Emerging Cybersecurity Capability Gaps in the Industrial Internet of Things: Overview and Research Agenda

IIoT Capability Gaps

LOUISE AXON

All authors are with the University of Oxford

KATHERINE FLETCHER

ARIANNA SCHULER SCOTT

MARCEL STOLZ

ROBERT HANNIGAN

ALI EL KAAFARANI

MICHAEL GOLDSMITH

SADIE CREESE

Internet of Things (IoT)-enabled devices are becoming integrated into a significant and increasing proportion of critical infrastructures, changing the cybersecurity-risk landscape. Risk is being introduced to industry sectors such as transport, energy and manufacturing, with new attack surfaces exposed and potential for increased harm. Furthermore, risk and harm arising in the Industrial IoT (IIoT) could propagate across interconnected organisations and sectors, resulting in systemic risk. Aspects of this changing risk landscape are not addressed by current cybersecurity approaches, leaving cybersecurity-capability gaps. In this paper, we show how current and emerging cybersecurity needs in the IIoT align with a key industry cybersecurity standard, the NIST Cyber Security Framework. The key capability gaps emerging in the IIoT are identified based on our findings from a series of workshops with over 100 expert participants. We present a comprehensive research agenda to enable researchers to prioritise research focus to address these gaps; this research agenda covers the full lifecycle of IIoT development (design, implementation, use and decommission). Further, we conclude that there is a significant gap in understanding of the nature of systemic risk, which should be a key priority if we are to develop effective solutions for cybersecurity and safety in IIoT environments.

CCS CONCEPTS • Network security • Embedded and cyber-physical systems • Ubiquitous and mobile computing systems and tools

Additional Keywords and Phrases: Cybersecurity, risk assessment, cyber-harm, systemic risk and propagation, Industrial Internet of Things, frameworks and standards

1 INTRODUCTION

The Industrial Internet of Things (IIoT) is growing rapidly, as IoT-enabled industrial control systems are integrated into a significant and increasing proportion of critical infrastructures. In a range of sectors including transport, energy systems, manufacturing facilities and the built environment, "smart" and Internet-connected technologies are being adopted, enabling new forms of innovation, operational control, monitoring and prediction. Often referred to as Industry 4.0, technological advances in mobile communications and data analytics are facilitating an ongoing scale-up that will continue over the coming years to meet industry drivers for operational efficiency and enhanced functionality.

2692-1626/2022/1-ART1 $15.00
http://dx.doi.org/10.1145/3503920

As a result of the expansion of the IIoT, the cybersecurity risk to these industry sectors is growing. The integration of new Internet-connected devices into the missions of critical-infrastructure organisations is creating new attack surfaces that could expose critical functionalities to cyber-attack with severe consequences, including consequences for physical safety. The potential for systemic risk is growing as industrial organisations communicate and interoperate, with exposure to risks from upstream services and downstream users. IIoT adoption exposes firms to risks in the technology supply chain, and creates potential for harm to propagate within and beyond the organisation. The role of IIoT, bridging traditional Information Technology and Operating Technology systems, for physical processes like manufacturing, transport and energy generation, means cyber risk can lead to significant systemic incidents [68, 71].

The IIoT's impact on the risk landscape will challenge many of the cybersecurity approaches currently used. The sheer pace, scale and dynamism of the emerging IIoT environment will create technical challenges for cybersecurity operations (for example, how to protect, monitor and mitigate attacks on large-scale and fast-evolving networks). There are also significant challenges associated with integrating cybersecurity practice into industrial environments that traditionally prioritise safety (bringing a mindset that may conflict with security), employ personnel who may not have needed to manage cybersecurity until now, and run industrial operational technologies (which may include legacy systems). A lack of clarity around risk ownership will exacerbate risk-management issues: risk controls rely on being able to assign responsibility and then take action – but shared responsibility, infrastructure and ownership in new business models can blur the lines between roles.

It is clear that gaps are emerging where existing cybersecurity capabilities are not sufficient to manage risk in the IIoT. New technologies and cybersecurity methods will be needed to address the technical challenges for operational cybersecurity, while work will be needed to develop and align regulation and incentive models to create the necessary cybersecurity practices. Research is urgently needed to support preparation for cybersecurity in these emerging environments. There is already relevant research underway in a number of key areas (e.g., specific technological developments to meet the emerging challenges). There is a range of prior research exploring specific security and privacy challenges of the IIoT from various angles (e.g., technical, legal), as we describe in Section 2.2. Current research topics for general IoT cybersecurity have also been reviewed [19] (as well as attitudes and perceptions of IoT in critical societal services [67]).

None of the prior work provides a comprehensive account of the key cybersecurity capability gaps emerging in the IIoT. A broad view of the key gaps and how research efforts fit together is essential to ensuring that the efforts of the research community are aligned to address the areas most critically in need of attention. In this paper, we identify the key cybersecurity capability gaps emerging in the IIoT, and present a comprehensive research agenda to address these gaps. The insights we present into capability gaps are based on our findings from a series of workshops with over 110 expert participants from the IIoT and cybersecurity industries, government, civil society and academia. We anticipate that this paper will help the cybersecurity research community to better address the challenges that will emerge over the coming years.

The rest of this paper is organised as follows. In Section 2, we present background on the IIoT, background and related work on IIoT cybersecurity risk (drawing insights from the workshops), and background on cybersecurity standards and the NIST CSF. In Section 3 we present the methodology used in the workshops. In Section 4 we present our findings on the key cybersecurity capability gaps arising in the IIoT, categorised according to the NIST CSF and linked to IIoT lifecycle. We present our assessment of the research agenda required to address the capability gaps in Section 5, and conclude with priorities for a capability to understand systemic risk in the IIoT in Section 6.

2 BACKGROUND

2.1 The IIoT

The IIoT can be considered to be composed of three key parts, as illustrated in Figure 1. Firstly, **physical devices and appliances**: sensors collect data from the physical world, (sometimes) apply algorithms via analytical and local control-systems software components, take instructions from remote control systems via communication networks, and interfaces take actions in the physical world (e.g., operating manufacturing machinery or controlling the movements of vehicles). Secondly, **communications networks** of heterogeneous types with capacity for transmitting and processing IP traffic, connect these devices to the Internet, carrying both the data to be processed and used in analytics, and the information and control instructions that result. Lastly, **data and meta-data** is processed using analytics technologies both in cloud-service environments and increasingly at edge-computing sites, generating information and control instructions that are communicated back to the devices interacting with the physical environment.

As a result of ongoing and anticipated advances in wireless communications technologies (e.g., the new 5G standard for cellular communications, and peer-to-peer technologies), data analytics (including Machine Learning) and process automation, the IIoT is expanding. Industry is developing a critical reliance on these IIoT systems as they use them to perform increasingly sophisticated functions.

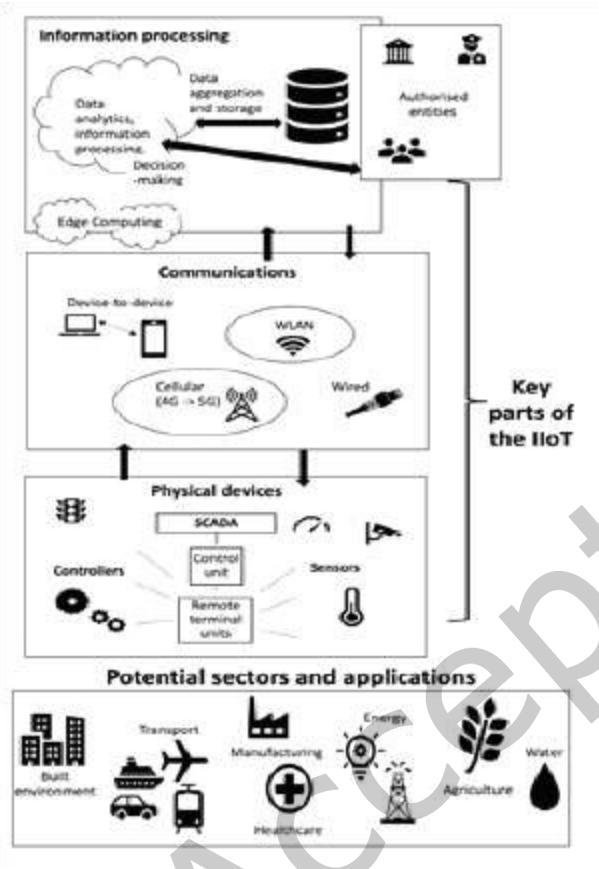

Figure 1: Key parts of the IIoT.

2.2 Characteristics of the IIoT that impact on cybersecurity

The IIoT possesses a unique combination of a number of characteristics, listed below, which create a specific set of cybersecurity considerations. Many of these characteristics are not unique in themselves (e.g., the prevalence of resource-constrained, low-cost devices, is a feature shared by many IoT systems, not only industrial). For this reason, many of the challenges faced in the IIoT overlap with challenges faced across other segments of the digital environment. What makes the challenge of securing the IIoT unique is the combination of these characteristics, which creates several IIoT-specific challenges (highlighted in Section 5). An example is the use of these resource-constrained devices in safety-critical industrial applications with potential for physical harm.

- **Scale.** The scale of IIoT devices, networks and data is growing, and will continue to grow rapidly. Put simply, this means that there is more to secure: larger networks to map out and assess risk over; more assets and data to protect and monitor; and a greater density of devices to coordinate security between.
- **Pace.** The promise of the IIoT is near-instant, coordinated actions taken in the physical world based on sensed data. In order to achieve the necessary functionalities and interoperability, extremely fast

communications and decision-making analytics will be needed, and the actions of physical devices will need to be automated.

- **Interconnection.** As industry seeks to realise the benefits of interoperability, previously siloed digital systems within and across organisations and industries are becoming increasingly interconnected with and dependent on each other, creating shared and systemic risks. Data will increasingly need to be shared across industries and jurisdictional boundaries to enable sophisticated, cohesive functionalities across industrial segments. An example would be the sharing of information between various sectors of a smart city such as transport, energy generation and transmission, traffic-flow control and lighting systems, which can be coordinated to improve the time-, cost- and energy-efficiency of transport across the city [70].
- **IT-OT.** By definition the IIoT combines IT systems with industrial operational technologies (OT). IIoT organisations are therefore responsible for increasingly complex networks of IT and OT technology (including legacy operational systems), and are needing to include traditionally industrial devices in assessment of risk and security architecture. The differing requirements of OT and IT systems create challenges for managing this convergence [110, 111].
- **Dynamism.** IIoT systems will need to be dynamic and agile, shifting continuously (through automation and software-definition) to incorporate new devices and interface with new networks [68, 71], and to support evolving business models, processes and supply-chains. Connections between devices and systems may be temporal: devices may be loosely coupled to perform a task, and then disconnect, and the same device may be part of different systems at different times – or simultaneously [42]. IIoT systems may also incorporate devices that are not traditionally "industrial", for example, individual travellers' smart phones providing location and demand information to the city transit system, and receiving real-time bus location data and route recommendations.
- **Physical harm.** In many IIoT environments, system functionality is safety-critical, and as such cyber-attacks on digital systems have the potential to cause physical harm. This means that there is increasingly potential for cybersecurity compromise to result in physical harm, for example through the manipulation of the actions of vehicles or manipulation of smart-building environments. In many IIoT environments, system functionality is safety-critical, and as such cyber-attacks on digital systems have the potential to cause physical harm.
- **No-downtime.** Many IIoT organisations will have a strong priority to keep mission-critical systems operational, since downtime could damage revenue, or may conflict with safety requirements (for example, shutting down an operational transport system could have safety-critical consequences). This can limit their range of defensive options.
- **Device constraints.** Low-cost devices are common in the IoT and increasingly the IIoT, due largely to market drivers. These low-cost devices may not achieve a sufficient level of security by design. Some devices may also be low-resourced, and thus unable to run resource-intensive cryptographic algorithms and other defensive software.
- **Culture.** As industrial-control systems become newly connected to the IIoT, maintaining their cybersecurity will become a critical part of the responsibility of a vast and increasing majority of personnel. These systems may be managed by personnel working in roles that may not previously have required cybersecurity or IT skills, and also in organisations that may not have prioritised cybersecurity skills and awareness before. Use

and maintenance of IIoT systems often falls to personnel whose background is in "safety" rather than "security", with associated technical, mindset and communication challenges.

