft of data
Driver 4: Convenience and customer experience
Increase attack surface as more data and systems exposed to outside world

Figure 7: How the IIoT drivers are changing the cyber risk landscape

Threat and harm

Operational risk in an IIoT-enabled environment can result from accidents, errors, natural events and intentional attacks. Therefore, it is vital that organisations consider incidents, as well as accidents, when planning for resilience. These terms often overlap and are used differently in different contexts: the important distinction for the purposes of this report is that "accidents" do not include intentionality. Common feedback is that organisations tend to treat cyber security incidents as if they were accidents. As one workshop participant summarised it: "We don't consider: what if a person set out to make this happen?"

Security becomes an essential requirement for safety in the IIoT context. Attacks can take a wide variety of forms: distributed or targeted, performed by internal or external threat actors, active or passive, exploiting physical systems or software vulnerabilities.

It is anticipated that risk of deliberate attack will increase as the IIoT expands as cyber attackers, from criminals to nation states, seek to exploit newly connected systems and newly created vulnerabilities.

The harm that results from cyber incidents can also take a range of forms, including physical, economic, reputational, psychological and societal harm.

As the IIoT advances, there will be greater potential for cyber harm, which will be more severe and potentially systemic as crucial, essential systems are connected and automated. Figure 8 shows the most common point of entry for cyber attacks on enterprises in 2019, and figure 9 overleaf lists recent high-profile attacks which impact IIoT – some explicitly targeting industrial control systems and others indirectly (sometimes, possibly inadvertently) affecting IIoT-related functions. Taken together, they paint a picture where the routes of attack are widely distributed and, because malware can spread in unexpected ways, virtually impossible to completely defend against or predict. An attack that starts with a phishing email (31% of all enterprise attacks in 2019) could give attackers remote control of industrial control systems and also disable the IT backbone (BlackEnergy); an escaped piece of malware designed for one purpose could end up having drastic consequences in other environments (NotPetya) (both examples included in figure 9 overleaf).

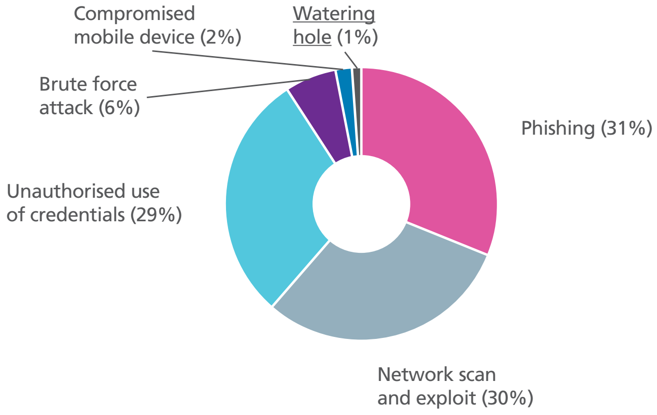
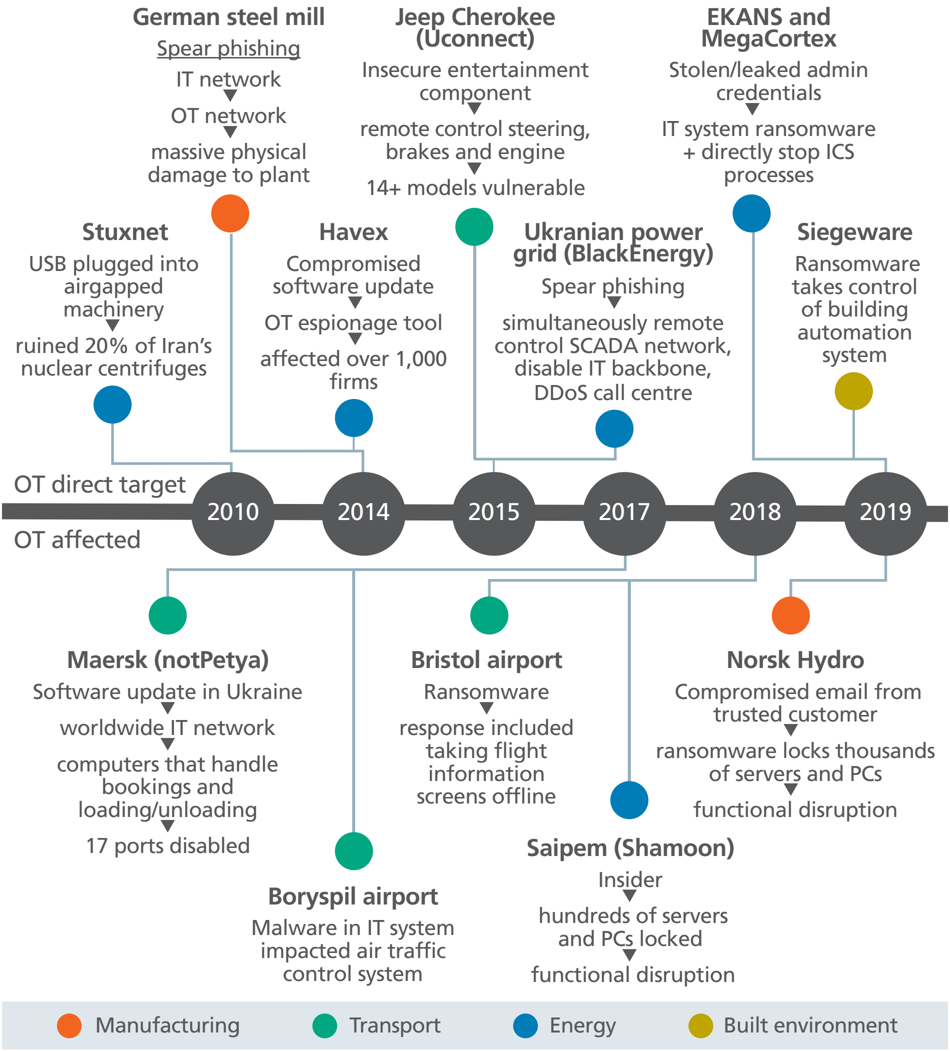


Figure 8: First point of entry for cyber attacks on enterprises in 2019[5]



German steel mill
Spear phishing
IT network ▼ OT network ▼ massive physical damage to plant

Jeep Cherokee (Uconnect)
Insecure entertainment component ▼ remote control steering, brakes and engine ▼ 14+ models vulnerable

EKANS and MegaCortex
Stolen/leaked admin credentials ▼ IT system ransomware + directly stop ICS processes

Stuxnet
USB plugged into airgapped machinery ▼ ruined 20% of Iran's nuclear centrifuges

Havex
Compromised software update ▼ OT espionage tool ▼ affected over 1,000 firms

Ukranian power grid (BlackEnergy)
Spear phishing ▼ simultaneously remote control SCADA network, disable IT backbone, DDoS call centre

Siegeware
Ransomware takes control of building automation system

OT direct target

2010 2014 2015 2017 2018 2019

OT affected

Maersk (notPetya)
Software update in Ukraine ▼ worldwide IT network ▼ computers that handle bookings and loading/unloading ▼ 17 ports disabled

Bristol airport
Ransomware ▼ response included taking flight information screens offline

Norsk Hydro
Compromised email from trusted customer ▼ ransomware locks thousands of servers and PCs ▼ functional disruption

Boryspil airport
Malware in IT system impacted air traffic control system

Saipem (Shamoon)
Insider ▼ hundreds of servers and PCs locked ▼ functional disruption

● Manufacturing ● Transport ● Energy ● Built environment

Figure 9: Examples of cyber attack affecting a range of systems that use IIoT

The special requirements of infrastructure providers

A key feature of industries included in this foresight review is that they often have an overwhelming priority to keep core systems operational. This can limit their range of defensive options and shapes their perception of what needs to be protected. Underlying this priority is an explicit economic case (downtime damages revenue or contracts) and often a safety or safety-adjacent case (people inside and outside the organisation rely on these systems being available). Legal and reputational issues are often perceived as secondary (safety aside). In the future, following the trajectory of the drivers described above, some organisations may pivot from being an infrastructure provider to a data firm, or a hybrid of the two: in this case, they will have a different range of concerns, such as preventing loss of intellectual property, and a different range of defence strategies.

Categories of risk in the IIoT

Traditional cyber security risks evolve and increase as the IIoT scales up

The risks common to traditional computing environments may expand in tandem with the large-scale adoption of IIoT due to the increased pace, scale, density, and variety of devices.

- **New technology creates expanding attack surface**. As devices are introduced and physical infrastructures changed, new attack surface is created. This can result from vulnerabilities in the technology itself, unexpected use of the technology creating attack surface in operational processes, or attack surface in humans resulting from their interaction with technology. All vulnerabilities when exploited can create further opportunities to compromise data and systems as attackers use these as platforms from which to pivot through systems.
- **Software-based attack surface.** As functions and communications are increasingly software based (through software-defined networks and virtualised network functions) there is a growing software-based attack surface in which vulnerabilities can be exploited. This could exacerbate the shortcomings of software-development and maintenance practice, which are often not sufficiently secure even in existing environments.
- **Malware attacks**. The number of malware attacks (ransomware, data exfiltration and sabotage, for example) will increase with the number of internet-connected and software-driven devices, with growing likelihood of cyber-physical impact.
- **"Hidden risk"**. There is a risk that insecure devices will be "hidden", or otherwise neglected, in the scale-up of connected systems. Security methodologies might miss devices which are intuitively classified as irrelevant (for example, a smart kettle in the canteen, or contractors' devices, might be used as an attack vector but neglected by the organisation's security review).

- **Continuous threat**. A constant connection to the threat vector (ie, the internet) is almost unavoidable and it may become infeasible to disconnect devices as a means of reducing an attack's impact. Perimeters may be hard to maintain.
- **Cyber-physical risk**. In the IIoT world, sensors and computers will be more localised and dispersed: it will be difficult (or impossible) to physically secure all endpoints against damage or tampering. Key cases in point are smart electricity grids (where smart meters, which could be considered critical national infrastructure, are distributed into individual homes) and 5G (where base stations are built into the urban environment).

