PETRAS

Industry Briefing

IoT in the Supply Chain & Control Systems Sector

Dr Zakiyya Adam
Edited by:
Prof. Pete Burnap

About PETRAS

The PETRAS National Centre of Excellence aims to ensure that technological advances in the Internet of Things (IoT) are developed and applied in consumer and business contexts, safely and securely. This is done by considering social and technical issues relating to the cybersecurity of IoT devices, systems and networks.

The Centre is a consortium of 22 research institutions and the world's largest socio-technical research centre focused on the future implementation of the Internet of Things. The research institutions are: University College London, Imperial College London, University of Oxford, Lancaster University, University of Warwick, University of Southampton, Newcastle University, University of Nottingham, University of Bristol, Cardiff University, University of Edinburgh, University of Surrey, Coventry University, Northumbria University, Tate, University of Glasgow, Cranfield University, De Montfort University, Durham University, University of Manchester, Royal Holloway, University of London, and University of Strathclyde.

As the research wing of UKRI's Security of Digital Technologies at the Periphery (SDTaP) Programme, PETRAS runs open, national level funding calls which enable us to undertake cutting edge basic and applied research. We also support the early adoption of new technologies through close work with other members of the SDTaP programme, such as InnovateUK, supporting demonstrations of new technology and commercialisation processes.

Further information can be found at https://petras-iot.org/about-us

In addition, we build the capacity of the UK to remain a world leader in IoT through our training and development programmes for early career researchers. Finally, we offer consultancy services to the public and private sectors to provide decision makers with insight and advice on a range of cybersecurity related issues.

The wider PETRAS community has played a role in creating this report - in particular Prof Pete Burnap, Sector Lead for Supply Chains and Control Systems at PETRAS, at Cardiff University for his critical role in review, and Emilie Didier from the PETRAS Business Development Team for her editorial overview.

Design work by Dr Catherine Wheller is based on original work by Dr Michael Stead.

This report should be referenced as follows:

Adam, Z. 2021. IoT in the Supply Chain & Control Systems Sector A PETRAS Baseline Report, PETRAS National Centre of Excellence for IoT Systems Cybersecurity, London, UK

DOI:

From the Director

It is my pleasure to present this Industry Briefing on Cybersecurity for the Internet of Things and Artificial Intelligence at the intersection between digital infrastructure and critical national infrastructure. This is the fifth in a series of Industry Briefings, intended to link with and inform the six PETRAS Sectors: Ambient Environment, Supply Chains and Control Systems, Infrastructure, AgriTech, Health and Wellbeing, and Transport and Mobility.

PETRAS has a large network of industry partners and expert academics, and works directly in collaboration with these and government partners to ensure that research can be directly applied to benefit society, business and the economy. I am delighted to see that as a Centre dedicated to identifying and addressing some of the needs within IoT, PETRAS has managed to connect industry with social and physical scientists to work towards some of the major challenges and questions around the cybersecurity of the Internet of Things. As IoT technology develops at speed and embraces AI and machine learning 'at the Edge', so do the challenges around cybersecurity and systems, and it is critical that these are addressed by industry, government and academia.

We hope that these Industry Briefings, which have highlighted insights into the challenges of deploying IoT systems, provide a fresh perspective on the existing and emerging opportunities for industry and those working within the Transport and Mobility sector. With exciting innovative ideas, we are positive that PETRAS will be able to encourage collaboration between academia and industry, supporting the opportunities these challenges present, and we look forward to opening these discussions.

I hope this Industry Briefing will catalyse further debate and collaboration between researchers and users, making the use of the IoT safe and trustworthy, and maximising its social and economic value to the UK.