2.3 IIoT Cybersecurity Risks

A range of prior work has explored the cybersecurity risks and challenges arising with the growth of the IIoT. The security and privacy challenges in the IIoT and critical infrastructures have been reviewed [20, 22, 27, 30, 34, 35, 38], including reflections on lessons learned from past incidents such as Stuxnet malware attack on a nuclear power plant [33][65]. In [37], the authors present a literature survey of IIoT security requirements, to support the design of security solutions.

Approaches to modelling and mitigating IIoT cybersecurity risks have been presented [69] (e.g., for industrial-control systems such as SCADA [21, 26, 29, 31, 32, 36]). In [24], the authors developed design principles for the IIoT through the integration of security frameworks and models. In [25], the authors explored the effective assignment of security controls in the IIoT, accounting for its unique architecture and operational processes [25]. In [23], the potential for systemic risk in the IIoT is explored, based on an ecological perspective. [40] proposes a set of design principles for assessing cyber-risk in the IIoT. In [42] the authors present an argument for the need to consider possible future scenarios of use when conducting risk assessments, so that resulting risk-management plans remain relevant in dynamic systems.

Emerging IIoT cybersecurity and privacy risks have been explored from a regulatory and legal perspective (e.g., focusing on the smart energy supply chain [17]), and policy recommendations for hardening the IIoT and its supply chains (e.g., focusing on the smart manufacturing context [28]) have been made. There has also been work exploring emerging cybersecurity risks and challenges, focusing on specific sectors: for example, Manufacturing [11-13, 18] and Energy [14-16].

Based on this prior work and also our findings on emerging IIoT cybersecurity risks from the workshops (more detail is presented in [anonymised for review; reference provided in cover letter]), we can identify a wide range of avenues for risk. The impact of traditional cybersecurity risks will widen, mirroring the evolution of the IIoT threat landscape. Risks common to traditional computing environments – malware and ransomware attacks, information tampering and disclosure, and denial-of-service – are set to expand as part of large-scale adoption of the IIoT. This is due to the increased pace, scale, density, and variety of devices, resulting in novel attack surfaces in both hardware and software as new technologies are integrated, and increasing volumes of data at risk of breach.

Beyond the classic technical security challenges above, shared and systemic cybersecurity risks are being created as industrial systems and their supply chains become interconnected. This interconnection could result in unclear risk ownership, and in challenges for identifying risk sources. It is also likely to result in a higher risk of widespread systemic failure, as risks and harms propagate between services upstream and downstream, and across device supply chains. The SolarWinds supply-chain attack illustrated the potential for attackers to cause systemic harm through attacks on supply chains [72], just as the Heartbleed vulnerability showed the potential for many platforms to be affected by a common software dependency [76]. Supply-chain attacks are not limited to the insertion of malware into hardware and software in the manufacturing environment, but can also exploit trusted relationships in supply chains to effect propagation once IIoT devices are in use. The proliferation of compromised devices and systems across the IIoT could be one source of systemic risk, potentially made more complex via the supply-chain relationships.

2.4 Cybersecurity standards and the NIST Cyber Security Framework (CSF)

Various international standards and frameworks exist that inform cybersecurity risk assessment and management approaches, and make recommendations for how to prioritise risk controls within a system. Key examples are the NIST Cyber Security Framework (CSF) [1], the Center for Internet Security (CIS) Critical Security Controls (CSCs) [2], the ISO 27001 security standard [3], and the UK National Cyber Security Centre's Cyber Essentials guidance aimed at small and medium-sized enterprises [4]. Good-practice guidelines recommend risk-management approaches for the IIoT specifically, such as those provided by the Industrial Internet Consortium [6, 73], ENISA [7], and the IoT Security Institute [8]. There are also emerging good practices around establishing trustworthiness for devices and systems, for example the Industrial Internet Consortium's efforts in this area and NIST's guidance for IoT device manufacturers [5, 9, 10].

We base our exploration of cybersecurity capability gaps on the capabilities described in the NIST CSF [1]. The CSF organises cybersecurity capabilities into five high-level categories: **Identify, Protect, Detect, Respond** and **Recover**, within each of which subcategories are described. The framework is for critical infrastructure cybersecurity, and so is specifically relevant to the industrial context, and it has been adopted across many industrial sectors internationally [74]. The basic components are representative of the recognised good practice embodied in the numerous reference points detailed above. Furthermore, it details requirements for response and recovery, which are absent or limited in other cybersecurity frameworks such as the CIS CSCs [2] and ISO 27001 [3][40].

2.5 Limitations of Prior Work, and Contributions of this Paper

As described, a range of cybersecurity risks and challenges associated with the growth of the IIoT have been identified in prior work, but these have not yet been compared with operational cybersecurity frameworks, nor has a comprehensive research agenda for addressing IIoT cybersecurity challenges been provided.

This paper makes two key contributions to the field. Firstly, in consolidating the views of over 100 experts on the key cybersecurity capability gaps that will arise with the growth of the IIoT, we both validate existing literature that has identified some categories of issue, and identify issues that have not yet been explored in detail. We show how the gaps relate to the NIST CSF so that readers can comprehend where these gaps appear in a widely followed operational cybersecurity framework. Secondly, we provide a comprehensive research agenda, describing the key requirements to address the identified capability gaps. We show how existing work has started to address some of these requirements, in order to provide an overview of current progress, and enable researchers in the field to prioritise research.

3 WORKSHOP METHODOLOGY

Over 110 experts from the IIoT and cybersecurity industries, government, civil society and academia participated in three workshops held in Singapore, Oxford, and San Francisco between October 2019-February 2020. Participants represented a cross-section of stakeholders from component manufacturing, to organisations using IoT in a variety of contexts (including transport, energy, manufacturing, building and infrastructure, utilities and smart cities), security firms, insurers, regulators, government agencies, academics, and consultants with knowledge of a variety of firms across the sector.

The aim across all workshops was to elicit the views of a wide range of experts, drawing on their experiential knowledge, on the cybersecurity risks arising from the expansion of the IIoT, the emerging capability gaps, and recommendations for action. Figure 2 shows the methodology followed in the workshops, and how the findings from

each workshop informed the next, resulting in a final set of validated capability gaps and recommendations. In each workshop, the researchers moderated the group discussions and took detailed notes.

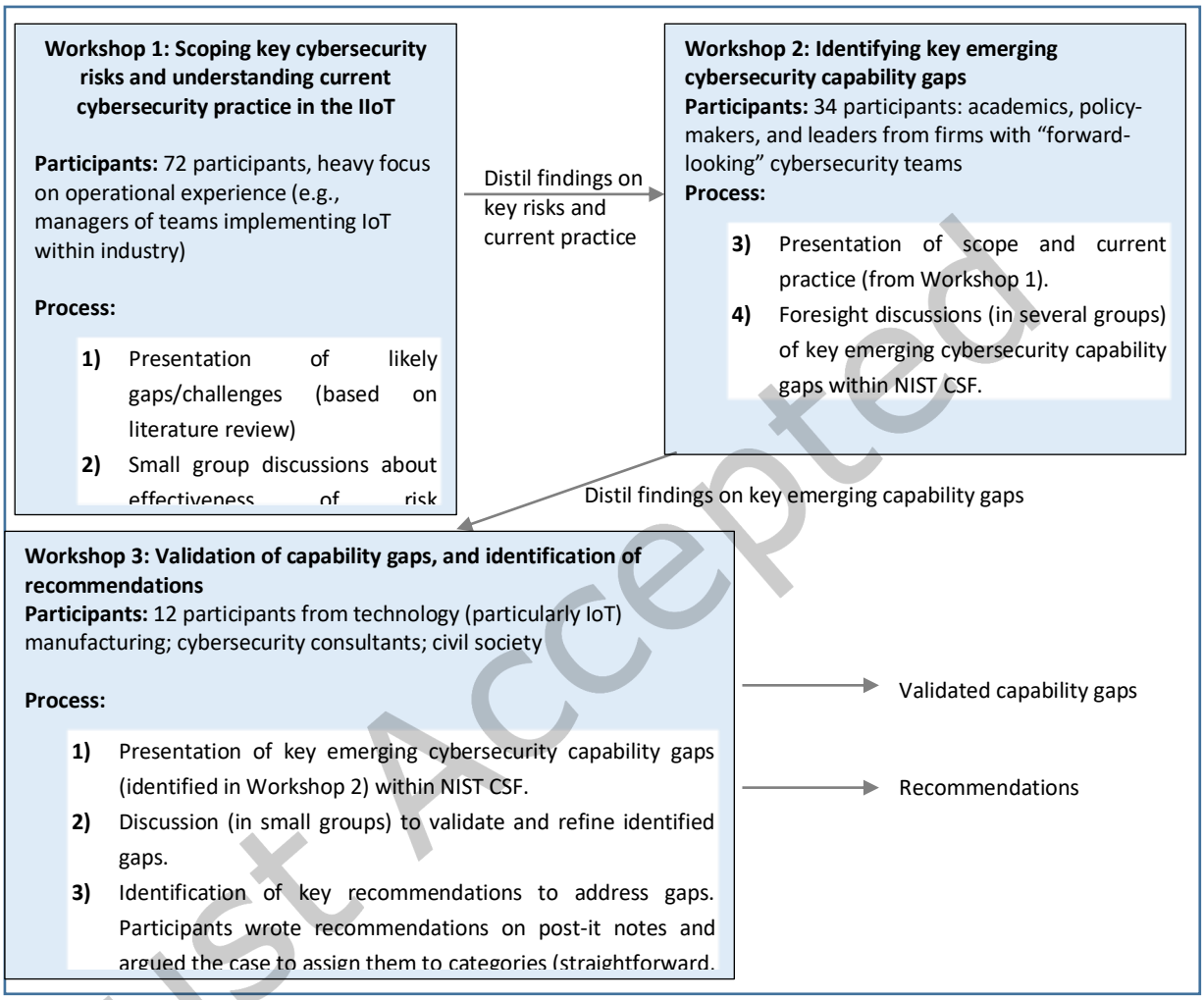

Figure 2: Workshop overview

As shown in Figure 2, a key part of the workshops was discussing the capability gaps emerging with the IIoT in relation to the US National Institute of Standards and Technology (NIST) Cyber Security Framework (CSF) for critical infrastructure cybersecurity [1]. While many participants were already very familiar with the CSF, we also provided an outline of its capability categories and subcategories on paper. In moderating sessions focused on the NIST CSF, the researchers did not seek to exhaustively cover each category of the NIST CSF, but followed the lead of the participants' discussion, asking questions and prompting discussion where necessary.