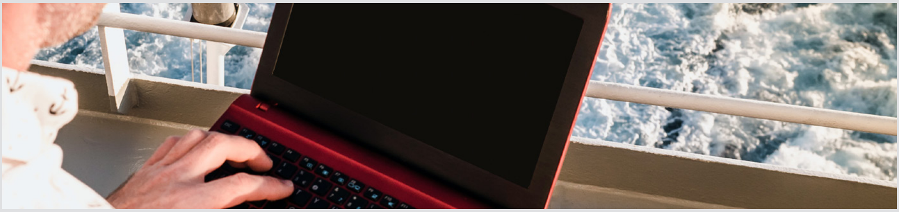
Interconnectedness creates shared and systemic risks

As industrial systems and their supply chains become interconnected, risks will increasingly be shared by organisations. Furthermore, the nature of systemic risks to industrial systems changes and the risk of widespread systemic failure may become more likely.

- **Risk of harm propagation**. As interoperability between organisations is used to improve efficiency and support new business models, their interconnectedness creates the risk that harms will propagate across critical industrial systems, with systemic societal impacts.
- **Unclear responsibility.** Deciding responsibility for applying operational cyber security measures becomes a challenge in distributed systems (in which ownership of assets and network segments is not necessarily clear cut). Deciding responsibility for the security of devices and services is also complicated as individuals and companies increasingly rely on service providers. These factors may prevent adequate security measures being taken.

Example: cruise ship

A new ship was designed with a careful consideration of cyber security. Even the resistance factors of Ethernet cables was specified. However, the ship was returned for repair within few months as the Ethernet cables needed replacing. The crew had stripped the wires and sold them, and replaced them with copper wires. The crew were oblivious to the risk they were creating for themselves and their passengers by doing this.



- **Supply-chain risk**. Supply-chain dependence will further increase the risk introduced by specific components. As the density of IIoT devices and connections develops, mapping, monitoring or mitigating supply-chain risks will become increasingly difficult: it may be difficult to tell what is "in" or "out" of the supply chain (for example, vehicles which are not currently carrying your goods) or to ensure the provenance of IoT devices, which include components from multiple vendors.
- **Exposure to upstream and downstream risk**. The upstream or downstream data flow might not be under an organisation's control (either technically or contractually) but the organisation will still be exposed to resultant risks. This may present as an availability risk (for example an attack on an internet service provider knocks client devices offline), but could equally include risks resulting from how downstream organisations use or secure their portions of the industrial ecosystem.
- **Shared ownership**. Manufacturers and customers share risk and ownership of data. Contracts increasingly relate to the provision of services, or licensed use of data, rather than defining straightforward data ownership. The emerging risks can be shared at many levels, including business, individual, societal, community, or national.
- **Exposure to risk through users**. Users of devices can expose the device owner, or even manufacturer, to risk. Security measures may be circumvented, ignored or removed by users. Data sources might become compromised, or organisations might be subject to liability for failed components. This can also lead to (or result from) unclear attribution of fault – for example whether law enforcement or insurers ascribe an incident to a person (insider) working with the victim organisation who accidentally introduces malware into the system, a criminal attempting to insert the malware into the system, or a technical fault (for example, algorithmic bias or manufacturer's default) within an IoT environment. Where IoT devices have human-user interfaces, the humans can become targets, which could introduce attack surface into areas where it would not previously have been considered.
- **Enslaved IoT**. There is the risk that botnets made of compromised IoT devices could be coordinated in highly distributed attacks and used to create much greater harm. Far larger botnets will be achievable, simply due to the numbers of devices available for enslavement, and these new IoT botnets will be extremely difficult to defend against. Should significant damage arise from such IoT-powered botnets, then legal liability of device owners and manufacturers is likely to become a focus for risk control.

Risks arise from data created by the IIoT

The increase in the data volume produced by IIoT systems and communications creates significant data risk.

- **Malicious use of data**. As the control of critical IIoT functions increasingly relies on data-driven automated decision-making, the risk posed by potential data corruption becomes increasingly severe. Corruption or manipulation of data used to train machine learning algorithms, for example, could enable attackers to sabotage systems or alter critical system functionality.
- **Risk of data breach**. Data breach may become increasingly prevalent as data, from personal data to national security information, is collected and shared – data that is both valuable to attackers and potentially highly sensitive for individuals, companies and states.
- **Impact of data breach**. Data breaches will also lead to increasingly negative impacts. The EU's General Data Protection Regulation (GDPR) and other emerging data-protection regulations add a financial component to the risk for organisations, leading to fines in the event of a serious data breach. The loss or leakage of data (including client data) also risks harming an organisation's reputation and the potential to use leaked data for espionage could damage competitive edge for organisations, for example through exposure of intellectual property or business intentions.
- **Availability of data**. As devices and human decision-making increasingly rely on data, its availability becomes more important. The risk could be through not enough data (for example attacks which stop devices sending telemetry back), or through too much (in the case of denial of service attacks which overwhelm a system with more data than it was designed to handle).
- **Privacy.** Organisations may find that they are collecting and processing data which relates to individuals (location, consumption, IP addresses, etc). This could result in relatively straightforward (but possibly burdensome) regulatory compliance, but also reputational risk or loss of business if employees or customers become concerned by how this is handled.

Photo by chuttersnap on Unsplash

Risks emerge that are specific to the industrial context

The functionalities and interactions of industrial systems, and the operational processes carried out in the industrial context, create a specific set of risk management considerations in the IIoT.

- **Safety risk**. As safety- and security-critical functionalities are implemented together (for example, IoT-enabled access control on a door to a power plant control room, or security settings on an internet-connected temperature control for a smelting furnace) there is increasing potential for cyber attacks to result in safety incidents. Security becomes essential to ensuring safety.
- **Legacy system risk**. Industrial SCADA (Supervisory Control and Data Acquisition) systems often remain in use for 20 years or more – long after original manufacturers have ceased to support them. Legacy systems, which were not designed for IIoT environments and lack security protection, are being increasingly linked to IT and/or IoT networks, creating risk.
- **Risk of contagion**. There is a potential risk of contagion, given the small number of IIoT device and component manufacturers compared to the number of users, and the relatively limited options for communication protocols. Vulnerabilities in widely used device types or software could affect systems across large swathes of society and industry: this risk bottleneck is clear in examples like Spectre and Meltdown (hardware vulnerability affecting nearly all device types), Heartbleed (software vulnerability affecting millions of web servers), and URGENT/11 (TCP/IP stack vulnerability affecting billions of devices).
- **Human risk**. Human organisational systems (sometimes called human factors) are a generic security risk, but this has specific meaning in the industrial context as these organisations are likely to have entrenched training and culture. In newly connected industrial environments, personnel without cyber security experience (for example, OT specialists) are being brought into the cyber security arena, and organisations may face risk as a result of inexperience or lack of coordination between safety and security experts.

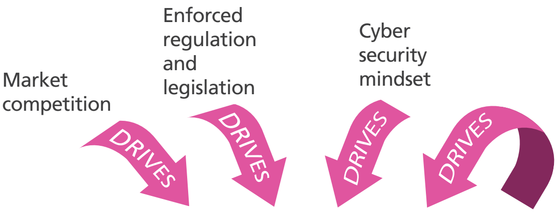
Emerging technologies create new risks

- **Quantum computing**. In the future, when sufficiently powerful quantum computers are built, adversaries will be able to dissolve the public-key cryptography relied on in many fundamental digital applications, including the cryptographic techniques fundamental to securing the IIoT, both in hardware and software. Recent promising advancements in quantum computing show that such a powerful machine could be built in the near future. Given the long lifecycle and/or lasting confidentiality requirements of many IIoT systems, quantum computing poses a serious risk that must be mitigated by using quantum-resistant cryptographic techniques.

- **AI and machine learning**. These technologies are already a common tool for cyber defence, for example using complex pattern-analysis to detect attacks and automate responses. Attackers are likely to take advantage of ongoing developments in AI and machine learning techniques to build more powerful cyber-attack capabilities as well. For example, AI can be used to orchestrate more effective botnet attacks, predict passwords, and speed up the process of finding software vulnerabilities and generating code to exploit those vulnerabilities. Adversarial learning may also enable adversaries to exploit weaknesses in AI processes themselves or contribute to overarching strategy changes.
- **The shared infrastructure of upcoming 5G cellular communications** creates shared risk, as well as the potential for systemic disruption. This may be particularly true where elements of security are outsourced to the 5G network by industry.

Current approaches to operational security and risk management

Cyber security risk is usually considered in terms of the confidentiality, integrity and availability (CIA) of the technological components of the operational environment: systems and data. The basis of existing cyber security risk management practice is illustrated in figure 10. Risks are controlled through technologies and processes, and transferred or shared through cyber insurance, with the aim of enabling five key areas of operational security. The adoption of risk controls and secure practice are driven by regulation and legislation, market competition (including contractual requirements and security as a competitive edge), cyber security mindset within organisations aiming to mitigate the harmful effects of a potential cyber incident, and the requirements of cyber insurance providers.



		Risk control		Risk transfer
		Technologies	Processes	Insurance
Identify	Manage cyber security risk to systems, people, assets, data and capabilities	▨	▨	
Protect	Ensure delivery of critical infrastructure services	▨	▨	
Detect	Identify the occurrence of a cyber security event	▨	▨	
Respond	Take action regarding a detected cyber security incident	▨	▨	▨
Recover	Maintain plans for resilience and restore any capabilities or services that were impaired	▨	▨	▨

Figure 10: The relationship of risk controls to operational security (defined in terms of the NIST CSF 5: Identify, detect, protect, respond and recover)

Various international standards, industry best practices and frameworks, capture cyber security risk assessment and management approaches and recommendations for how to prioritise risk controls within a system. Key examples are the Cyber Security Framework from the US National Institute of Standards and Technology (NIST CSF)[6], the Center for Internet Security (CIS) Critical Security Controls (CSCs)[7], the ISO 27001 security standard[8], the UK National Cyber Security Centre's Cyber Essentials guidance aimed at small and medium-sized enterprises[9], and best-practice guidelines on risk management for the IIoT specifically, such as those provided by the Industrial Internet Consortium[10, 11], ENISA[12], and the IoT Security Institute[13]. The Industrial Internet Consortium's IoT Security Maturity Model[10] seeks to provide a starting place for security investment decisions. There are also emerging best practices around establishing trustworthiness for devices and systems, for example the Industrial Internet Consortium's efforts in this area and NIST guidance for IoT device manufacturers[14, 15].