Professor Jeremy Watson CBE FREng
Director of the PETRAS National Centre of Excellence

Contents

PETRAS

THE PETRAS NATIONAL
CENTRE OF EXCELLENCE
FOR IoT SYSTEMS
CYBERSECURITY

Executive Summary

The Supply Chain and Control Systems sector is increasingly adopting digital and connected technologies. Supply chains utilise both external and internal real-time data to boost visibility enabling faster and better decision making. Use of IoT-technology within Industrial Control Systems (ICS) enables more efficiency, system scalability, performance accuracy and capital savings. Whilst adoption of these technologies brings numerous benefits to both supply chains and control systems, they also introduce new risks and challenges, such as cybersecurity concerns.

Based on research undertaken over the last few years, this brief offers insights into general trends and challenges in cybersecurity research and policy for IoT devices within the Supply Chain and Control Systems sector.

Challenges

Wide adoption of IoT technology in the sector poses numerous challenges, including:

- **Cybersecurity** concerns need to be identified, assessed and managed. For supply chains, this needs to account for the risk analyses of their partners across the network.
- **Safety** must be addressed, separately to – but in harmony with - cybersecurity, ensuring that unintentional harm is not caused as a result of technological upgrades. This is of particular importance in safety-critical systems.
- **Data** management needs to ensure that data confidentiality and privacy are protected, maintain data integrity, and facilitate effective data sharing practices.
- **Certification** compliance needs to be assured at all times, despite the increasing risk of malicious manipulation of manufacturing processes.

Policy

There are a range of frameworks and standards providing guidance for supply chains and control systems, including:

- The **Cyber Assessment Framework** is a set of 14 cybersecurity & resilience principles, one of which focuses on supply chains;
- In May 2021, the UK Government put out a **call for views** on cybersecurity in supply chains and Managed Service Providers, which will contribute to the development of policy solutions;
- The **NCSC has developed a series of 12 principles**, designed to help businesses establish effective control and oversight of their supply chains;
- A **range of standards** focused on the cybersecurity of (1) supply chains, including ISO 28000:2007 and ISO/IEC 27036, and (2) control systems, including BS EN / IEC 62443, ISO/IEC 27000 and ISA TR84.00.09-2013;

- The US **Executive Order 14017** looks to review and improve the resilience of critical supply chains;
- The revised EU Network and Information Security (NIS) Directive, **NIS2**, accounts for cybersecurity of the supply chain;
- The EU **Data Act** is intended to support data sharing between businesses;
- **NIST's Guide to Industrial Control Systems (ICS) Security** which provides guidance on how to secure ICS;
- **ICS-CERT**, in the US, have published a series of guidance documents for best practice with regards to cybersecurity of ICS.

Opportunities

The challenges posed by the increased use of connected technologies in supply chains and control systems raise the opportunity for further research. Broad areas of interest include:

- **Safer connectivity** in manufacturing factories, with regards to cybersecurity;
- Understanding the **value of data** in manufacturing;
- **Logistical** supply chain issues;
- **Technological** supply chain obstacles;
- **Decision making and policy challenges;**
- Understanding the overlap between **certification requirements and compliance with cybersecurity standards**;
- Optimal **architecture configuration** of edge devices

PETRAS has rich and expanding experience of working within the sector, and is well-placed to face the privacy, ethics, trust, reliability, acceptability, and security concerns that will emerge as IoT becomes increasingly more integral to our supply chain networks and control systems.

1. Introduction

1.1 Scope of this brief

This brief offers a summary of general trends and challenges in cybersecurity research and policy for IoT (Internet of Things) devices and in the Supply Chain and Control Systems sector. The geographic scope encompasses the UK, EU and the global level, based on research collected up to 2021. In addition, the document will offer insights into PETRAS activities that focus on supply chains and control systems.

The intended audience is primarily external industry and government organisations, including small, medium and large companies working around IoT, AI, security and cybersecurity in the Supply Chain and Control Systems sector, who would like to gain insights into PETRAS's work

1.2 Sector background

The use of IoT devices within supply chains and control systems is growing. 73% of Chief Supply Chain Officers reported that their organisations are increasingly using both external and internal real-time data to help them boost visibility so they can make faster and better decisions, according to Accenture's Business Futures 2021 report [1].