After each workshop, the researchers analysed the notes taken to identify key themes, engaging in frequent discussion to ensure accuracy and coherence of grouping as well as avoid the potential influences of bias and personal beliefs.

4 KEY EMERGING CAPABILITY GAPS

The key operational cybersecurity capability gaps with respect to the emerging IIoT, presented below in relation to the NIST CSF v1.1 [1], do not represent an exhaustive account of all capability gaps arising within each NIST CSF category (due to space limitations). The findings detailed here represent the **key** gaps; we posit that these are likely to be **representative** of the most prominent issues, and most critical to address.

4.1 Overarching Findings

At a conceptual level, the general categories of capabilities found in the NIST CSF (and many other frameworks and standards) are still relevant for the IIoT. It is at a practical level, however, that the ability to effectively deliver these capabilities is altered, and in some cases, it is likely that entirely new approaches will be needed. We identify potential shortcomings in most of the categories of cybersecurity practice recommended by the CSF.

It is important to note that, although we present our findings in terms of individual capability gaps, risk controls are interdependent and as such, deficiency in any one type of control could have consequences for others. An example is creating an inventory of devices (required in CSF: Identify – Asset Management): as we describe below, this may become increasingly difficult due to the scale and complexity of the IIoT, and other classes of control (including accurate log monitoring (CSF: Detect – Security Continuous Monitoring), incident response/forensics (CSF: Response – Analysis), and the training of personnel (CSF: Protect – Awareness and Training) depend on this foundational inventory.

In summary, the breadth of the capability issues across the portfolio of risk controls, and the inherent interdependency of risk controls, creates an overarching concern that we may arrive at a posture where our most critical sectors are left without an effective ability to orchestrate and deploy cybersecurity, including in safety-critical systems. The following sections (4.2-4.6) lay out the key findings from our discussions, organised according to the 5 main categories of the NIST CSF v1.1 [1]. Within each category of the CSF, we present the key themes that arose in the workshop discussions. Section 4.7 describes broader issues relating to regulation, liability and insurance that arose during workshop discussions but are not directly captured by the CSF.

The focus of this work is on operational cybersecurity, which means that the controls we consider relate to the IIoT lifecycle when deployed (in-use) and during the decommissioning process (moving to not in use). The solutions developed to address the capability gaps discussed may also have consequences for design and implementation phases of the IIoT lifecycle; reducing attack surface within IIoT components (where vulnerability management activities feed back to the IIoT vendors); IIoT components could also be developed to directly support system monitoring for cybersecurity purposes. As our focus is on business operations, the language of the CSF is used in the discussion below, but note that the observations made here carry implications for non-commercial organisations as well.

Table 1 shows the key capability gaps that were identified through the workshops, structured according to the NIST CSF. The characteristics of the IIoT (as introduced in Section 2.2) that contribute to the capability gaps are indicated.

Table 1: Capability gaps identified through the workshops, structured according to the NIST CSF.

NIST CSF Category	Capability Gap	Contributing IIoT Characteristics
Identify		
Asset Management	Identifying large-scale IT/OT estate	Scale; IT-OT
	Understanding dependencies in interconnected networks	Interconnection; dynamism
	Dealing with the lack of visibility of "black-box" third-party software	Interconnection; dynamism; device constraints
	Managing reputation as an asset	No-downtime
Governance and Business Environment	Understanding ownership and responsibility in distributed systems	Interconnection
Risk Assessment and Risk-Management Strategy	Active-assurance techniques challenged	Interconnection; no-downtime
	Simulation-based assurance approaches challenged	Interconnection; dynamism
	Identifying risk-assessment scope and gathering necessary information	Interconnection, dynamism
	Understanding IIoT organisations' need for threat intelligence	IT-OT
	Inadequacy of periodic risk-assessment approaches for dynamic IIoT environments	Dynamism
Supply-Chain Risk Management	Managing upstream and downstream risk exposure	Interconnection
	Ensuring security of low-cost devices	Device constraints
Protect		
Identity Management and Access Control	Delivering secure machine-to-machine (M2M) authentication	Pace, scale, dynamism
	Data sharing based on the "need to know"	Interconnection
Awareness and Training	Security becomes responsibility of non-security personnel	Culture
	Conflicts between "security" and "safety" mindset	Culture
	The need to understand exposure to systemic risk	Interconnection
	Rapid adoption of IIoT in developing countries	
Data Security	Securing large volumes of data	Scale
	Conflicts of interest around data privacy	Interconnection

Information-Protection Processes and Procedures	Identifying attack surface and managing vulnerabilities	Scale; dynamism
	Dependence on orchestration of low-security devices	Device constraints
	Reconciling IT and OT monitoring-system outputs.	IT-OT
	Timeliness of firmware updates	Scale, no-downtime
Maintenance	Timeliness of maintenance	Scale, no-downtime
Protective Technology	Computationally costly defences	Device constraints; pace
	Traditional boundary defences conflict with interoperability	Interconnection; dynamism; pace
	Lacking understanding of secure IIoT architectures	
Detect		
Anomalies and Events	Learning "normal" on fast-evolving networks.	Dynamism
	Detecting anomalies in noisy IIoT datasets	Scale; IT-OT
Security Continuous Monitoring and Detection Processes	Monitoring requires large-scale data analysis and sharing of data	Scale; interconnection
Respond		
Communications and Analysis	Higher performance requirements for reporting approaches	Scale, pace, dynamism
	Cultural aversion to reporting	culture
Improvements and Response Planning	Incident-response practice to keep pace with evolving IIoT organisations	Dynamism
	The need to exercise safety and security together	Culture
Recover		
Recovery Planning	Manual fall-back and recovery become infeasible	Pace, interconnection, scale

4.2 Identify

Description: "*Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities. The activities in the Identify Function are foundational for effective use of the Framework. Understanding the business context, the resources that support critical functions, and the related cybersecurity risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs.*" [1]

4.2.1 Asset Management.

ID.AM.1. Identifying large-scale IT/OT estate. In large, interconnected networks, asset management becomes an even greater challenge. Identifying (inventorying) the full IT/OT estate, and knowing its state will be challenging (particularly for systems where components routinely join and leave the network). Without an inventory, asset-management and configuration control cannot be put in place effectively. Current approaches to creating such inventories are not typically implemented in a continuous fashion, meaning that situational awareness of the state may be extremely difficult to achieve in a dynamically changing IIoT system.

ID.AM.2. Understanding dependencies in interconnected networks. Understanding dependencies between organisations at the asset level will be an increasing challenge, but necessary in order to accurately assess risk. This is especially true for interconnected networks where the sensor owner, the sensor-data user, and the analysis or data broker agency may all be different. The challenge will be exacerbated if organisations are unwilling or unable to share information (e.g., for privacy, regulatory or IP reasons).

ID.AM. 3. Dealing with the lack of visibility of "black-box" third-party software. Traditional controls such as inventory of software are challenged in a 'Software as a Service' era, where third-party software is often implemented on a black-box basis. Organisations cannot necessarily fully understand all of the software they are using, meaning that the responsibility for establishing and monitoring security controls may need to shift from organisations implementing software to those providing it. This holds true for all systems depending upon such service models, and so the IIoT. What is specific to the IIoT is that these environments are likely to have an increased dependency on computational service models as they use low-resource devices.

ID.AM.4. Managing reputation as an asset. In the context of industrial systems, concerns about reputational or legal damage are often secondary to a need to keeping critical systems online at all times. There is a need to balance these considerations in the IIoT. Current approaches to valuation often do not account for a realistic worst-case scenario for an IIoT harm cascade; we might find ourselves in a situation where reputational or legal risk is grossly underestimated, leading to ill-informed balancing decisions.

4.2.2 Governance and Business Environment

ID.GV.1. Understanding ownership and responsibility in distributed systems. An organisation's ability to understand their regulatory, legal and operational requirements (Governance) and their objectives, stakeholders and activities (Business Environment) will be challenged in situations where the ownership of network segments and assets, and responsibility for the functionality of systems, may be unclear. Some segments or sub-systems may not be fully within the operational control of the organisation, posing a structural challenge for managing risk (and mitigating harm): organisations cannot control their downstream users, or upstream providers, but are exposed to risk that those actors create. As with SaaS, this issue is true for other types of system, but may become particularly acute in the IIoT; without addressing how to deliver methods for increasing visibility of risks across supply-chains it may become extremely difficult to deliver risk mitigation controls, and risk avoidance could be either impossible or inconceivable given business needs.

4.2.3 Risk Assessment and Risk-Management Strategy

ID.RA.1. Active-assurance techniques challenged. Once a system is in operation, assurance techniques (e.g., live testing and observation) can be conducted in a number of ways. These methods are situated on a spectrum from passive to active (automated and semi-automated). Where assurance methods are active and interact with live-systems all the

normal concerns around possible undesirable side-effects (e.g., down-time accidental or deliberate) will apply in the IIoT as they do today. Whilst it may at first appear that there is nothing specific about the IIoT that changes this situation, and therefore current approaches to dealing with the issue would simply apply, it may be the case that there are hidden interdependencies between sub-systems (both within and outside the organisations control), then the risk of undesirable side-effects could be significantly heightened.

ID.RA.2. Simulation-based assurance approaches challenged. The lack of transparency of the IIoT estate, and the dynamism of IIoT systems makes high-fidelity simulations on cyber-ranges more difficult to architect. This is because such simulations are a passive form of assurance that cannot convincingly establish coverage of potential system state/s without realistic system insights.

ID.RA.3. Identifying risk-assessment scope and gathering necessary information. While current approaches require identification of the assets to be protected and the scope of the system, identifying the scope and boundaries of complex, dynamic and interconnected IIoT systems will be increasingly challenging [42]. When considering IIoT cybersecurity we will need to assess the impact of dynamism in networks whose subsystems may be under the control of different and possibly highly diverse users. The scope of IIoT systems, when assessed for risk and security architecture in a particular organisational context, may need to include allowances for greater flexibility around system topology.

ID.RA.4. Understanding IIoT organisations' need for threat intelligence. Threat intelligence is difficult in the field of Operational Technologies (OT), as usually cyber-threat intelligence is focused on IT systems. There is a need to expand the scope of threat intelligence to support IIoT security operations, noting that the OT threat may vary by sector. It is also possible that limitations in estate discovery and situational awareness will result in inadequate threat intelligence (missing something that is pertinent to the enterprise); this is an example of the interdependency of controls. So, the specific capacity gap that needs addressing here is how to scope an organisation's need for threat intelligence in the IIoT. There is a secondary need, for capacity to produce such intelligence, but this is considered out of scope for this paper and not highlighted as a capability gap, as there is sufficient expertise and interest in the supplier market.