While these standards and best practice guides differ, they all share commonalities and a subset of risk controls, either explicitly or by implication. These are the key classes of risk control that are widely agreed on by experts, practitioners and researchers as being essential to addressing cyber security risk. Figure 11 is a simplified example of how this fits together, showing where common classes of risk control could be applied to the IIoT schematic from figure 1.

Some other classes of risk control, that are critical to the protection of IIoT environments as a whole, include regular risk assessment and assurance activity (penetration tests, for example); the monitoring and analysis of logs of activity across systems; and the development and exercising of incident-response plans and plans for the continuity of operations. These are not represented in the diagram but should be viewed as essential in every organisation involved in the IIoT.

As figure 11 shows, deployment of risk controls in the IIoT is potentially quite complex and the interdependency of these risk controls (as shown in figure 12 overleaf) simply adds to this complexity. However, certain classes of control (such as device inventories and log monitoring) are critical in that a large majority of other classes of control are dependent on them, meaning that risk management is even more difficult to orchestrate in reality.

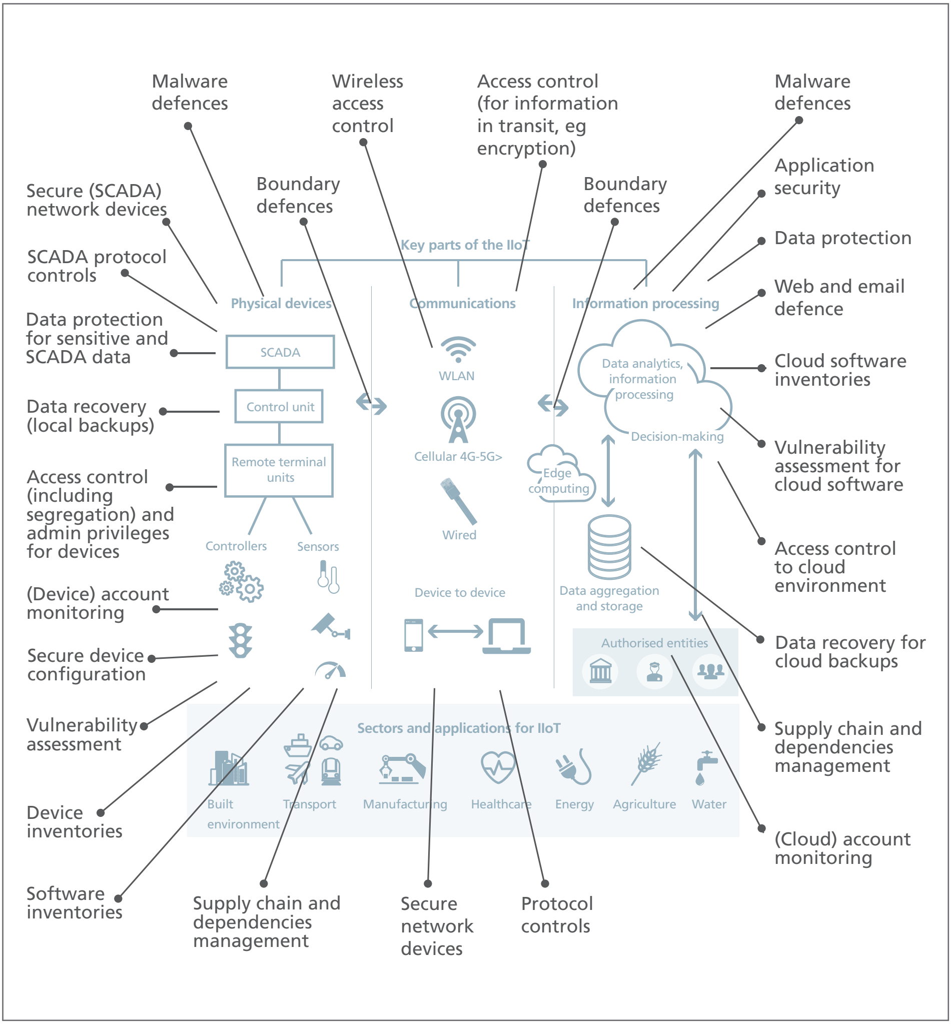

Malware defences
Wireless access control
Access control (for information in transit, eg encryption)
Malware defences
Secure (SCADA) network devices
Boundary defences
Boundary defences
Application security
SCADA protocol controls
Key parts of the IIoT
Data protection
Physical devices
Communications
Information processing
Web and email defence
Data protection for sensitive and SCADA data
SCADA
WLAN
Data analytics, information processing
Cloud software inventories
Data recovery (local backups)
Control unit
Cellular 4G-5G>
Decision-making
Edge computing
Vulnerability assessment for cloud software
Remote terminal units
Wired
Access control (including segregation) and admin privileges for devices
Controllers
Sensors
Access control to cloud environment
Data aggregation and storage
(Device) account monitoring
Device to device
Authorised entities
Data recovery for cloud backups
Secure device configuration
Vulnerability assessment
Sectors and applications for IIoT
Supply chain and dependencies management
Built environment
Transport
Manufacturing
Healthcare
Energy
Agriculture
Water
Device inventories
(Cloud) account monitoring
Software inventories
Supply chain and dependencies management
Secure network devices
Protocol controls

Figure 11: The deployment of widely recommended classes of cyber security risk controls in the IIoT

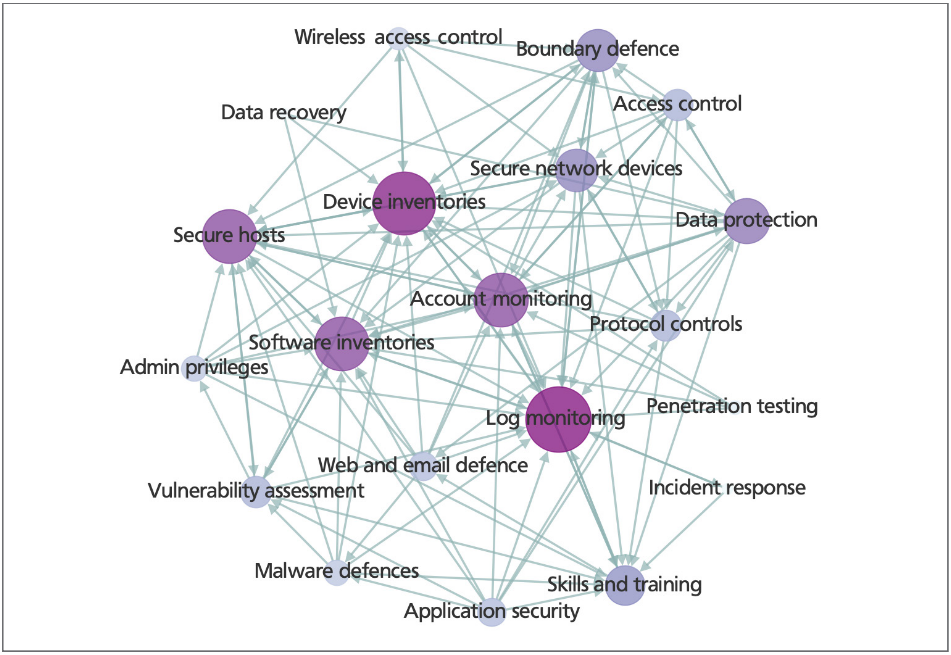


Figure 12: Map of dependencies between risk controls (adapted from prior work[16]). The arrow source is at the dependent control. Node colour and size represent the degree to which a control is depended on by others.

The management of cyber security risk for traditional systems already faces many challenges. These include the sheer difficulty of trying to map the complicated relationships between technical and human systems, and the challenges of communication between different communities where the frameworks for understanding risk are fundamentally different (for example, operations and board members, companies and regulators, procurement and cyber security teams). There will be vast differences between organisations and between teams within organisations: how they are trained, how they react in a crisis, which people and systems they trust, etc. Many of these existing challenges[17] will remain and be exacerbated, and new ones will arise, as risk-management approaches are translated into the IIoT, creating key capability gaps.

Operational cyber security for the IIoT: Capability gaps

The IIoT can simultaneously enable progress and increase operational risk. It is important to get the balance right, with organisations making properly informed decisions based on a realistic understanding of risk and a clearly articulated appetite for risk: as the smart road network example below shows, lack of clarity on either point can lead to missed opportunities and wasted investment.

Current approaches to operational security and risk management, which have been developed across years in traditional IT environments, may not translate effectively as they are taken up by industries that, traditionally, have achieved a level of cyber security through not connecting many of their systems to the internet. Historically this disconnection was referred to as the air gap, meaning that there was no direct digital connection. However, in recent years this has been questioned as a method for providing security, as humans and mobile data storage devices are often used to connect said systems, which removes (if only for a short time) the gap. The truth is that the current pace of change in operational capabilities will not match the fast emergence of new security risks in IIoT environments.

At a conceptual level, the operational-security and risk-management outcomes described by existing security standards and guidelines are still relevant for the IIoT. At a practical level, however, achieving these outcomes is difficult for a number of reasons: capabilities do not scale, are not interoperable, are not technically feasible, do not exist yet, or are not tested – and competing incentives in evolving relationships can compound the difficulty. Table 1, overleaf, presents the capability gaps. The main issues emerging from this analysis are considered on pages 36-39.

Example: Smart road network
Road tunnels can be heavily dependent on IoT sensors and IoT-enabled signalling to drivers, to control traffic flows in real time. For one high-traffic tunnel, cyber security concerns were raised about what might happen if these systems were hacked. As a result, the tunnel was effectively disconnected and manual control reasserted, which impacted performance and brought its own safety risks (as well as wasting the budget spent on equipping the tunnel). There was a huge skills and understanding gap that fed a tendency to risk aversion.