Mitigating cybersecurity-related risks is of growing importance due to both the rise in the production of data and the inclusion of IoT-enabled devices (i.e. edge devices) into systems traditionally separated from IT systems for security reasons. Whilst this report focuses on supply chains and control systems more broadly, Industry 4.0 also plays an integral role in this landscape.

Supply Chains

Supply chains are global networks of organisations that cooperate to improve the flows of material and information between suppliers and customers at the lowest cost and the highest speed [2]. They include the entirety of operations from procurement of raw materials and manufacturing, to distribution and sale of goods [3].

Control Systems

Control systems are used to maintain a desired result or value. For example, a room thermostat that switches the heater on or off to achieve the required room temperature [4].

Industrial Control Systems (ICS) are mainly used to control the overall structure of a production plant, or equipment, and to achieve the desired production goals according to the specifications and requirements. Use of IoT-technology within ICS enables more efficiency, system scalability, performance accuracy and capital savings [5].

Control systems feature throughout the supply chain, are crucial to the safe and effective operation of the supply chain, and may be vulnerable to cyber attacks.

Industry 4.0

Industry 4.0 - also referred to as Smart Manufacturing [6] - considers the integration of the factory with the entire product lifecycle and supply chain activities. Industry 4.0 relies on the adoption of digital technologies to gather and analyse data in real time, providing useful information to the manufacturing system [7].

The rise of IoT, cloud services, big data and AI allow the creation of the physical-to-digital-to-physical (PDP) loop concept of Industry 4.0. Throughout this cycle, real-time access to data and intelligence is driven by the continuous and cyclical flow of information and actions between the physical and digital worlds [8].

2. Challenges

Numerous challenges arise regarding the use of IoT technology within supply chains and control systems. This section explores the main challenges in how they relate to both supply chains and control systems, and concludes by summarising the key challenges specific to Industry 4.0.

2.1.1 Cybersecurity

Increasing points of connectivity in a system result in a greater number of potential attack vectors. Thus, as the adoption of IoT technologies expands in the sector, so does the importance of, and challenge posed by, cybersecurity.

The European Union Agency for Network and Information Security (ENISA) report that supply chain attacks increased in number and sophistication in the year 2020 [9]. This trend is continuing in 2021, posing an increasing risk for organisations. It is estimated that there will be four times as many supply chain attacks in 2021 than in 2020. With regards to control systems, globally, during the first half of 2021 over a third (33.8%) of ICS computers were attacked [10].

Case Study 1

The ICS attack on Colonial Pipeline Co. in the United States in May 2021, had long-lasting and far-reaching effects. Colonial Pipeline, which controls nearly half the gasoline, jet fuel and diesel flowing along the East Coast, decided to turn off the pipeline to prevent the malware that had infected its back-office functions from spreading into the pipeline's operating system. Even after it paid the extortionists nearly $5 million in digital currency to recover its data, the process of decrypting the data and turning the pipeline back on again was very slow, taking days before the East Coast could get back to normal. A confidential assessment prepared by the Energy and Homeland Security Departments found that the country could only afford another 3 -5 days with the Colonial Pipeline shut down before buses and other mass transit would have to limit operations due to a lack of diesel fuel. Chemical factories and refinery operations would also shut down because there would be no way to distribute what they produced. The ICS attack on the Colonial Pipeline had ramifications that extended far beyond its own operations, impacting other industries in the supply chain [11] [12].