ID.RA.5. Inadequacy of periodic risk-assessment approaches for dynamic IIoT environment. The dynamism of IIoT environments will mean that periodic, static snapshots of cybersecurity risk-posture could very quickly become out of date; current risk-assessment processes may, therefore, leave exploitable attack surfaces undetected for long periods of time in the fast-moving IIoT environment. Dynamic, continuous forms of risk-assessment are needed to prevent newly evolved risks remaining unaccounted-for and unaddressed.

4.2.4 Supply-Chain Risk Management

ID.SC.1. Managing upstream and downstream risk-exposure. The growing interconnection of IIoT networks poses a structural challenge for identifying, assessing and managing supply-chain risk (and mitigating harm) since the systems of individual organisations are but a link in the chain. Organisations are dependent on downstream users and upstream providers. They have no control over the actions of these parties, however, and are increasingly exposed to risk that they create. For organisations that are dependent on or interoperable with others, getting assurance that the components and services they use are trustworthy and secure is a challenge, complicated by the entanglement of services (which might mean organisations are not even sure who they depend on) and the different assurance requirements between players. If organisations are unwilling to share the necessary level of information, e.g., due to privacy, reputational, regulatory or IP concerns, this will intensify issues around transparency and assurance.

ID.SC.2. Ensuring security of low-cost devices. IIoT systems are composed, in part, of low-resource, low-cost devices. Measures (e.g., regulations) need to be put in place to ensure that devices being used in critical infrastructure are not insecure or delivered with inherent attack surface (e.g., due to economic drivers of IoT suppliers to produce devices at a low cost). Methods for designing verifiably correct computing systems have been supported in the past (ubiquitous computing was an active research space in the early 21st century), but not widely adopted. Supply-chains supporting the IIoT will need to find ways to demonstrate integrity in the services they offer (as well as availability and confidentiality), both for the devices themselves and the supporting computational cloud services and the communications methods used to connect to them.

4.3 Protect

Description: "*Develop and implement appropriate safeguards to ensure delivery of critical services. The Protect Function supports the ability to limit or contain the impact of a potential cybersecurity event.*" [1]

4.3.1 Identity Management and Access Control

PR.AC.1. Delivering secure machine-to-machine (M2M) authentication. Authentication currently has a user/account-device focus. The scale-up of the IIoT will demand more machine-to-machine authentication, since the utility of the IIoT lies in pervasive connectivity, with meshes talking to other meshes. Currently much M2M authentication occurs on a scale where it is manageable with some level of human supervision. Connections on the scale that is required in the IIoT cannot be manually managed by humans, and trying to do so will limit the system's capabilities. As enabling multiple machines to authenticate to each other (with reduced human oversight) becomes integral to the operations of CI, the security of M2M authentication will be critical to preventing unintended consequences and functionalities of systems interacting in unexpected ways [75]. The community does not yet have experience in delivering secure M2M authentication on this scale.

PR.AC.2. Data sharing based on the "need to know"? Access control is traditionally administered on the basis of "the need to know", with parties being afforded the minimum access rights required to carry out their role (role-based access control). This is not a good match for the IIoT environment where data-sharing is key to functionality. What is "need to know" in the context of a smart city, for example? Defining system actors and what is, can and should be known, is not a straightforward task. This is especially the case in a context where devices may have multiple functions, or the same information may be used by different actors for different purposes. There is a need to consider how the "need to know" access-control approach applies in these environments, and whether new access-control paradigms are needed.

4.3.2 Awareness and Training

PR.AT.1. Security becomes responsibility of non-security personnel. The cybersecurity skills gap is already prominent and well-recognised. In the 2019 Center for Strategic and International Studies report on the Cybersecurity Workforce Gap [39] over 70% of employers already reported that the cybersecurity skills gap measurably impacts their organisations. This problem will increase with the adoption of IIoT, as security becomes the responsibility of non-security personnel.

PR.AT.2. Conflicts between "security" and "safety" mindset. Conflicts can arise between security and safety requirements, e.g., in cases where shutting down a system could have safety-critical consequences, yet leaving it running could enable an attack to continue and potentially propagate to other systems.

PR.AT.3. The need to understand exposure to systemic risk. As relationships across supply-chains build, the exposure of organisations to systemic risk will increase. The cybersecurity capabilities of personnel (and particularly leaders within organisations) will therefore need to extend to sensing exposure to and mitigating systemic risk, which could impact critical relationships across supply-chains and with customers. This level of understanding is not currently possessed by personnel within most organisations (IIoT or otherwise)

PR.AT.4. Rapid adoption of IIoT in developing countries. These challenges 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. The rapidity of this change may mean they have not developed a sufficiently broad and deep base of cybersecurity expertise in the workforce (or related regulatory and legal frameworks).

4.3.3 Data security

PR.DS.1. Securing large volumes of data. The IIoT will create large volumes of data, spread across geographic locations and possessed by different platforms and companies. Data-security approaches will need to scale to meet the challenge of protecting the confidentiality, integrity and availability of this information. This will require considerations of how to protect data-at-rest on devices and in the cloud, as well as in transit around the IIoT. Consequently, components of IIoT systems may be subjected to data-security requirements not faced before, and integrating such functionality will need addressing – both in design and in validation. In many cases these techniques will need to be redesigned to cope with the limited resources available on some devices.

PR.DS.2. Conflicts of interest around data privacy. The IIoT will provide another scale-up in the data points available for collection, but correlation of data points may prove concerning for privacy. There is an inherent mismatch: individuals may wish to minimise data-sharing and preserve privacy – and this position may be supported by data-protection law – but the value for the firm is often in sharing or re-using data in new ways. There is potential for adversarial relationship between the customer and the service provider over data (especially in context of personal data, but also in business-to-business (B2B) context where a service provider effectively has access to trade secrets about another organisation's process).

There is need for technical, social, legal and business models for establishing trust and handling data sovereignty in a connected society. The community is pursuing differential privacy as a means to handling trade-offs between data utility and privacy concerns, but the sufficiency of this approach remains untested, and in the context of the IIoT where there are also safety-critical concerns, we may find the safety of a community of users taking precedence over a single individual's security. We currently lack the analytical frameworks to reason about such complex concerns as a basis for trade-off decisions.

4.3.4 Information-Protection Processes and Procedures

PR.IP.1. Identifying attack surface and vulnerability management. With the combined acceleration in pace, scale and scope for IIoT adoption, it is unclear whether we will be able to identify potential attack surface in the IIoT. There is a need to explore whether current approaches to threat and vulnerability management will scale up to protect information systems and assets. It is likely that speed of propagation of threats will be enhanced by the connectivity offered by the IIoT, and this will place additional burden on the ability of organisations to react quickly enough with protection measures. The result is likely yet more investment in the automation of detection and prevention. This is already a research topic, but in the IIoT new limitations associated with resources at end points will need to be overcome if operational cybersecurity is to be achieved.

PR.IP.2. Dependence on orchestration of low-security devices. Possessing the knowledge and experience to be shrewd customers of technology, of advice and of security solutions is an ongoing challenge. Making a risk-management decision about whether to accept, mitigate or avoid risk is difficult. This is especially the case where a base level of technical, social and operational familiarity is needed, as such decisions cannot be made lightly or delegated. There is a concern that this may become a more acute issue in the IIoT, particularly as systems are designed to be composed, in part, by many low-cost devices with inescapable inbuilt attack surface. This may result in cybersecurity becoming even more dependent on the ways in which such systems are composed and orchestrated – something that requires even more expertise.

PR.IP.3. Reconciling IT and OT monitoring-system outputs. The outputs of IT and OT monitoring and management systems (e.g., data format and type of data recorded) tend to differ. Combining these data streams for a unified Security (or general Operations) overview is extremely difficult and not currently supported by commercial orchestration packages.

PR.IP.4. Timeliness of firmware updates. Policies on frequency of updates are not always keeping up with the pace of change even in current IoT systems, and patching already poses a challenge across IT systems (e.g., 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, systems, and 62% were using long-outdated Windows 2000 and XP [62]). Updating firmware is likely to be even more unmanageable in large-scale, distributed IIoT environments: existing update approaches may not be efficient enough to meet the functionality requirements of safety-critical systems, for example [66]. Furthermore, timely firmware updates may not be feasible e.g., in production lines in where any downtime is costly, or where updates could invalidate certification status, and may even be unsafe in some environments.

4.3.5 Maintenance

PR.MA.1. Timeliness of maintenance. In industrial environments, maintenance and repairs of industrial control and information system components need to be performed consistent with policies and procedures. However, timely maintenance may be infeasible in some environments due to the costs of downtime, as above.

4.3.6 Protective Technology

PR.PT.1. Computationally costly defences. Many of the low-power end-point devices being incorporated as sensors and controllers in IIoT environments are not suitable for running current controls such as cryptographic protocols, malware defences, intrusion-detection systems and associated software sensors [59]. These security steps could also add unacceptable time delays in systems where low latency is key. There are therefore challenges to implementing technical security solutions to ensure the security and resilience of systems incorporating these devices.

PR.PT.2. Traditional boundary defences conflict with interoperability. Traditional boundary-based cybersecurity controls no longer apply in the same way in the IIoT environment. Boundary-defence measures such as firewalls conflict with the basis of IIoT functionality, and conflict with the drive to realise the benefits of interoperability. Continuous machine-learning based vulnerability assessment may be an alternative to rules-based firewalls, but the technology is still developing. If this is indeed the only viable way to deliver the functionality, then machine-learning assets will need protecting from compromise. There is currently a community of researchers interested in the security model for machine learning, but this is at the beginning of its development even as a research topic, and so solutions which can be deployed will be a long way behind adoption of the IIoT. This will leave a capability gap in the interim (at least).

PR.PT.3. Lacking understanding of secure IIoT architectures. The community does not yet have a sufficient understanding of how to architect interconnected IIoT environments securely. This includes how to orchestrate risk controls to optimise security while aligning with the drive for interoperability and with potentially conflicting safety requirements.

4.4 Detect

Description: "*Develop and implement appropriate activities to identify the occurrence of a cybersecurity event. The Detect Function enables timely discovery of cybersecurity events.*" [1]

4.4.1 Anomalies and Events

DE.AE.1. Learning "normal" on fast-evolving networks. Current anomaly-detection approaches define what is "normal" and then watch for threatening levels of deviation from it. With the emergence of reconfigurable, fast-changing networks in the IIoT, more responsive methods will be needed. Generative models of systems will be required, as normal will evolve. These models will need protection so as to avoid threats being able to train the system to learn a normal that is incorrect and provides cover for an attack. It will not be sufficient, in a cybersecurity operations context, to rely on promises that these approaches work, they will need to be verifiable or explicable whilst in-use. However, for true effectiveness a mindset change is required, focusing on quick, flexible response rather than brute-force application of policy (since policy is likely to quickly become outdated as the IIoT systems evolve).