Photo by Burak K from Pexels

Table 1: Operational security capability gaps

	What's broken?	Can it be addressed?
Identify		
Identifying network components/ mapping connections	• Best practice does not scale • Competing incentives in evolving relationships	
Device naming conventions	• Lack of interoperability across IoT subsystems •Best practice does not scale	
Identifying and protecting reputation-as-asset		• Emerging approaches, insufficiently tested
Establishing ownership and responsibility for network components		• Emerging approaches, insufficiently tested
Risk assessment/risk management strategy, especially blending IT and OT	• Lack of interoperability across IoT subsystems	• May be amenable to technical solution
Assurance techniques (penetration testing, vulnerability scanning, etc)		• May be amenable to technical solution
Supply chain risk management (whether for intangibles, like software-as-a-service, or physical components)	• Best practice does not scale • Competing incentives in evolving relationships	• Emerging approaches, insufficiently tested
Protect		
Identity management and access control	• Best practice does not scale	• Emerging approaches, insufficiently tested
Awareness and training	• Lack of interoperability across IoT subsystems	• Emerging approaches, insufficiently tested • May be amenable to technical solution
Data security	• Best practice does not scale • Competing incentives in evolving relationships	
Information protection processes and procedures	• Lack of interoperability across IoT subsystems • Best practice does not scale	• May be amenable to technical solution
Maintenance of systems and components	• Lack of interoperability across IoT subsystems	• May be amenable to technical solution

	What's broken?	Can it be addressed?
Protect continued		
Protective technology	• Lack of interoperability across IoT subsystems	• Emerging approaches, insufficiently tested • May be amenable to technical solution • Not technically feasible*
Boundary defence	• Lack of interoperability across IoT subsystems	• May be amenable to technical solution
Detect		
Anomalies and events/detection processes	• Lack of interoperability across IoT subsystems • Best practice does not scale	• Emerging approaches, insufficiently tested • May be amenable to technical solution
Security continuous monitoring	• Lack of interoperability across IoT subsystems • Best practice does not scale	• May be amenable to technical solution
Respond		
Response communications (reporting)	• Best practice does not scale • Competing incentives in evolving relationships	• Emerging approaches, insufficiently tested
Planning and mitigation	• Best practice does not scale	• Emerging approaches, insufficiently tested
Analysis of incidents	• Best practice does not scale	• May be amenable to technical solution
Recover		
Recovery planning and improvements	• Lack of interoperability across IoT subsystems • Best practice does not scale	• Emerging approaches, insufficiently tested • May be amenable to technical solution
Fall back to "dumb" system		• Not technically feasible
Recovery communications (eg PR)	• Best practice does not scale	• May be amenable to technical solution

* Some current technologies may be infeasible on low-powered devices

Risk assessment approaches

Existing risk assessment methodologies were established prior to the development of the IIoT and are unlikely to cope with the complexity, dynamism and pervasiveness of this automated system of systems. While current approaches require identification of the assets to be protected and the scope of the system, identifying the scope and boundaries of complex IIoT systems will be increasingly challenging, and furthermore the dynamism of IIoT environments will mean that static snapshots could very quickly become out of date. If organisations use current static risk-assessment methods for the IIoT, it could leave them blind to new risks arising in this ecosystem: there is a need for more dynamic monitoring of risk through real-time data.

There is a need for a collective shift away from compliance-based risk assessment (using recommended control sets, standards and frameworks) which is not appropriate or practical for the IIoT. More outcome-oriented assurance approaches are needed, that start by considering the potential outcomes for a particular industry (the harms and risks) and work backwards to establish the risk-control requirements.

Organisations that are dependent on, or co-dependent and interoperable with, others need to be able to get assurance that the components and services they buy are trustworthy and secure – but this is complicated due to the entanglement (which might mean organisations are not even sure who they are depending on) and the different assurance requirements between players. There is at present no obvious solution for this, but the recommendations section of this report suggests ways forward.

Operational defence processes

The range of existing approaches to operational defence will not be sufficient in large-scale and fast-evolving IIoT environments. Many of the processes involved already pose a challenge: for example, a 2019 survey of maintenance and patching processes in 1,821 production networks found that 71% of sites were using unsupported (or soon-to-be-unsupported) Windows systems (including Windows 7, unsupported as of January 2020): 62% were using long-outdated Windows 2000 and XP[18]. Updating firmware is likely to be even more unmanageable in large-scale, distributed IIoT environments and existing update approaches may not be efficient enough to meet the functionality requirements of safety-critical systems, for example. A new wave of enhanced continuous and dynamic cyber security processes will be needed for identifying assets, data flows and vulnerabilities; designing secure architectures and maintaining security of their systems; authentication and access control; monitoring IIoT networks and detecting anomalous activity; and performing forensics in response to incidents.

Human-centred recovery processes

Industry may be reaching a tipping point for recovery after a security incident. Resilience, safety and security requirements require effective fallback solutions and in most current IIoT systems an analogue or human failsafe is achievable: analogue components can still broadly achieve enough of the smart functionality to keep systems running and people can still operate systems manually if needed, in order to maintain a level of functionality. This was demonstrated by the recovery from the 2017 WannaCry ransomware attack on the UK's National Health Service (NHS), for example[20]. As the IIoT advances and expands its reach, analogue systems and humans may no longer have the capacity to carry out its complicated functionalities, and particularly the ability to reinstate complicated systems-of-systems and mesh environments. Manual fallback and recovery may no longer be an option for industry, and the approach to recovery will need to change, leveraging effective automated solutions.

Defensive technologies

Many of the low-power end-point devices being incorporated as sensors and controllers in IIoT environments are not suitable for running current cryptographic protocols and therefore will not achieve communications security and data confidentiality requirements. NIST is driving lightweight cryptography standardisation efforts and post-quantum cryptography, but it is unclear to what degree users and producers of IoT devices will be ready (or able) to phase in quantum-ready devices and software. The emerging IIoT architectures also challenge other existing technical defensive approaches, such as network segmentation and air gapping: the logical separation of IT and OT environments within and between sites and organisations may conflict with the drive to realise the benefits of interoperability and may provide a false sense of security where they do exist (as in the example of the Stuxnet attack[19] overleaf).

Example: Stuxnet
Stuxnet is a piece of malware discovered in 2010, deployed in a state-sponsored attack against Iran. Stuxnet targeted the programmable logic controllers of a specific model of centrifuge used to separate nuclear material, causing them to provide false readings while triggering the machinery to operate outside of its tolerance (making the centrifuges spin too quickly and tear themselves apart). This was the first major cyber attack to result in physical damage and also managed to “cross the air gap” as it was installed via a compromised USB stick on machines that were not connected to the internet.

Widening gaps in skills and awareness

As industries and their systems become highly connected for the first time, maintaining their cyber security will become a critical part of the responsibility of a vast and increasing majority of personnel. This will include personnel working in roles that may not previously have required cyber security skills. There will be a need to invest more resources in creating cyber security skills and awareness than ever before (and for some organisations this may be the first concerted effort). Awareness and training approaches will need to scale, improving the pipeline of people who understand cyber security in the industrial space, and to cover the full breadth of IIoT applications. A holistic understanding of how IoT systems fit into the mission of the organisation is difficult to teach, yet it is vital that staff are able to respond appropriately: this includes deciding which systems to leave operational and which to pull offline in the event of a cyber security incident, for example. New concepts will pose a challenge: for example, OT staff and management are often used to considering physical plant, whereas boundaries of networks (and therefore risk) can be difficult to define in the IIoT.

In the 2019 Center for Strategic and International Studies report on the Cybersecurity Workforce Gap[21] over 70% of employers already reported that the cyber security skills gap measurably impacts their organisations, and the problem will increase with the adoption of IIoT. Some examples of training and professional certification offerings already exist in this space[22], but the evolving training needs of personnel across a wide range of industries, taking into account factors such as differing business priorities and a diversity of base knowledge, are not yet being comprehensively addressed. There is concern that this challenge may be particularly acute in developing countries, some of which are now rapidly adopting IIoT, having leapfrogged some of the important technological developments of the past years and, therefore, not necessarily built a sufficient base of cyber security personnel.

Interdependence of risk controls

There is a wide range of anticipated gaps where existing risk controls and capabilities will not translate effectively into the IIoT (see table 1, pages 34-35). The problem is more complicated than simply considering how individual classes of control will measure up in the IIoT. The deficiency of any one type of control could have consequences for (potentially many) others because, as shown in figure 12, cyber security controls are interdependent. Figure 13 shows the chain of downstream effects for failure of a single key control. All classes of control depend to some degree on having an inventory of devices: but current approaches to device inventory will likely struggle to cope with the scale-up, dynamism and complexity of the IIoT.

Risk controls are fundamentally designed for a world where there is clear liability or responsibility – where someone is able to take action. This is already becoming complicated in modern interconnected operational environments, and could become worse with the proliferation of shared data/device/service models possible in the IIoT.

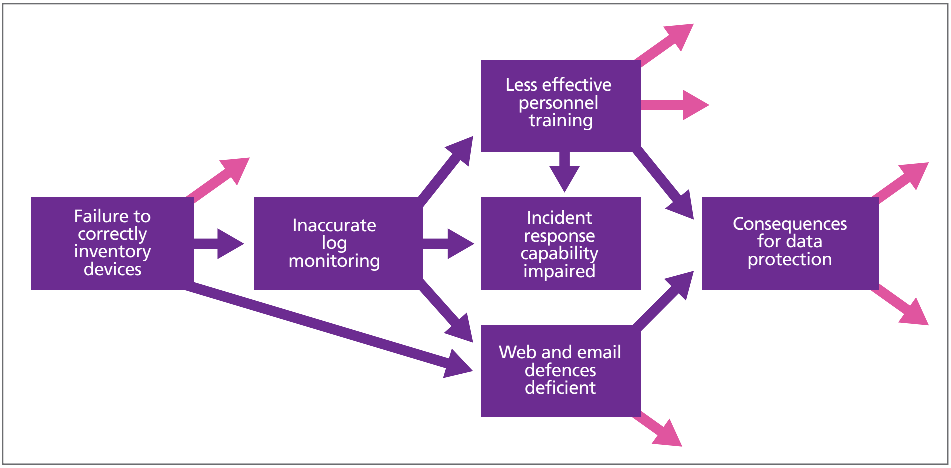

Failure to correctly inventory devices
Inaccurate log monitoring
Less effective personnel training
Incident response capability impaired
Web and email defences deficient
Consequences for data protection

Figure 13: Example of the chain of dependencies between cyber security control measures

Cyber security practice: Challenges for mindset, regulation and insurance

Regulation, cyber insurance and adopting a cyber security mindset could drive progress towards bridging operational capability gaps and developing risk controls

Regulation, the requirements of cyber insurance providers, and the adoption of a cyber security mindset within organisations could drive progress towards bridging operational capability gaps and developing risk controls that translate effectively into the IIoT. There are overarching challenges to these influences, however.