DE.AE.2. Detecting anomalies in noisy IIoT datasets. False positives and the difficulty of finding important information in large, heterogeneous datasets is already a known problem for Security Operations Centres. These monitoring challenges will increase in the very noisy systems that the IIoT will enable. Setting an appropriate sensitivity threshold for baseline pattern-of-life analysis, and identifying datapoints of interest in something as vast as a smart city will be a major challenge.

4.4.2 Security Continuous Monitoring and Detection Processes

DE.CM.1. Monitoring requires large-scale data analysis and sharing of data. In IIoT environments, the vast quantities of potential log data will be too big for most current monitoring/analysis systems. Big data approaches might help, but innovation will be needed to apply them successfully in the context of cybersecurity operations. Analysts will need methods for interrogating both large scale IIoT systems and data, as well as the security log data. These methods will need to support exploratory functionality with the capacity to disregard data, create new models explaining relationships, and then to rewind and disregard. It is likely that data will need to be shared across supply chains in order to facilitate the situational awareness required, and this will require solutions to data normalisation and interoperability. These challenges are not new, but are not solved for current systems; the need will become more acute in the IIoT.

4.5 Respond

Description: "*Develop and implement appropriate activities to take action regarding a detected cybersecurity incident. The Respond Function supports the ability to contain the impact of a potential cybersecurity incident.*" [1]

4.5.1 Communications and Analysis

RS.CO.1. Higher performance requirements for reporting approaches. Reporting effectively on incidents and to share threat intelligence is typically achieved in three forms currently: opensource resources; bespoke threat and vulnerability intelligence as service; sharing amongst trusted groups. All of these are human intensive in distribution and in the translation into action with cybersecurity controls. There is a continuous effort to standardise in order to support information sharing and reporting in current cyber-systems (including IoT). However, the IIoT scale and dynamism is likely to create additional performance requirements in order for organisations to react at the necessary pace.

RS.CO.2. Cultural aversion to reporting. Heavy-industry and safety-related sectors often have a culture of reporting incidents only when legally required: cybersecurity incidents are often reported only in the context of a data breach or as part of a safety incident. In some sectors there is strong cultural aversion (or even fiduciary responsibility, for Board members) to avoid public disclosure of security status. Sharing information between organisations on "near misses" is particularly difficult – but workshop attendees felt it was a highly valuable learning tool. To achieve operational cybersecurity maturity, organisations may need to embrace a level of openness that they are uncomfortable with. Methods to enable sharing with confidence will be needed.

4.5.2 Improvements and Planning

RS.RP.1. Incident-response practice to keep pace with evolving IIoT organisations. Practice is already an important part of incident response preparedness, and also enables organisations to improve their incident-response capability by incorporating lessons learned. There is a building capacity in the design and delivery of simulations and exercises designed to help organisations practice. These are beginning to extend to IoT environments. What is missing from our knowledge base is an ability to know whether an exercise is effective. An additional requirement will be to ensure that this form of practice can keep pace with the dynamic nature of IIoT organisations.

RS.RP.2. The need to exercise safety and security together. the IIoT specifically, consideration will need to be given to the safety critical nature of systems, and approaches developed that can exercise both safety and security in tandem. Methods for assessing applicability will eventually be required to ensure organisations can commission wisely. Many organisations have not practiced incident response sufficiently for standard cybersecurity environments; this will be exacerbated by the increased number and diversity of personnel who will need to be trained to respond, from the C-Suite to the factory floor (see Awareness and Training, above).

4.6 Recover

Description: "*Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident. The Recover Function supports timely recovery to normal operations to reduce the impact from a cybersecurity incident.*" [1]

4.7 Recovery Planning

RC.RP.1. Manual fall-back and recovery become infeasible. Resilience, safety and security all require effective fallback solutions. In current IIoT systems, some sort of non-IoT failsafe is often possible, falling back to manually operated systems or relying on analogue components to maintain basic functionality. For example, following the 2017 WannaCry ransomware attack, the UK National Health Service (NHS) was able to fall back to paper-based record-keeping systems to keep services running [63]. However, as the IIoT takes on more central roles in important

processes, it may no longer be possible to replace "smart" functionality with "dumb" equivalents. Equally, if complex interconnected systems go down, a simple "manual reset" button may not exist.

Recovery will need to rely on some amount of automation, which will need to be set up in advance. Furthermore, fully testing these recovery systems may be impossible, as the systems they are meant to restart cannot be fully pulled offline for testing. Digital twins may be a helpful technology in this case, but they must be orchestrated with **Awareness and Training**, and **Practical Incident Response**, above. Such an approach also limits the ability of the organisation to iteratively improve its incident-response plan through "live fire" practice.

4.8 Broader Issues

4.8.1 Regulation

There is a multitude of IoT standards [77], with over 20 important standards-setters working in this area [78]. However, despite the forest of technical details for how devices can connect and interoperate, very little of it deals with cybersecurity. The data collected by IoT devices may be caught up in other laws (e.g., GDPR for data collected on European citizens, or as part of ISO27001 certification), but security-by-design for IoT data and devices is only just beginning to be formally addressed.

The 2019 European Cybersecurity Act established a certification framework for products, processes and services [79], and in January 2020, NIST (the US standards body) published draft recommendations for IoT device manufacturers [80]. These efforts are gaining momentum: in January 2020, the UK government announced that it will introduce mandatory requirements for IoT device manufacturers [81]; and California went a step further, enacting a law requiring minimum security standards for IoT devices sold in the state [82]. However, at present, for firms seeking to manage IIoT cybersecurity risk, standards and regulations provide limited support.

Safety-security regulation may provide a path for progress. There are some examples where safety and security overlap, which provide targets for security to be improved through regulation. The European Union Aviation Safety Agency's proposed 2019-01 amendment for aircraft cybersecurity could serve as a precedent for similar cooperation in other sectors [84]. Legislation and technological standards could mandate a base level of security provision, and manufacturers' liability could create an even more proactive security stance. However, creating such an environment requires cross-border cooperation and meaningful international regulation.

A second theme which emerged in the workshops is **responsibility**: several attendees speculated that a step-change in our conception of responsibilities may be coming, especially between manufacturers and users. Who is responsible for what, and how long should that relationship last (for example, should a software provider be required to support a product for a set period by law? How long would be reasonable?). For example, the UK and California security standards both incorporate a responsibility for the manufacturer to ensure that devices leave the factory with unique passwords, moving (some of) the burden away from the user. A key difficulty in addressing regulation is that security is a process, rather than an end-point; as threats change, mitigations evolve, and it is difficult for a security requirement to remain relevant. Research may help to establish some evergreen principles which could be used to inform law, but long-lasting security standards will likely remain a challenge for this discipline.

4.8.2 Liability

In distributed systems, it can be difficult to establish ownership of components or assets, which in turn makes it hard to assign liability [41]. Furthermore, in the software-as-a-service era, organisations using

"black box" assets may not be in possession of the necessary information of permissions to assure them; recognition of this fact will need to inform the assignment of liability.

4.8.3 Insurance

The cyber-insurance industry will face challenges: identifying the full range of potentially large-scale and propagating harms that may arise from a cyber-incident; assessing cyber-risk for the full IT and OT estate of complex IIoT systems; 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.

Furthermore, cybersecurity cuts across a range of insurable siloes, with cyber-related losses arise from traditional policies that were not designed to cover cyber-risk. The 'silent cyber' issue describes this phenomenon and is already observed today. 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.

4.8.4 Procurement

While organisations say that that want security (or privacy), this does not always drive purchasing choices [83]. This is likely to continue into the IIoT, which may result in larger attack surface and systemic risk across supply-chains.

5 RESEARCH REQUIREMENTS

Based on the capability gaps presented, we present key research requirements. This describes the areas in which research is needed to address emerging and anticipated cybersecurity capability gaps, and to prepare to address cybersecurity risks emerging with the IIoT. Where existing and emerging approaches are relevant, we highlight them to enable researchers to prioritise areas of focus and explore what further research is needed.

5.1 Predicting, identifying and mitigating systemic risk

There is a need to develop the research basis to support prediction emergence of systemic risk, identification of its emergence, and understanding of how to respond for resilience. The key areas requiring research are how to account for systemic risk in risk assessments; how to build trust in the IIoT supply chain; and how to account for the interdependence of risk controls and its implications for risk propagation.

Research requirement	Gaps addressed	IIoT only?	State-of-the-art
Risk assessment			
Dynamic monitoring of risk across supply-chains and based on real-time data, to enable continuous or at least more frequent risk assessment. This would benefit from techniques for automatically detecting changes in risk, and analytical models for predicting risk propagation.	ID.RA.5	N	Design principles for assessing cyber-risk in the IIoT [40]. Proposal of an automated risk-assessment system for IIoT and industrial-control systems: prediction and prevention; information gathering; assessment, analysis and reporting [85].
Outcome-focused risk-assessment approaches for IIoT sectors: development of approaches that start from the potential harms to derive risk priorities (rather than compliance-based approaches starting from the controls needed).	ID.RA.3	Y	
Approaches to developing trust in the IIoT supply chain			
Methods to make safe (potentially "black-box") software from unknown third parties (including trusted hardware solutions).	ID.SC.1; ID.AM.3	N	
Zero-trust solutions for operating across untrusted infrastructures.	ID.SC.1	N	Work on zero-trust architectures by NIST [88]. Zero-trust hierarchical management, to validate transactions at different trust levels in the IoT [89]. Micro-segmentation approaches to zero trust (not IIoT-specific) [87].
Transitivity methods for propagating and projecting trust through supply-chains.	ID.SC.1; ID.SC.2	N	Approach to IoT supply-chain trust based on Blockchain [90]
Codes of conduct and methods for verifying trustworthiness attestations.	ID.SC.1; ID.SC.2	N	Techniques for practical trustworthiness attestation [91].
Methods for restricting or limiting risk propagation from compromised devices and subsystems, suitable for application by controllers of compromised components, or by targets of risk propagation.	ID.SC.2; PR.PT.3	N	Theoretical background, risk modelling and simulation of "cascading failure" in interdependent IIoT environments [93].
Interdependence of risk controls			
Modelling the interdependence of risk controls, and how contagion may spread depending on which nodes or risk controls are compromised.	PR.PT.3	N	Analysis of the potential for systemic risk in the IIoT, based on an ecological perspective [23].

5.2 Deploying risk controls for optimal effect in limiting risk propagation in IIoT systems

Research is needed to enhance understanding of how to deploy risk controls for optimal effect in limiting risk propagation throughout IIoT systems. This includes how to identify assets and attack surface at scale; how to monitor for "normal" and "anomalous" in constantly evolving networks; how to meet the need for firmware updates in large-scale environments where downtime is not an option; how to defend IIoT environments with unclear or shifting boundaries; how to authenticate devices and humans in the IIoT; and how to achieve resilience and recover systems when fall-back to manual approaches is infeasible.

Research requirement	Gaps addressed	IIoT only?	State-of-the-art
General			
Defences that work on resource-constrained IIoT devices. This needs to extend beyond cryptography into support for operational cybersecurity such as host-based intrusion detection sensor solutions for IIoT devices.	PR.PT.1	Y	Research into and development of approaches for low-resource security applications (such as NIST lightweight cryptography standardisation efforts [56])
Resilient cybersecurity architectures for the IIoT, support for adaptation (potentially automated to keep pace). Includes the need for hardening solutions for devices presented at the edge.	PR.PT.3	Y	Exploration of the effective assignment of security controls in the IIoT [25]. Design principles for the IIoT developed through the integration of security frameworks and models [24]. Proposal of a Blockchain-based architecture for privacy preservation and security in the IIoT [86]. Software-defined networking approached to cyber-resilience in the IIoT [92]
Asset and attack-surface identification at scale			
Inventorying (scan and control) and managing large-scale interconnected networks (with potentially unclear boundaries). Including how to understand and track asset dependencies.	ID.AM.1; ID.AM.2	N	
Approaches to identifying attack surface/vulnerabilities over large, shifting asset lists.	PR.IP.1	N	
Security monitoring			
Monitoring and anomaly detection at scale over large amounts of (potentially noisy) data (and associated inventory and logging at scale).	DE.CM.1; DE.AE.2	N	Big Data analysis/deep learning-based approaches are needed and are already being explored [49-54].
Changing networks and dynamism: delivering capacity to detect anomalies when "normal" is constantly	DE.AE.1	N	

shifting.			
How to provide comprehensible, actionable security-monitoring information to IIoT personnel (personnel may have a low level of cybersecurity expertise, or may need to monitoring while multitasking with other industrial tasks, for example).	PR.AT.1	Y	
Methods for integrating OT into the IT/IIoT monitoring and analysis workflows	ID.RA.4	Y	Explores practical IT-OT integration for safety monitoring in order to predict equipment failures and remove employees from hazardous situations [94].
Patch management			
Approaches to patch-management at scale, with associated methods for identifying priorities. Likely to require automated support given scale and dynamism of the estate.	PR.IP.4	N	Patch systems for keeping many heterogeneous devices updated in complex IoT environments [95, 96].
Patch strategies for environments where downtime is not an option.	PR.IP.4	Y	Exploration of the issue of timely software-update management in the IIoT [97]. Proposed quarantine mode-based live patching for zero-downtime safety-critical systems [98].
Boundary defences and firebreaks			
Assessment of the benefits of alternatives to boundary defence and network segmentation, for IIoT environments where boundaries are unclear or constantly shifting.	PR.PT.2	Y	Assessment of the benefits of defence-in-depth approaches for the IIoT [99].
Assessing the need for firebreaks: where, when and how to include non-smart components, hardware-based solutions and human processes.	PR.PT.3	Y	
Authentication and access			
Machine-to-machine (M2M) authentication protocols that can authenticate devices dynamically (potentially continuously). Includes need for human oversight mechanisms for ensuring trust in highly automated methods.	PR.AC.1	N	Lightweight M2M authentication schemes for resource-constrained IIoT environments [100, 101].
Scalable digital identity architectures for people, with support for continuous authentication in highly critical applications. Development of approaches will need to be supported by algorithms that can determine risk exposure related to	PR.AC.3	N	Decentralised digital-identity architectures including self-sovereign identity [102, 103].

digital identity and personal data.			
Access-control/ "need-to-know" paradigms for IIoT contexts such as smart cities.	PR.AC.2	Y	
Automated fall-back solutions			
Development of automated approaches to fall-back for critical systems, as in IIoT reliance on fall-back to manual methods and "dumb" instrumentation is likely to become infeasible. This includes the need for methods for protecting fall-back solutions (noting that automated, ML-based approaches may be required with associated attack surface)	RC.RP.1	Y	

5.3 Tests, Exercises and Simulations

There is a need to develop approaches to testing the security of IIoT systems (both live and simulated), and effectiveness of risk-control technologies. Approaches are also needed for simulating and exercising incident-response procedures for IIoT environments.

Research requirement	Gaps addressed	IIoT only?	State-of-the-art
Security-testing of live environments			
Vulnerability and resilience test strategies for external and insider threats, that can ensure continued safety and security even in live environments.	ID.RA.1; ID.RA.2	N	Graph-based and automated approaches for testing for and securing against vulnerability exploitation in IIoT systems [104, 105]. Digital twins for security-testing of factories of the future [106]. Review of cyber ranges and testbeds, including for IoT [107].
Exercising and evaluation of security approaches			
Development of best practice in incident-response exercises and simulations for the IIoT. Includes establishing characteristics of an effective exercise or simulation for enhancing incident response capabilities (for security operations teams, as well as wider leadership etc.). Includes the need for simulation environments to guide response in the IIoT specifically	RS.RP.1; RS.RP.2	Y	Assessment of the incident-response requirements of the IIoT [108].

5.4 Developing approaches to building the necessary cybersecurity skills and culture in the IIoT

There is a need to develop approaches that enable and incentivise the reporting and information-sharing culture that will be necessary to achieve security across the IIoT, as well as to develop training approaches that can meet the unique needs of IIoT personnel.

Research requirement	Gaps addressed	IIoT only?	State-of-the-art
Reporting and information-sharing structures and incentives			
Trust and incentives models that promote sharing of the necessary threat and risk information [43]. Including mechanisms that can promote information-sharing in the face of deterrents (reputational concerns, IP, etc.). Could be technical measures like cryptographic guarantees, but also legal or social systems.	RS.CO.2	N	Mechanism for secure cyber-attack information sharing between interdependent CI operators [109].
Methods to share at a pace appropriate to defend against threats in a highly connected IIoT (likely to require automated support).	RS.CO.1	N	
Incident-reporting structures for safety-security critical IIoT, able to span industry and jurisdictional boundaries	RS.CO.2; ID.RA.4	Y	
Threat-intelligence/information-sharing models that account for IT and OT which can span IT/OT data formats. The requirements of (OT relevant to) various IIoT sectors will differ	ID.RA.4	Y	Exploration of the requirements and challenges of information sharing in the IIoT [112].
Adapting training approaches to achieve the necessary workforce skills			
Solutions to meet the evolving training needs of personnel (including non-security personnel) with a range of different backgrounds and base knowledge, across a wide range of different industrial contexts with differing business priorities.	PR.AT.1; PR.AT.2; PR.AT.4	Y	Work towards agreement on key definitions (e.g., for accountability, data protection, privacy) is useful underpinning [113]. Development of approaches to teaching IIoT cybersecurity (targeting researchers and developers, rather than IIoT personnel) [114]. Development of gamified and testbed approaches to teaching industrial-control system cybersecurity [115, 116].
Training content adapted for IIoT dynamism and interdependency, potential harms, their criticality (e.g., including potential physical harms in safety-critical environments), and propagation characteristics.	PR.AT.3; PR.AT.2	Y	

Development of education to help leaders normalise IIoT cyber-risk into the broader risk management practice, and identify what services are required (e.g., outsourcing to cybersecurity consultancies [117]) Leaders will need to be able to comprehend and manage risks in the wider organisational context, including emerging risks and systemic risk.	PR.AT.1; PR.AT.2; PR.AT.3; PR.AT.4	Y	

5.5 Developing the necessary liability models and regulatory approaches

Research is needed to support the development of liability models and regulatory approaches that are appropriate for the IIoT, taking into account key factors such as the need to reconcile security and safety concerns.

Research requirement	**Gaps addressed**	**IIoT only?**	**State-of-the-art**
Liability models			
Liability models for vendors of technologies and services, and for users of IIoT devices. There would be value in research studying the form these liability models might take (how liability/responsibility might be assigned, and what the terms might be in terms of perpetuity and the conditions under which liability holds), how they would impact the markets, how they would be enforced.	"Liability"	Y	
Regulation			
Reconciling safety and security culture and regulation. While some such regulation is emerging (e.g., [84]), there is a need for research to evidence the balancing of safety and security needs in IIoT contexts.	"Safety-security regulation"	Y	
Development of models and reasoning frameworks for evaluating interplay between security and safety controls, and risk propagation in critical systems	"Safety-security regulation"	Y	

6 CONCLUSION

The research requirements are extensive. However, our conclusion is that whilst all of the above are needed in order to deliver operational cybersecurity in the IIoT, there is what amounts to a structural gap in our combined knowledge which should be central to a research agenda: There is significant potential for systemic and possibly hidden cyber-risk in the IIoT due to: common and pervasive vulnerabilities in tech; digital dependencies within sectors, across supply-chains, linking cyber and physical assets, and process control systems. Resilience and safety in the IIoT cannot be assumed. In order to address these issues, there are a number of capacity requirements which will need to be met and should form the goals for the community's research agenda in this space:

1. We need to be able to predict emergence of systemic risk, identify its emergence and respond for resilience.
2. We need to know how to deploy risk controls for optimal effect in limiting risk propagation throughout IIoT systems.
3. We need to develop approaches to testing the security of, and simulating and exercising security procedures for, IIoT environments.
4. We need to develop approaches to building the necessary cybersecurity skills and culture, that meet the unique needs of the IIoT and its personnel.
5. We need to develop policy (liability models and appropriate regulatory approaches) that can support the development of a secure IIoT.

We urgently require research investment into understanding the nature of this systemic risk. We need models and simulations for understanding and predicting aggregated and systemic risk. Upon this we can develop metrics and tools for preventing, detecting and responding to IIoT risk, we can create systemic risk scenarios for use by the science base in developing and testing new ideas, but also the professional community and policy makes when managing the IIoT and its deployment in our critical national infrastructures.

REFERENCES

[1] National Institute of Standards and Technology (NIST). Cybersecurity Framework v1.1. https://www.nist.gov/cyberframework [accessed 27 January 2021]

[2] Center for Internet Security. 2019. CIS Controls. https://www.cisecurity.org/controls/ [accessed 27 January 2021]

[3] ISO. ISO/IEC27001Informationsecuritymanagement. https://www.iso.org/isoiec-27001-information-security.html [accessed 27 January 2021]

[4] National Cyber Security Centre. CyberEssentials. https://www.cyberessentials.ncsc.gov.uk/ [accessed 27 January 2021]

[5] 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 27 January 2021]

[6] 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]

[7] 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 27 January 2021]

[8] IoT Security Institute. Smart cities & critical infrastructure framework. https://iotsecurityinstitute.com/iotsec/index.php/artefacts [accessed 27 January 2021]

[9] Fagan, M; Megas, KN; Scarfone, KA; Smith, M. (2020). NIST8259A, 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 27 January 2021]

[10] 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 27 January]

[11] D. Wu, A. Ren, W. Zhang, F. Fan, P. Liu, X. Fu, and J. Terpenny, "Cybersecurity for digital manufacturing," *Journal of manufacturing systems*, vol. 48, pp. 3–12, 2018.

[12] A. Ren, D. Wu, W. Zhang, J. Terpenny, and P. Liu, "Cyber security in smart manufacturing: survey and challenges," in *IIE Annual Conference. Proceedings*. Institute of Industrial and Systems Engineers (IISE), 2017, pp. 716–721.

[13] U. P. D. Ani, H. He, and A. Tiwari, "Review of cybersecurity issues in industrial critical infrastructure: manufacturing in

perspective," *Journal of Cyber Security Technology*, vol. 1, no. 1, pp. 32–74, 2017.