Mindset

In many IIoT industries a cyber security mindset is not yet common, which creates a difficult starting point from which to achieve these operational capabilities. A mindset of safety versus security (particularly in industries that have traditionally had strong safety-compliance cultures) means that security requirements often lose out to safety requirements. The cyber security mindset also comes into conflict with availability priorities. For example, at a leadership level, if avoiding downtime is the main objective this might incentivise keeping compromised systems online (to avoid powering down an electrical plant, for instance). At an operational level, new IIoT systems are likely to be managed, at least initially, by OT teams, who may lack a security focus (specifically integrity and confidentiality): often, there is a cultural bias towards keeping systems running (potentially even if they are legacy or otherwise insecure systems). This could result in solutions to maintain and reinstate system functionality that involve minimal consideration of security.

Mindset: The unique challenges of maritime
Local engineers on ships are used to a high degree of independence, and “solving problems with a wrench and duct tape”. They may be talented network engineers but do not necessarily have a security mindset: for example, stories of engineers “optimising” a network for speed by installing a patch which removes security segregation. This challenge is compounded because ships can pick up spare parts and new crew anywhere in the world.

Persuading an organisation's management to invest in the resources and personnel required to tackle cyber security challenges is an ongoing issue; this issue will be particularly acute in organisations that are newly becoming internet-connected tech or data companies, where investing resources in cyber security has not been a priority up until now. There are signs that the mindset is already beginning to shift, and that cyber security awareness and "paranoia" in the industrial space is growing, boosted by reports of large-scale IIoT security incidents such as the 2019 ransomware attack on aluminium producer Norsk Hydro (and other examples in figure 9, page 22).

These issues emerging internally within organisations make it even more important that effective external approaches incentivise the required advances in capability. Regulation and cyber insurance are two leading examples, yet they also face challenges.

Regulation

There are a growing number of industries for which cyber security regulation will be needed, some of which may not have been regulated for cyber security before. Regulation will need to address both safety and security requirements in an integrated way (without being burdensome or conflicting), particularly in applications where safety and security overlap. Some examples already exist in the aviation sector, such as avionics which must be cyber secure in order to be safety certified[23, 24]. The way in which the internet and technology have been regulated up until now is too static, prescriptive and reactive to be effective in the IIoT, and could hamper realisation of the benefits its new business models can bring.

The complex interdependencies between IIoT organisations, and increasing dependence of organisations on service providers, create ambiguities around where responsibility lies for securing systems. These in turn create challenges for understanding how to regulate in this space[25]. For example, there are conflicting views around the need for regulation to shift the responsibility for secure device configuration (like secure passwords) and integration from the consumer to the manufacturer, as internet-connected devices are implemented in increasingly critical applications[26]. Lastly, the disintegration of the internet into separate enclaves (for example with China and Russia taking an increasingly strong position on international policy) may drive regulation in new directions and there is a need to consider the geopolitical situation.

Regulation: Who makes the call?
A commercial airline does not use commercial data links, which can be used to transmit airline operational control messages and for the plane's crew to stay in contact with air traffic control. It uses 3G on the ground and voice radio; it does not use a data link while in the air because this is cheaper. This creates risks which are accepted by the airline. Where do we (industries, governments, society) want to allow organisations to make choices like this?

Photo by Nur Andi Ravsanjani Gusma from Pexels

Cyber insurance

The cyber insurance industry will face challenges in assessing cyber risk for the full IT and OT estate of complex IIoT systems, identifying the full range of potentially large-scale and propagating harms that may arise from a cyber incident, and deciding primary liability for incidents that occur in interdependent systems. There is a perception that existing cyber-insurance provision for the IIoT is not optimal: maritime cyber risk, for example, is insurable but does not cover the full range of OT, or the value of lost or damaged cargo.

The issue of 'silent cyber' already exists where, because cyber cuts across a range of insurable silos, cyber-related losses arise from traditional policies that were not designed to cover cyber risk. There is a view that this challenge may be exacerbated as boundaries and responsibilities are blurred in the IIoT, preventing the clarity needed to create effective policies.

Strategic findings and recommendations

The current pace of change in operational cyber security is simply not enough to meet the likely demands of a future IIoT. Concerted efforts are needed by a range of groups, from enterprise leaders to device manufacturers to regulators and governments, to address emerging risks and widening capability gaps. A number of common themes have emerged, that form the basis of this review's recommendations:

The current pace of change in operational cyber security is simply not enough to meet the likely demands of a future IIoT

- Leaders within organisations using IIoT will need to act to ensure that they have the right risk-management practices in place to secure their systems and services.
- Carrying out research into the vulnerabilities of, and security solutions for, many live IIoT environments is impractical and potentially dangerous. There is a need to be able to conduct research into how to secure the IIoT in a safe, consequence-free environment.
- The increasing interconnectedness and interdependence of IIoT organisations and potential for shared and systemic risk will create complex challenges for deciding the primary responsibility and liability for cyber security.
- The IIoT will involve device supply chains and third-party service provision that span the globe and security assurance approaches will be needed that create trust on an international scale.

Recommendations are divided into two parts: practical next steps for users of the IIoT and recommendations for further research and investigation. The report ends with a call to action, suggesting areas where Lloyd's Register Foundation and the wider community may wish to focus attention to create impact from this report.

Underpinning all of the recommendations below is a set of guiding principles which should be adopted by all stakeholders in the IIoT ecosystem to help create a common understanding for how to approach risk, responsibility, and resilience.

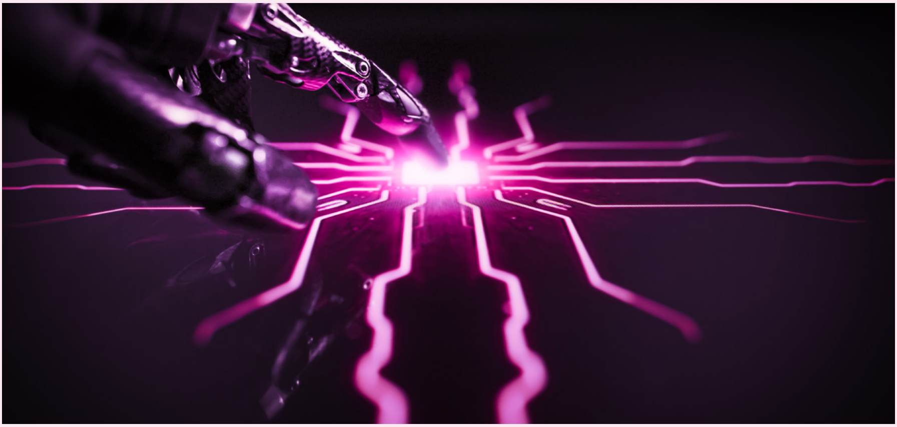
- Assume failure as a basis for risk scenario planning, architecture and security strategy development.
- Assume insider threat within systems and supply chains.
- Assume potential for systemic risk and seek ways to identify and test for where it might manifest, and methods for limiting harm propagation.

Looking ahead

The internet is built on a few foundational technologies: packets of information are sent through a network, using TCP/IP conventions around addressing (for example, IPv6) and a set of domain name conventions overseen by ICANN. Together, these technologies are highly flexible and resilient – but they were not designed with cyber security in mind.

The underpinning systems are not expected to change quickly: they are the platform upon which all of today’s new digital technology is built.

At this time, the most important potential for disruption comes from quantum computing. There may one day be a need to optimise the internet and associated tech for supporting quantum algorithms and applications, which could fundamentally upset existing systems. This would realistically only occur if industry or society were to move wholesale to a quantum-computing paradigm (a timeframe well beyond the scope of this report). However, there is the potential for quantum computers to break the cryptographic protection mechanisms used today, which would require a rethink of common security assumptions, and this may be on the 10-year horizon.



Practical next steps for users of the IIoT

For those organisations using IIoT today, there are a number of measures that should be considered when planning security operations or developing products and services for the near and far term. Generally, organisations should seek to move from compliance- to outcomes-based risk management.

1. **Always consider harm consequences when planning how to manage risks.** It is possible that in the future, devices and technologies already in use will be found to have exploitable vulnerabilities that can introduce risk. This is true for all technology; however, the situation is likely to be more complex with the IIoT as the connectivity potential for IoT architectures means that harm will have more vectors for propagation. Therefore, when designing security architectures it will be necessary to consider the possible connectivity – not just the currently used connectivity. Assuming that connectivity will be limited to what is currently in use will not be a viable strategy.

2. **Consider how security controls may fail as use of IoT devices increases.** Technologies that help implement security controls are as at risk as any other IoT technology. Given the complexity of planning for possible futures, it would be prudent to identify stretch points, where security controls may fail, and measures for identifying situations that are approaching such a point of failure. A good example of this would be to put in place mechanisms for detecting IoT assets not included in the security architecture, or being used in a way which was not anticipated when the security architecture was designed. This forms part of the organisation's situational awareness capability and will be a necessary part of ensuring that its control set remains fit for purpose.

3. **Use techniques that can provide an organisation with a continuous assessment of its position (near real-time) as opposed to periodic assessments.** The dynamics of the IoT may render assumptions on threat, vulnerability and likelihood of risk quickly out-of-date. Moving towards an ability to maintain situational awareness of risk as it changes will not only provide a pace change in security decisions, but also enable monitoring compliance to security and safety standards in nearer real-time.

4. **Consider how supply chains are using IoT: consider their failure to maintain cyber security as a risk to security risk management plans.** An organisation should seek to achieve maximum understanding and real-time visibility of its supply chain, orchestrating its cyber security through the chain, and ensuring that any remaining vulnerability is being dealt with by its risk controls.