[14] J. C. Balda, A. Mantooth, R. Blum, and P. Tenti, "Cybersecurity and power electronics: Addressing the security vulnerabilities of the internet of things," *IEEE Power Electronics Magazine*, vol. 4, no. 4, pp. 37–43, 2017.

[15] J. McCarthy, D. Faatz *et al.*, "[project description] securing the industrial internet of things: Scenario-based cybersecurity for the energy sector (draft)," National Institute of Standards and Technology, Tech. Rep., 2019.

[16] A. S. Sani, D. Yuan, J. Jin, L. Gao, S. Yu, and Z. Y. Dong, "Cyber security framework for internet of things-based energy internet," *Future Generation Computer Systems*, vol. 93, pp. 849–859, 2019.

[17] L. Urquhart and D. McAuley, "Avoiding the internet of insecure industrial things," *Computer law & security review*, vol. 34, no. 3, pp. 450–466, 2018.

[18] L. Thames and D. Schaefer, *Cybersecurity for industry 4.0*. Springer, 2017.

[19] Y. Lu and L. Da Xu, "Internet of things (IoT) cybersecurity research: A review of current research topics," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 2103–2115, 2018.

[20] A.-R. Sadeghi, C. Wachsmann, and M. Waidner, "Security and privacy challenges in industrial internet of things," in *2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC)*. IEEE, 2015, pp. 1–6.

[21] G. Falco, C. Caldera, and H. Shrobe, "IIoT cybersecurity risk modeling for scada systems," *IEEE Internet of Things Journal*, vol. 5, no. 6, pp. 4486–4495, 2018.

[22] M. Lezzi, M. Lazoi, and A. Corallo, "Cybersecurity for industry 4.0 in the current literature: A reference framework," *Computers in Industry*, vol. 103, pp. 97–110, 2018.

[23] B. van Lier, "The industrial internet of things and cyber security: An ecological and systemic perspective on security in digital industrial ecosystems," in *2017 21st International Conference on System Theory, Control and Computing (ICSTCC)*. IEEE, 2017, pp. 641–647.

[24] P. Radanliev, D. De Roure, J. R. Nurse, R. Nicolescu, M. Huth, S. Cannady, and R. M. Montalvo, "Integration of cyber security frameworks, models and approaches for building design principles for the internet- of-things in industry 4.0," 2018.

[25] A. Hassanzadeh, S. Modi, and S. Mulchandani, "Towards effective security control assignment in the industrial internet of things," in *2015 IEEE 2nd World Forum on Internet of Things (WF-IoT)*. IEEE, 2015, pp. 795–800.

[26] A. Lamba, S. Singh, S. Balvinder, N. Dutta, and S. Rela, "Mitigating cyber security threats of industrial control systems (scada & dcs)," in *3rd International Conference on Emerging Technologies in Engineering, Biomedical, Medical and Science (ETEBMS–July 2017)*, 2017.

[27] L. A. Maglaras, K.-H. Kim, H. Janicke, M. A. Ferrag, S. Rallis, P. Fragkou, A. Maglaras, and T. J. Cruz, "Cyber security of critical infrastructures," *Ict Express*, vol. 4, no. 1, pp. 42–45, 2018.

[28] S. Shackelford, "Smart factories, dumb policy?: Managing cybersecurity and data privacy risks in the industrial internet of things," *Minnesota Journal of Law, Science & Technology*, pp. 18–80, 2020.

[29] J. Romero-Mariona, R. Hallman, M. Kline, J. San Miguel, M. Major, and L. Kerr, "Security in the industrial internet of things-the c-sec approach," in *International Conference on Internet of Things and Big Data*, vol. 2. SCITEPRESS, 2016, pp. 421–428.

[30] W. Schwab and M. Poujol, "The state of industrial cybersecurity 2018," *Trend Study Kaspersky Reports*, p. 33, 2018

[31] E. J. Colbert and A. Kott, *Cyber-security of SCADA and other Industrial Control Systems*. Springer, 2016, vol. 66.

[32] T. Macaulay and B. L. Singer, *Cybersecurity for industrial control systems: SCADA, DCS, PLC, HMI, and SIS*. CRC Press, 2011.

[33] L. J. Trautman and P. C. Ormerod, "Industrial cyber vulnerabilities: Lessons from Stuxnet and the internet of things," *U. Miami L. Rev.*, vol. 72, p. 761, 2017.

[34] G. Gardašević, L. Berbakov and A. Mastilović, "Cybersecurity of industrial internet of things," in *Cyber Security of Industrial Control Systems in the Future Internet Environment*. IGI Global, 2020, pp. 47–68.

[35] L. Maximilian, E. Markl and A. Mohamed, "Cybersecurity management for (industrial) internet of things: Challenges and opportunities," *J Inform Tech Softw Eng*, vol. 8, no. 250, p. 2, 2018.

[36] Z. Drias, A. Serhrouchni, and O. Vogel, "Analysis of cyber security for industrial control systems," in *2015 International Conference on Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC)*. IEEE, 2015, pp. 1–8.

[37] K. Tange, M. De Donno, X. Fafoutis, and N. Dragoni, 2020. A systematic survey of industrial internet of things security: Requirements and fog computing opportunities. *IEEE Communications Surveys & Tutorials, 22*(4), pp.2489-2520.

[38] Brass, I; Carr, M; Kruakae, P & Tanczer, L. (2019). Cybersecurity 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 27 January 2021]

[39] 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]

[40] P. Radanliev, R. M. Montalvo, S. Cannady, R. Nicolescu, D. De Roure, J. R. Nurse, and M. Huth, "Cyber security framework for the internet- of-things in industry 4.0," 2019.

[41] M. Paez and K. Tobitsch, "The industrial internet of things: Risks, liabilities, and emerging legal issues," *NYL Sch. L. Rev.*, vol. 62, p. 217, 2017.

[42] J. R. C. Nurse, S. Creese, and D. De Roure, "Security risk assessment in internet of things systems," *IT professional*, vol. 19, no. 5, pp. 20–26, 2017.

[43] I. Brass, K. Pothong, L. Tanczer, and M. Carr, "Standards, governance and policy. cybersecurity of the internet of things (IoT)," *PETRAS Stream Report*, 2019.

[44] M. Baldi, "Cybersecurity defense for industrial process-control systems," *Chemical Engineering*, vol. 123, no. 7, p. 36, 2016.

[45] M. Zolanvari, M. A. Teixeira, L. Gupta, K. M. Khan, and R. Jain, "Machine learning-based network vulnerability analysis of industrial internet of things," *IEEE Internet of Things Journal*, vol. 6, no. 4, pp. 6822–6834, 2019.

[46] S. Lee, S. Lee, H. Yoo, S. Kwon, and T. Shon, "Design and implementation of cybersecurity testbed for industrial iot systems," *The Journal of Supercomputing*, vol. 74, no. 9, pp. 4506–4520, 2018.

[47] B. Craggs, A. Rashid, C. Hankin, R. Antrobus, O. Serban, and N. Thapen, "A reference architecture for IIoT and industrial control systems testbeds," 2019.

[48] M. Arnaert, Y. Bertrand, and K. Boudaoud, "Modeling vulnerable internet of things on shodan and censys: An ontology for cyber security," in *Proceedings of the Tenth International Conference on Emerging Security Information, Systems and Technologies (SECUREWARE 2016), Nice, France*, 2016, pp. 24–28.

[49] B.B. Zarpelaõ, R.S. Miani, C.T. Kawakani, and S.C. de Alvarenga, "A survey of intrusion detection in internet of things," *Journal of Network and Computer Applications*, vol. 84, pp. 25–37, 2017.

[50] A.-H. Muna, N. Moustafa, and E. Sitnikova, "Identification of malicious activities in industrial internet of things based on deep learning models," *Journal of Information security and applications*, vol. 41, pp. 1–11, 2018.

[51] M. Wu, Z. Song, and Y. B. Moon, "Detecting cyber-physical attacks in cyber manufacturing systems with machine learning methods," *Journal of intelligent manufacturing*, vol. 30, no. 3, pp. 1111–1123, 2019.

[52] L. Zhou and H. Guo, "Anomaly detection methods for IIoT networks," in *2018 IEEE International Conference on Service Operations and Logistics, and Informatics (SOLI)*. IEEE, 2018, pp. 214–219.

[53] G. De La Torre, P. Rad, and K.-K. R. Choo, "Implementation of deep packet inspection in smart grids and industrial internet of things: Challenges and opportunities," *Journal of Network and Computer Ap- plications*, 2019.

[54] M. H. ur Rehman, I. Yaqoob, K. Salah, M. Imran, P. P. Jayaraman, and C. Perera, "The role of big data analytics in industrial internet of things," *Future Generation Computer Systems*, vol. 99, pp. 247–259, 2019.

[55] G. Settanni, F. Skopik, A. Karaj, M. Wurzenberger, and R. Fiedler, "Protecting cyber physical production systems using anomaly detection to enable self-adaptation," in *2018 IEEE Industrial Cyber-Physical Systems (ICPS)*. IEEE, 2018, pp. 173–180.

[56] NIST Information Technology Laboratory Computer Security Resource Centre. Lightweight Cryptography project. https://csrc.nist.gov/Projects/lightweight-cryptography [accessed 1 February 2021]

[57] L. Belli, "BRICS countries to build digital sovereignty. In L. Belli (eds) CyberBRICS. Springer, Cham.

https://doi.org/10.1007/978-3-030-56405-6_7 [Accessed 1 February 2021]

[58] A. Laszka, W. Abbas, Y. Vorobeychik, and X. Koutsoukos, "Synergistic security for the industrial internet of things: Integrating redundancy, diversity, and hardening," in *2018 IEEE International Conference on Industrial Internet (ICII)*. IEEE, 2018, pp. 153–158.

[59] K.-K. R. Choo, S. Gritzalis, and J. H. Park, "Cryptographic solutions for industrial internet-of-things: Research challenges and opportunities," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 8, pp. 3567– 3569, 2018.

[60] C. Vijayakumaran, B. Muthusenthil, and B. Manickavasagam, "A reliable next generation cyber security architecture for industrial internet of things environment." *International Journal of Electrical & Computer Engineering (2088-8708)*, vol. 10, 2020.

[61] M. Mylrea and S. N. G. Gourisetti, "Blockchain for supply chain cybersecurity, optimization and compliance," in *2018 Resilience Week (RWS)*. IEEE, 2018, pp. 70–76.

[62] CyberX (2020). 2020 global IoT/ICS risk report. https://cyberx-labs.com/resources/risk-report-2020/ [accessed on 27 January 2021]

[63] 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/report/investigation-wannacry-cyber-attack-and-the-nhs/ [accessed 27 January 2021]

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

[65] S. Karnouskos, (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]

[66] M. Höst, J. Sönnerup, M. Hell, and T. Olsson, 2018. Industrial practices in security vulnerability management for iot systems–an interview study. In *Proceedings of the International Conference on Software Engineering Research and Practice (SERP)* (pp. 61-67). The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp).