5. **Invest in forensic readiness processes**. It is considered best practice for organisations to ensure that they are prepared for an incident in any critical system. In an IoT environment this requirement becomes more acute as the information to collect, log, protect and audit will be more distributed and located within more devices. Where cyber insurance is being used as a means for sharing or transferring risk, it would be wise to plan for data and information capture in conjunction with insurance providers, to ensure that appropriate evidence is collected to maximise the losses that can be recovered.

6. **Include a consideration of future scenarios in risk assessments** (not solely the current position) to try and gain some future-proofing. Given that IoT architecture is inherently designed to be flexible, scalable (in both directions) and amenable to adoption of new technology and analytics, organisations should ensure that their risk assessments are not limited to their systems as constituted today. Consider possible and likely futures. Risk management plans might be stress tested by considering challenging cases, such as

    - No security perimeters are maintained (for example, because IoT introduces unmanageable amounts of vulnerable attack surface).
    - Staff-based attack surfaces present throughout the environment (what if IoT enables an attacker to deploy machine learning to produce highly targeted attacks on colleagues?).
    - Unexpected asset base (when internet connected assets are not recorded or documented when they are installed, and especially if they are located in highly secure areas).
    - Key security controls fail (when the capability of threats from IoT and related technologies are enhanced: for example, crypto not strong enough, firewalls ineffective, social engineering resistance training ineffective).

7. **Invest in training for staff on IoT standards and good practice:** particularly those related to cyber security and safety aspects of the technologies planned or in use. It is important for an organisation to apply good practices and options for controls – but the there is no "right" way to do education. Organisations should be aware that relevant training may not exist (and existing training packages may be inadequate) and some of the most valuable learning comes from opportunities to talk to peers. Organisations with the highest cyber security maturity tend to be willing to discuss their difficulties, rather than treat them as trade secrets or barriers to promotion. The most important thing is to ensure that employees understand operational priorities and their role within them, so they can make good decisions in complex situations. People must understand what is required of them in order to deliver organisational policy.

Further research and investigation

It is clear that the market is unlikely to simply deliver the change needed without concerted efforts first being made to better understand the challenges and test potential solutions. This report proposes a series of recommendations for further research and investigation. This list is deliberately short and aimed at those with the potential to significantly impact the foreseeable limitations in operational cyber security for the IIoT.

Develop an IIoT simulator and research trials capability

The lack of adequate simulation facilities means the research and operational communities are not able to explore the full range of possible failures or recovery options. For example, in civil aviation, an academic team had some interesting security vulnerability ideas to test but could not try them: they could not find an adequate simulator and could not afford to test the ideas on a real plane as they could not fund the hundreds of thousands of pounds to strip, replace and recertify the plane afterwards.

The research and operational communities urgently need the capacity to generate knowledge on the impact of IoT dynamics on outcomes for cyber security and safety, in an environment that can provide the evidential basis to innovate new solutions for risk.

There is a deep need to explore the full range of possible failures and recovery options in a consequence-free environment. Testing security capabilities and assumptions, and testing for vulnerabilities, is impractical and has safety implications in many live IIoT environments: sites are the only instance of a particular combination of devices and suppliers, and cannot simply be pulled offline for experimentation. Questions that a simulator and research trials environment could investigate include

- How to introduce firebreaks inside the networks: the value of reintroducing non-smart components, hardware-based solutions and human-centric components.
- Approaches to controlling network architectures and limiting threat and harm propagation.
- Approaches to the dynamic inventory of devices in large-scale distributed systems and the dynamic monitoring and assessment of risk through real-time data.
- The value of decentralisation and heterogeneity strategies.
- The impact of control interdependence, node centrality and criticality, and modelling of resulting contagion.
- How to deliver optimal immunity and resilience in the face of threat, including patch-management strategies but also the impact of training and mindset developments.

- Effective approaches to automated recovery in the case of an incident and exploration of the need to retain manual fall-back positions.
- Norms of behaviour change and measures of relative resilience.

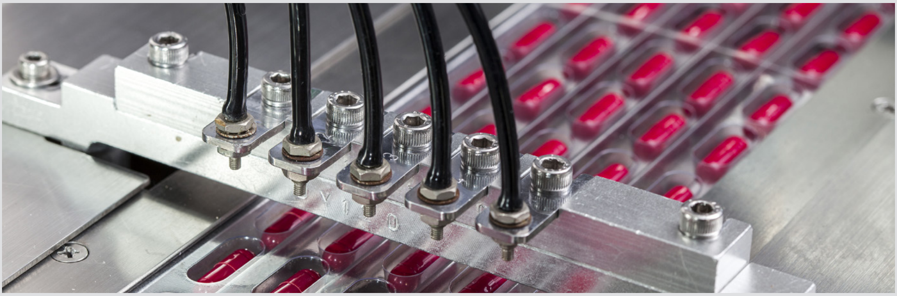
It could also be used as a foundation for testing assurance techniques (including testing the value of assurance programmes that leverage AI) in the face of hyperconnectivity, its enabling technologies (including 5G and network virtualisation), and the risks created by its interaction with other emerging technologies including AI and quantum computing.

Example: Simulation for the shipping sector
A simulation in the shipping industry would bring together a host of connected maritime systems found on an actual vessel and in its extended ecosystem (third-party providers, including cloud providers) to analyse the cyber security vulnerabilities of the single components and the system as a whole.

Thinking in a near future of vessels with the ability to operate autonomously (potentially unmanned) and by remote control, new cyber security threats come from data transfer through satellite link bridges for remote sensing and performance optimisations or predictive maintenance of the monitored components.

As a concrete example, with the International Maritime Organization's climate goals of fuel wastage and greenhouse gas emissions reduction, it is reasonable to expect analysis of the avoidable fuel wastage being modelled with data collected on board and transferred to shore (test bed or operation centre). A simulator could investigate the nature and extent of the cyber security threats coming from this data transfer and remote link.

Example: Research for the manufacturing sector
With manufacturing processes becoming increasingly dependent on IIoT devices and data provision (for example, just-in-time inventory management), modelling the impacts of different types of attack has become difficult. Further research could investigate how to quantify emerging risks from increasing interdependence, as well as how to dynamically manage these in real-time. Additionally, for manufacturing processes that require assurance (for example, pharmaceutical production) modelling could assess whether this assurance can be maintained in the face of a large-scale dynamic system with many unpredictable inputs.



Further study on liability models, practicalities and implications for IIoT markets

If the harm resulting from a lack of cyber security in IIoT grows significantly, then so will the pressure to consider a liability model – for vendors of technologies and services, and for users of IoT devices. In anticipation of this possible future there is value in further study on what shape these models might take, how they would impact the markets, how they would be enforced, and in particular models should be developed which could underpin a cost/benefits assessment exercise. This study should take into account not only national views on the IoT, but international markets dependent on data flows and the likely codes of conduct that will emerge in the operation of the IIoT and the technologies and services such infrastructures depend upon.

Explore approaches to developing trust in the IIoT supply chain, including international collaboration

The IIoT will involve device supply chains (both the supply chains for providing the IIoT devices and the supply chains that are supported by the IIoT devices) and third-party services that span the globe. Such collaboration brings with it inherent risk and the community needs methods for building well-founded trust in supply chains and shared services. This report recommends that an international effort be made to explore ways to bring about a sustained platform for such trust.

Avenues for consideration might include

- The value of certification schemes for component and service integrity, and how to effect meaningful oversight to build trust. This might include consideration of what monitoring of products and services should be a necessary minimum for supply chain assurance.
- Whether and how to utilise open-source code governance as a means of delivering integrity without also exposing vulnerability.
- Collaboration between IIoT device manufacturers to establish a device interface protocol for sharing security information. This should enable risk emergence and propagation to be detected quickly and tracked, and would enable fast and near real-time consideration of compliance and cyber risk; ideally, manufacturers should seek to bridge IT and OT data formats/standards.
- The development of an international cyber security-safety code of conduct for IIoT environments, which can ensure standards are maintained throughout supply chains and which builds culture that can deliver dependability (with consideration of how to regulate or self-regulate such a scheme).
- Ways to seek to align the OT and IT security cultures, avoiding a monoculture but developing a meaningful interface between the two that could facilitate joined-up risk management.
- Consideration of an observatory of cyber security best practices for the IIoT and how such a global effort might collect data in order to synthesise and share knowledge and facilitate more data sharing on the effectiveness of risk controls.
- Exploration of the potential for pre-competitive alliances around safety-security critical threat, vulnerability and control effectiveness information sharing and reporting that could underpin information sharing and distribution of best practice.

Call to action

Understanding systemic risk potential in the IIoT

Given the dynamics of the IoT there is a very real potential that IIoT ecosystems will be developed with inherent potential for systemic risk. Where supply chains span the globe and IIoT organisations are multinational in nature, then this systemic risk may also be global. The community of IIoT stakeholders need, with some urgency, to develop the capability to predict possible outcomes, evaluate response strategies should risk be emerging, detect risk as it emerges and ideally plan prevention and deterrence solutions. There is an urgent need for a programme of study which brings together the relevant expertise to develop initially the models, then the analytical capabilities, and then the computing capabilities to perform such analysis and begin to shape the collective knowledge in this space. Such an effort must involve stakeholders from all relevant sectors and might benefit from the insights of experts from other industries with experience of identifying and mitigating systemic risks. It should seek to generate actionable insights for the research and technology development community, including policy, regulators, international standards and insurance communities.

Proof-of-concept demonstrators for emerging IIoT environments

The IoT is going to be a technology capable of underpinning both economic growth in poorer nations and in developing solutions to some of the world's biggest problems (global warming, food security etc). Supply chains will be global and promotion of IIoT cyber security and safety practice around the globe can help build resilience into the system. This report predicts there would be value in a demonstrator capability engaged with by industry, but vendor neutral and aimed at building capacity in the global IIoT user and supplier communities. This could bring together innovators of products and services with IoT infrastructure providers and users and representatives of civil society in order to build awareness of requirements, barriers and solutions.

Appendix A: References

1 Desai, N. (27 April 2016). **IT vs. OT for the industrial internet – Two sides of the same coin?** [blog post] https://www.globalsign.com/en/blog/it-vs-ot-industrial-internet [accessed 10 June 2020]

2 Leal-Ayala, D; Castañeda-Navarrete, J; Carlos López-Gómez, C. (2019). **OK computer? The safety and security dimensions of Industry 4.0.** University of Cambridge. https://www.ciip.group.cam.ac.uk/reports-and-articles/ok-computer-safety-and-security-dimensions-industr/download/OK_Computer.pdf [accessed 10 June 2020]

3 World Economic Forum (2020). **The Global Risks Report 2020.** http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf [accessed 10 June 2020]

4 Tech Pro Research (2019). **The rise of Industrial IoT: Industrial sector leverages IIoT uses.** https://www.techrepublic.com/resource-library/downloads/research-why-industrial-iot-deployments-are-on-the-rise/ [accessed 10 June 2020]

5 IBM (11 February 2020). **IBM X-Force: Stolen credentials and vulnerabilities weaponized against businesses in 2019**. https://newsroom.ibm.com/2020-02-11-IBM-X-Force-Stolen-Credentials-and-Vulnerabilities-Weaponized-Against-Businesses-in-2019 [accessed 10 June 2020]

6 National Institute of Standards and Technology (NIST) (nd). **Cybersecurity Framework**. https://www.nist.gov/cyberframework [accessed 10 June 2020]

7 Center for Internet Security (2019). **CIS Controls.** https://www.cisecurity.org/controls/ [accessed 10 June 2020]

8 ISO (nd). **ISO/IEC 27001 Information security management**. https://www.iso.org/isoiec-27001-information-security.html [accessed 10 June 2020]

9 National Cyber Security Centre (nd). **Cyber Essentials**. https://www.cyberessentials.ncsc.gov.uk/ [accessed 10 June 2020]

10 Industrial Internet Consortium (2019). **IoT security maturity model: Description and intended use.** https://www.iiconsortium.org/pdf/SMM_Description_and_Intended_Use_FINAL_Updated_V1.1.pdf [accessed 10 June 2020]

11 Industrial Internet Consortium (2019). **The Industrial Internet of Things, managing and assessing trustworthiness for IIoT in practice.** [Whitepaper] https://www.iiconsortium.org/pdf/Managing_and_Assessing_Trustworthiness_for_IIoT_in_Practice_Whitepaper_2019_07_29.pdf [accessed 10 June 2020]

12 European Union Agency for Network and Information Security (ENISA) (2018). **Good practices for security of Internet of Things in the context of smart manufacturing.** https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot/at_download/fullReport [accessed 10 June 2020]

13 IoT Security Institute (nd). **Smart cities & critical infrastructure framework.** https://iotsecurityinstitute.com/iotsec/index.php/artefacts [accessed 3 July 2020]

14 Fagan, M; Megas, KN; Scarfone, KA; Smith, M. (2020). **NIST 8259A, IoT device cybersecurity capability core baseline.** NIST 8259A. National Institute of Standards and Technology. May 2020. https://csrc.nist.gov/publications/detail/nistir/8259a/final [accessed 10 June 2020]

15 Fagan, M; Megas, KN; Scarfone, KA; Smith, M. (2020). **Foundational cybersecurity activities for IoT device manufacturers.** NIST 8259. National Institute of Standards and Technology. May 2020. https://csrc.nist.gov/publications/detail/nistir/8259/final [accessed 10 June 2020]

16 Agrafiotis, I; Creese, S; Goldsmith, M; Nurse, J; and Upton, D. (2016). **The relative effectiveness of widely used risk controls and the real value of compliance.** University of Oxford. https://www.cs.ox.ac.uk/files/8869/The_Relative_Effectiveness_of_widely_used_Risk_Controls_and_the_Real_Val....pdf [accessed 10 June 2020]

17 Ponemon Institute (2019). **The fourth annual study on the cyber resilient organization.** https://www.ibm.com/account/reg/uk-en/signup?formid=urx-37792 [accessed 10 June 2020]

18 CyberX (2020). **2020 global IoT/ICS risk report.** https://cyberx-labs.com/resources/risk-report-2020/ [accessed on 10 June 2020]

19 Karnouskos, S. (November 2011). **Stuxnet worm impact on industrial cyber-physical system security.** In *IECON 2011-37th Annual Conference of the IEEE Industrial Electronics Society* (pp. 4490-4494). IEEE. https://ieeexplore.ieee.org/document/6120048 [accessed 10 June 2020]

20 National Audit Office (2018). **Investigation: WannaCry cyber attack and the NHS.** Report by the Comptroller and Auditor General, UK Department of Health. https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf [accessed 10 June 2020]

21 Crumpler, W & Lewis, JA. (2019). **The cybersecurity workforce gap.** Center for Strategic and International Studies, Washington, DC. https://www.csis.org/analysis/cybersecurity-workforce-gap [accessed 3 July 2020]

22 IoT Security Institute (nd). **Smart cities & critical infrastructure professional certification.** https://iotsecurityinstitute.com/iotsec/index.php/iotsi-certified [accessed 10 June 2020]

23 UK Civil Aviation Authority (2019). **The cyber security oversight process for aviation (CAP 1753).** http://publicapps.caa.co.uk/docs/33/CAP1753%20OCT2019.pdf [accessed 10 June 2020]

24 Bellamy, W. (1 March 2019). **EASA proposes new aircraft cybersecurity certification amendments.** *Avionics International.* https://www.aviationtoday.com/2019/03/01/easa-proposes-new-aircraft-cyber-security-certification-amendments/ [accessed 10 June 2020]

25 Brass,I; Carr, M; Kruakae, P; & Tanczer, L. (2019). **Cyber security of the Internet of Things.** PETRAS Stream Report. https://www.researchgate.net/publication/335175129_Standards_Governance_and_Policy_Cybersecurity_of_the_Internet_of_Things_IoT_PETRAS_Stream_Report [accessed 10 June 2020]

26 Wheeler, T. (2020). **Big Ideas: Placing a visible hand on the digital revolution.** Brookings Institution. https://www.brookings.edu/policy2020/bigideas/placing-a-visible-hand-on-the-digital-revolution/ [accessed 10 June 2020]

Appendix B: Contributors

Andres Andreu
Chief Technology Officer, Bayshore Networks

Gerry Bonner
General Manager Fleet Services,
China Navigation Company

Martin Borrett
IBM Distinguished Engineer;
CTO & Technical Executive
IBM Security Europe

Hugh Boyes
Principal Engineer at WMG Cyber Security Centre, and Director, Bodvoc Ltd

Ruth Boumphrey
Director of Research, Lloyd's Register Foundation

Elisa Cassi
Cyber Product Manager, Nettitude

Lizzie Coles-Kemp
Professor of Information Security,
Royal Holloway University of London

Ben Densham
Chief Technology Officer, Nettitude

Duncan Duffy
Head Electrotechnical Systems,
Lloyd's Register Marine & Offshore

Taylan Durmus
Associate, CyLon

Kevin Forshaw
Director of Industrial and Strategic Partnerships, University of Plymouth

Derwen Hinds
Independent Strategic Technical Advisor in Future and Emerging Technologies.
Honorary Professor, UCL STEaPP and Honorary Principal Research Fellow, ISST, Imperial College London

Paul Hopkins
Global Head of Security Architecture,
Vodafone

Mohammad Jbair
Senior ICS Security Consultant,
Airbus CyberSecurity

Chronis Kapalidis
Cybersecurity Practice Lead, Europe,
HudsonAnalytix; Researcher, University of Warwick

Jens-Peter Kjær Jensen
Senior Program Manager, Force Technology

Srinivas Kumar
Chief Product Officer, Mocana

Irving Lachow
Deputy Director, Cyber Strategy and Execution, MITRE

Kenny Lee
Technical Manager, Technical Services Division, Electronic/Automotive/Wireless, Bureau Veritas

Phil Litherland
CNI Energy and Utilities, PwC

Ross McKerchar
CISO, Sophos

Andrew McKinven
Consultant

Daniel Ng
CEO, CyberOwl

Ng Soon Lee
Vice President, Product Service,
TÜV SÜD PSB Singapore

Gbenga Olugbodi
Programme Manager, Lloyd’s Register Foundation

Raghav Pant
Senior Postdoctoral Researcher,
University of Oxford

Jan Przydatek
Director of Technologies, Lloyd’s Register Foundation

Stuart Quick
Cyber Centre of Excellence Lead,
AXIS Capital

Tim Rawlins
Director & Senior Adviser, NCC Group

Simon Reeve
Director of Commercial Engagement,
Lloyd's Register Foundation

Siraj Shaikh
Professor of Systems Security, Institute for Future Transport and Cities (IFTC), Coventry University, and Chief Scientist, CyberOwl

Greg Shannon
Chief Scientist, Carnegie Mellon University CERT

Christina Skouloudi
Officer in Network and Information Security, European Union Agency for Network and Information Security (ENISA)

Matt Smith
Researcher, University of Oxford

Joel Snape
Senior Research Analyst, Nettitude

William Tanuwijaya
Business Development Manager,
Beckhoff Automation Pte. Ltd.

Jacqui Taylor
Founder, CEO, FlyingBinary LTD; Smart City Tsar, G20 Secretariat (G20SS) expert advisor for Digital Economy

Vincent Turmel
VP of Field Engineering, Bayshore Networks

Janne Uusilehto
Lead Privacy Programme Manager, Google

Cheryl W
HMG UK

Carolin Weisser Harris
Lead International Operations,
Global Cyber Security Capacity Centre,
University of Oxford

Tarah Wheeler
Cybersecurity Policy Fellow,
New America Foundation

Zhang Yiran
Consultant, Cyber Security Services,
TÜV SÜD PSB Singapore

Appendix C: Glossary

5G	The fifth-generation technology standard for cellular telecommunication networks. Compared to current networks, 5G technology will enable more data to travel more quickly and reliably, allow more devices to join the network and will enable organisations to segment and oversee their communications network in new ways. 5G is an important underpinning technology for the IoT.
Adversarial learning	Technique used by attackers to make machine learning systems give a wrong result, altering inputs in a way calculated to confuse the system.
AI	Artificial intelligence. The term encompasses a range of computer science, statistical science and information engineering techniques that enable computers to perceive their environments and take steps to achieve the goals set for them. See also machine learning.
Accident	An unfortunate event that happens unexpectedly and unintentionally, typically resulting in damage or injury (in some fields, accidents are specifically limited to injury to humans). The important distinction for the purposes of this report is that "accidents" do not include intentionality. See also incident.
Asset	An item, tangible, virtual, or intangible, which is valuable to an organisation.
Attack surface	The sum of different points of attack on a system, conceptualised in terms of specific vulnerabilities which can be exploited. Generally, the goal is to keep the attack surface as small as possible and this is achieved by limiting access to sensitive software and systems (eg through physical or digital access control) and keeping software up to date where possible.
Attacker	A person or organisation who takes forceful physical or non-physical actions in order to harm another person or organisation. In the cyber security sense, an attacker is a person or group who acts with intent to cause harm, steal data, etc. They may also be called a threat actor outside the context of a specific attack.
Big data	The meaning of this term is expanding as data science develops, but generally refers to extremely large, diverse data sets, and the processes for making sense of them – often using AI, machine learning or statistical methods.