[67] M. Asplund and S. Nadjm-Tehrani, 2016. Attitudes and perceptions of IoT security in critical societal services. *IEEE Access*, *4*, pp.2130-2138.

[68] S. Creese, R. Hannigan, A. El Kaafarani, L. Axon, K. Fletcher, A. Schuler Scott, and M. Stolz, "Foresight Review of Cyber Security for the Industrial IoT", Lloyd's Register Foundation, July 2020: https://www.lrfoundation.org.uk/en/news/cybersecurity-foresight-review/ (link as of 26/10/20).

[69] H. Boyes, B. Hallaq, J. Cunningham, and T. Watson, 2018. The industrial internet of things (IIoT): An analysis framework. *Computers in industry*, *101*, pp.1-12.

[70] S. Mitchell, 2018. Managing shared risks in interdependent systems of smart cities. *Internet of Things, for Things, and by Things*, ch.8, p.156.

[71] S. Creese, J. Saunders, L. Axon and W. Dixon, 2020. Future Series: Cybersecurity, emerging technology and systemic risk. World Economic Forum.

[72] FireEye, December 13 2020, Highly evasive attacker leverages SolarWinds supply chain to compromise multiple global victims with SUNBURST backdoor. FireEye Threat Research. https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html [accessed on 27 January 2021]

[73] Industrial Internet Consortium, 2016. Industrial Internet of Things: Security Framework. https://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB-3.pdf [accessed on 27 January 2021]

[74] National Institute of Standards and Technology, 2018. Path Forward to Support Adaptation and Adoption of Cybersecurity Framework. https://www.nist.gov/system/files/documents/2018/02/06/session_iii_-_barrett_csf.pdf [accessed on 27 January 2021]

[75] Z. M. Fadlullah and M. M. Fouda, 2020. Authentication Methodology for Securing Machine-to-Machine Communication in Smart Grid. In *Combating Security Challenges in the Age of Big Data* (pp. 189-213). Springer, Cham.

[76] The Heartbleed Bug. https://heartbleed.com/ [accessed on 1 February 2021]

[77] Postscapes, 2020. IoT Standards and Protocols. https://www.postscapes.com/internet-of-things-protocols/ [accessed on 2 February 2021]

[78] Cisco Press, 2019. IoT and Security Standards and Best Practices. https://www.ciscopress.com/articles/article.asp?p=2923211&seqNum=4 [accessed on 2 February 2021]

[79] European Commission, 2019. The EU Cybersecurity Act. https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-act [accessed on 2 February 2021]

[80] National Institute of Standards and Technology (NIST), 2020. Recommendations for IoT Device Manufacturers. https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8259-draft2.pdf [accessed on 2 February 2021]

[81] UK Government, 2020. Press Release: Government to strengthen security of internet-connected products. https://www.gov.uk/government/news/government-to-strengthen-security-of-internet-connected-products [accessed on 2 February 2021]

[82] California Legislative Information, 2018. Information Privacy: Connected Devices. https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB327 [accessed on 2 February 2021]

[83] Ponemon Institute, 2020. The Economic Value of Prevention in the Cybersecurity Lifecycle. https://ponemonsullivanreport.com/2020/04/the-economic-value-of-prevention-in-the-cybersecurity-lifecycle/ [accessed on 2 February 2021]

[84] European Union Aviation Safety Agency, 2019. NPA 2019-01 Aircraft Cybersecurity. https://www.easa.europa.eu/document-library/notices-of-proposed-amendment/npa-2019-01 [accessed on 31 August 2021]

[85] B. Zahran, A. Hussaini, and A. Ali-Gombe, 2021. IIoT-ARAS: IIoT/ICS Automated Risk Assessment System for Prediction and Prevention. In *Proceedings of the Eleventh ACM Conference on Data and Application Security and Privacy* (pp. 305-307).

[86] V. Puri, I. Priyadarshini, R. Kumar and L. C. Kim, 2020. Blockchain meets IIoT: An architecture for privacy preservation and security in IIoT. In *2020 International Conference on Computer Science, Engineering and Applications (ICCSEA)* (pp. 1-7). IEEE.

[87] N. Sheikh, M. Pawar and V. Lawrence, 2021. Zero trust using Network Micro Segmentation. In *IEEE INFOCOM 2021-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)* (pp. 1-6). IEEE.

[88] National Institute of Standards and Technology, 2020. Zero Trust Architecture. https://www.nist.gov/publications/zero-trust-architecture?TB_iframe=true&width=921.6&height=921.6 [accessed on 31 August 2021]

[89] M. Samaniego and R. Deters, 2018, July. Zero-trust hierarchical management in IoT. In *2018 IEEE international congress on Internet of Things (ICIOT)* (pp. 88-95). IEEE.

[90] S. Malik, V. Dedeoglu, S. S. Kanhere and R. Jurdak, 2019. Trustchain: Trust management in blockchain and iot supported supply chains. In *2019 IEEE International Conference on Blockchain (Blockchain)* (pp. 184-193). IEEE.

[91] J. Lyle, 2011. *Trustworthy services through attestation* (Doctoral dissertation, Oxford University, UK).

[92] R. F. Babiceanu and R. Seker, 2019. Cyber resilience protection for industrial internet of things: A software-defined networking approach. *Computers in Industry*, *104*, pp.47-58.

[93] H. Peng, Z. Qian, Z. Kan, D. Zhao, J. Yu and J. Han, 2021. Cascading Failure Dynamics against Intentional Attack for Interdependent Industrial Internet of Things. *Complexity*, *2021*.

[94] P. Lipnicki, D. Lewandowski, D. Pareschi, W. Pakos and E. Ragaini, 2018. Future of IoTSP–IT and OT integration. In *2018 IEEE 6th International Conference on Future Internet of Things and Cloud (FiCloud)* (pp. 203-207). IEEE.

[95] J. Lee, 2018. Patch transporter: Incentivized, decentralized software patch system for WSN and IoT environments. *Sensors*, *18*(2), p.574.

[96] K. Kolomvatsos, 2018. An intelligent, uncertainty driven management scheme for software updates in pervasive IoT applications. *Future generation computer systems*, *83*, pp.116-131.

[97] I. Mugarza, J.L. Flores and J.L. Montero, 2020. Security Issues and Software Updates Management in the Industrial Internet of

Things (IIoT) Era. *Sensors*, *20*(24), p.7160.

[98] I.M. Inchausti, E.J. Taquet and J.P. Molina, 2019. *Quarantine-mode based live patching for zero downtime safety-critical systems* (Doctoral dissertation, Universidad del País Vasco-Euskal Herriko Unibertsitatea).

[99] A. Mosteiro-Sanchez, M. Barcelo, J. Astorga and A. Urbieta, 2020. Securing IIoT using defence-in-depth: towards an end-to-end secure industry 4.0. *Journal of Manufacturing Systems*, *57*, pp.367-378.

[100] A. Esfahani, G. Mantas, R. Matischek, F. B. Saghezchi, J. Rodriguez, A. Bicaku, S. Maksuti, M. G. Tauber, C. Schmittner and J. Bastos, 2017. A lightweight authentication mechanism for M2M communications in industrial IoT environment. *IEEE Internet of Things Journal*, *6*(1), pp.288-296.

[101] E. Lara, L. Aguilar, M. A. Sanchez and J. A. García, 2020. Lightweight authentication protocol for M2M communications of resource-constrained devices in industrial Internet of Things. *Sensors*, *20*(2), p.501.

[102] G. Goodell and T. Aste, 2019. A Decentralized Digital Identity Architecture. *Frontiers in Blockchain*, *2*, p.17.

[103] G. Fedrecheski, J.M. Rabaey, L.C. Costa, P.C.C Ccori, W.T. Pereira and M.K. Zuffo, 2020, June. Self-sovereign identity for IoT environments: a perspective. In *2020 Global Internet of Things Summit (GIoTS)* (pp. 1-6). IEEE.

[104] G. George and S.M. Thampi, 2018. A graph-based security framework for securing industrial IoT networks from vulnerability exploitations. *IEEE Access*, *6*, pp.43586-43601.

[105] N. Moustafa, B. Turnbull and K.K.R. Choo, 2018. Towards automation of vulnerability and exploitation identification in IIoT networks. In *2018 IEEE International Conference on Industrial Internet (ICII)* (pp. 139-145). IEEE.

[106] A. Becue, E. Maia, L. Feeken, P. Borchers and I Praca, 2020. A new concept of digital twin supporting optimization and resilience of factories of the future. *Applied Sciences*, *10*(13), p.4482.

[107] E. Ukwandu, M.A.B. Farah, H. Hindy, D. Brosset, D. Kavallieros, R. Atkinson, C. Tachtatzis, M. Bures, I. Andonovic, and X. Bellekens, 2020. A review of cyber-ranges and test-beds: Current and future trends. *Sensors, 20*(24), p.7148.

[108] A. Cook, L. Maglaras, R. Smith and H. Janicke, 2018. Managing incident response in the industrial internet of things. *International Journal of Internet Technology and Secured Transactions*, *8*(2), pp.251-276.

[109] F. Adamsky, M. Aubigny, F. Battisti, M. Carli, F. Cimorelli, T. Cruz, A. Di Giorgio, C. Foglietta, A. Galli, A. Giuseppi and F. Liberati, 2018. Integrated protection of industrial control systems from cyber-attacks: the ATENA approach. *International Journal of Critical Infrastructure Protection*, *21*, pp.72-82.

[110] P.K. Garimella, 2018, October. IT-OT integration challenges in utilities. In *2018 IEEE 3rd International Conference on Computing, Communication and Security (ICCCS)* (pp. 199-204). IEEE.

[111] M. Felser, M. Rentschler and O. Kleineberg, 2019. Coexistence standardization of operation technology and information technology. *Proceedings of the IEEE*, *107*(6), pp.962-976.

[112] N. Ulltveit-Moe, H. Nergaard, L. Erdödi, T. Gjøsæter, E. Kolstad and P. Berg, 2016. Secure information sharing in an industrial Internet of Things. *arXiv preprint arXiv:1601.04301*.

[113] isITethical, Key Terms, https://www.isitethical.org/key-terms/ [accessed 31 August 2021]

[114] T.M. Fernández-Caramés and P. Fraga-Lamas, 2020. Use case based blended teaching of IIoT cybersecurity in the industry 4.0 era. *Applied Sciences*, *10*(16), p.5607.

[115] D. Antonioli, H. R. Ghaeini, S. Adepu, M. Ochoa and N. O. Tippenhauer, 2017. Gamifying ICS security training and research: Design, implementation, and results of S3. In *Proceedings of the 2017 Workshop on Cyber-Physical Systems Security and PrivaCy* (pp. 93-102).

[116] A.P. Mathur and N.O. Tippenhauer, 2016. SWaT: A water treatment testbed for research and training on ICS security. In *2016 international workshop on cyber-physical systems for smart water networks (CySWater)* (pp. 31-36). IEEE.

[117] Deloitte, Industrial Internet of Things (IIoT) Security Services, https://www2.deloitte.com/us/en/pages/risk/solutions/industrial-internet-of-things-and-cybersecurity.html [accessed on 31 August 2021]