CIA	Confidentiality – Integrity – Availability. Triad of principles at the heart of information security considerations. Confidentiality: data, objects and resources can only be viewed by authorised entities. Integrity: data is reliable, correct, and protected from tampering. Availability: authorised users have access to the systems and resources they need.
Cloud	Term generally used to describe data centres available to many users over the internet, where "your" data is held by someone else. Often takes the form of subscription services: Gmail, Amazon Web Services, Dropbox, SAP and Oracle are all cloud providers.
Critical infrastructure	Term used to describe assets that are essential for the functioning of a society and economy: electricity, water, and communications are classic critical infrastructures. Often referred to in the context of critical national infrastructure but networks of assets can transcend national boundaries (as in the case of multinational energy grids or the shipping network).
CSC	Center for Internet Security's Critical Security Controls for effective cyber defence. A publication of 20 best practice guidelines and controls for computer security. More information: https://www.cisecurity.org/controls/
Cyber Essentials	A certification scheme provided by the UK National Cyber Security Centre (NCSC) to help businesses guard against the most common cyber threats and demonstrate their commitment to cyber security.
Cyber security	This term is used differently by various sub-communities but is commonly understood to encompass the practice of reducing the risk of cyber incident. It involves defending computers, servers, mobile devices, electronic systems, networks and data from malicious attacks, but can also encompass training and development of new systems (both social and technical) to help minimise attack surface or enable resilience in the event of attack.
Edge computing	Computing done at or near the source of data: in many IoT networks, data is collected by low-power devices and sent through the network to a central computing resource for processing, possibly with results of that processing sent back to the low-powered devices at the “edge” of the network for action.

The edge computing model pushes more of the computation to the devices at the periphery, often to minimise latency (the time taken for signals to be sent and returned). This model requires peripheral devices to have more computational power and brings different security challenges as data are held or shared in different places in the network: generally, these networks are more complicated to secure but it depends on the type of threat anticipated.

ENISA

European Union Agency for Network and Information Security. ENISA works closely together with EU Members States and other stakeholders to deliver advice and solutions as well as improving their cyber security capabilities. It supports the development of a cooperative response to large-scale cross-border cyber security incidents or crises and draws up cyber security certification schemes. More information: http://www.enisa.europa.eu/

Firmware

Basic low-level software that gives instructions to hardware: for example, instructing a traffic light to illuminate different bulbs in order for the light to change colours, or instructing a radio to broadcast on a particular frequency. In low-resourced devices (common in the IoT) firmware may be the only software running on the device.

GDPR

General Data Protection Regulation. The EU's legal framework for managing and enforcing data protection for data held on EU citizens (no matter where in the world that data may be held).

Hardware

The physical parts of a computer or device, such as the case, central processing unit (CPU), computer data storage, motherboard and communications equipment (radio, ports, etc). Hardware is typically directed by the software to execute any command or instruction.

ICANN

Internet Corporation for Assigned Names and Numbers. A global consortium overseeing coordination of the global domain name system, which is the system that links computer-readable IP addresses to human-readable domain addresses, effectively running the "phonebook for the internet" (for example, linking http://icann.org to the computer-readable address of 192.0.32.7). ICANN is involved in a number of important internet governance initiatives.

ICS	Industrial control system. ICS covers the wide collection of control systems, instruments and other hardware used for automating or remote-controlling industrial equipment. Subsets of ICS include process control systems (automated systems to ensure processes are operating within normal boundaries), distributed control systems (where autonomous controllers are distributed throughout the system) and SCADA (more centrally controlled, usually used to automate systems which require continuous monitoring).
IIoT	Industrial Internet of Things. This term can be used differently by different communities; for the purposes of this report it is interpreted as “the industrial applications of IoT technologies.” This encompasses internet-enabled ICS as well as smaller devices (sometimes including consumer-grade IoT devices).
Incident	An incident is an event that disrupts normal operations, which needs to be reported. A security incident is an event that may indicate that an organisation's systems or data have been compromised or that measures put in place to protect them have failed. An incident can include intentionality, whereas an accident does not.
Insider	An actor with legitimate access to a network or system. The term "insider threat" can apply to any person or entity within an organisation creating threat, whether intentional or unintentional.
IoT	Internet of Things. The network of technologies which interface and compute across the internet and its associated communications protocols, largely without human intervention: often (but not always) a collection of small, low-powered devices designed to function as part of a coordinated system for data collection and analysis. Common IoT devices include internet-enabled sensors (eg temperature or air quality gauges), beacons (eg tags that broadcast location), and actuators (eg motors to open and close gates on command). These systems are devised and used by humans, so any discussion of the IoT should include related socio-technical systems, training, psychological conditions, user interfaces, etc.
IP	Internet Protocol (see also TCP/IP). The principal communications protocol in the internet protocol suite for communication across network boundaries. Its routing function enables internetworking, and essentially establishes the internet.

IPv6	Internet Protocol version 6 is the most recent version of the Internet Protocol and defines the ways in which computers can establish addresses. See also: ICANN.
ISO 27001	International Organization for Standardization. ISO security standard 27001 specifies a management system that is intended to bring information security under management control and gives specific requirements. Organisations that meet the requirements may be certified by an accredited certification body following successful completion of an audit. More information: https://www.iso.org/isoiec-27001-information-security.html
IT	Information technology. The use of computers to store, retrieve, transmit and manipulate data or information. IT is typically used within the context of business operations (the kinds of computers, databases and software used in a typical office environment); the definition of IT does not (usually) include OT.
Machine learning	The range of techniques used to enable computer algorithms to improve themselves automatically, "learning" through iteration to optimise the rule-based path towards whatever goal has been set. Machine learning is often described as "supervised" (requiring direct human intervention) or "unsupervised" (requiring little or no human intervention). See also AI.
Malware	Malicious software designed to disrupt, damage or gain unauthorised access to a computer system: viruses, worms, Trojans, adware, spyware and ransomware are all types of malware.
NIST CSF	NIST Cybersecurity Framework. Provides a policy framework of computer security guidance for private sector organisations to assess and improve their ability to prevent, detect and respond to cyber attacks. More information: https://www.nist.gov/cyberframework. NIST is the USA's National Institute of Standards and Technology. Part of the US Department of Commerce, defining industrial standards, such as for cyber security processes and planning. More information: https://www.nist.gov/

Operational cyber security	Classical operational security (OPSEC) evolved in the military context and focuses on considering the adversary’s goals and capabilities, to help clarify defence requirements. In the cyber security context this involves a focus on threat modelling and using countermeasures to reduce or eliminate the adversary’s ability to cause damage.
OT	Operational technology. Hardware and software which detect or cause changes through direct monitoring and/or control of physical devices. Usually defined as distinct from IT.
Phishing	Fraudulent emails attempting to get recipients to visit malicious websites, download malicious software, reveal personal information like passwords or credit card numbers, etc. Phishing is often described in the following broad categories: • Highly targeted (eg purporting to be from the head of finance of a particular company, instructing an employee to complete an urgent financial transaction). • Targeted (eg sending an email to all employees of a particular company, asking them to click a link to receive a discount for a nearby coffee shop). • Untargeted (message sent at random to a large set of email addresses). See also spear phishing.
Ransomware	A type of malware which blocks access to a computer or asset, until a ransom has been paid: ransomware often encrypts the data and offers to give victims the key for decryption if they pay the ransom.
Risk	The potential for uncontrolled loss of something of value: the intersection of asset, threat and vulnerability.
SCADA	Supervisory Control And Data Acquisition. Computer systems for gathering and analysing real-time data on industrial processes. A subset of process control systems, which ensure that processes are operating within normal boundaries, SCADA systems are used to monitor and control a plant or equipment in industries such as telecommunications, water and waste control, energy, oil and gas refining and transportation. See also ICS.

Spear phishing	Another term for targeted phishing, where the attacker is seeking to gain access to a specific individual or organisation.
Software	A collection of data or computer instructions that tell the computer how to work. See also hardware.
Software-defined networks	Early networks were often defined by hardware: devices were physically connected to form a network. Contemporary networks are increasingly defined by software with a central hub controlling the list of which devices are in and out of the network (ie can communicate directly with each other) at any given time.
TCP/IP	Transport Control Protocol and Internet Protocol. Together, this set of rules governs how computers are able to connect to the internet, with data split into packets and routed through the network to their destination, where the packets are reassembled to recreate the original data. See also IP.
Threat	Anything that could cause damage to assets (hardware, software, data, social organisation, etc). Threats can be intentional (eg attackers) or unintentional (natural disasters, chance, etc). See also risk.
Threat actor	A threat actor can be an individual or a group of individuals working together. A threat actor with malign intent is usually considered an attacker (when the threat is realised in the form of an attack), but threat actors could also introduce risk unintentionally.
Vulnerability	A weakness which can be exploited by an attacker to gain unauthorised access to, or perform unauthorised actions on, a computer system. Vulnerabilities can affect any of the CIA considerations, allowing attackers to run code, access a system's memory, install malware, steal, destroy or modify data, etc.
Watering hole	Type of cyber attack where a target (usually a website) is infected with malware, in order to infect visitors to that target. For example, attackers could infect or impersonate a legitimate nuclear industry supplier’s website, in order to infect the computers of nuclear industry employees visiting the site

Lloyd's Register
Foundation

Life matters

July 2020

Lloyd’s Register Foundation
Report Series: No.2020.1

This cover and figures 1 and 11 have been designed using resources from Freepik.com