Case Study 2

SolarWinds is considered to be one of the largest supply chain attacks of the last few years. Affected entities included governmental organisations (including the US Treasury and the Departments of Homeland Security, State, Defence and Commerce) and large corporations (including Microsoft, Intel and Cisco), and it led to policy initiatives around the globe [9]. SolarWinds is a company that supplies management and monitoring software; Orion is SolarWinds' Network Management System (NMS) product. In December 2020, it was discovered that Orion had been compromised. An extensive investigation showed that attackers gained access to the SolarWinds network and used a routine software update to slip malicious code into Orion's software. 18,000 customers were estimated to have downloaded the code between March and June 2020. Once compromised, the attackers collected information for an extended period of time [14].

2.1.1.1 Supply Chains

Supply chain attacks leverage the interconnectedness of the global markets. When multiple customers rely on the same supplier, the consequences of a cyber-attack against this supplier are amplified, potentially resulting in a large-scale national, or even cross-border, impact. The Cyber Security Breaches Survey 2021 found that only 12% of businesses review risks coming from immediate suppliers, and 5% address risks coming from wider supply chains [13].

The ENISA report published in July 2021, Threat Landscape for Supply Chain Attacks, distinguishes between the four key elements in a supply chain:

(1) **Supplier**: entity that supplies a product or service to another entity;
(2) **Supplier Assets**: valuable elements used by the supplier to produce the product/ service;
(3) **Customer**: entity that consumes the product/ service produced by the supplier;
(4) **Customer Assets**: valuable elements owned by the target.

ENISA defines a supply chain attack as a **combination of at least two attacks**. The first attack is on a supplier that is then used to attack the target to gain access to its assets. The target can be the final customer or another supplier. For an attack to be classified as a supply chain one, both the supplier and the customer have to be targets.

ENISA has developed a **taxonomy to characterise supply chain attacks** [9]. It identifies the attack techniques utilised and assets targeted for both suppliers and customers; these are listed in Table 1, with an example for each presented in brackets.

2.1.1.2 Control Systems

The US Cybersecurity and Infrastructure Security Agency (CISA), the US Department of Energy (DOE), and the UK National Cyber Security Centre (NCSC) released joint guidance, titled *Cybersecurity Best Practices for Industrial Control Systems* [15]. The document identified the short-term and long-term impacts of a cybersecurity attack on a control system:

Short-term impacts: (1) operational shut downs; (2) loss of visibility over production and safety systems; (3) financial loss due to outages and downtime; (4) intellectual prop

Table 1: ENISA's proposed taxonomy for supply chain attacks [9]

SUPPLIER		CUSTOMER	
Attack Techniques Used to Compromise the Supplier	**Supplier Assets Targeted by the Supply Chain Attack**	**Attack Techniques Used to Compromise the Customer**	**Customer Assets Targeted by the Supply Chain Attack**
Malware Infection (spyware used to steal credentials from employees)	Pre-existing Software (software used by the supplier)	Trusted Relationship (trust an automatic update)	Data (payment data)
Social Engineering (phishing)	Software Libraries (software packages installed from third parties)	Drive-by Compromise (malicious scripts in a website to infect users with malware)	Personal Data (customer data)
Brute-Force Attack (guessing a web login)	Code (source code)	Phishing (messages impersonating the supplier)	Intellectual Property
Exploiting Software Vulnerability (SQL injection)	Configurations (passwords)	Malware Infection (ransomware)	Software (access to the customer product source code)
Exploiting Configuration Vulnerability (taking advantage of a configuration problem)	Data (personal data)	Physical Attack or Modification (modify hardware)	Processes (insertion of new malicious processes, documents of schematics)
Open-Source Intelligence (search online for credentials)	Processes (updates)	Counterfeiting (create a fake USB)	Bandwidth (use the bandwidth to send SPAM or to infect others on a large scale)
	Hardware (hardware produced by the supplier)		Financial (steal cryptocurrency)
	People (targeted individuals with access to data, infrastructure, or to other people)		People (individuals targeted due to their position or knowledge)
	Supplier		

erty theft; (5) health and personal safety risks; (6) damage and destruction of property and equipment; (7) loss of availability; (8) loss of control; and (9) denial of service.

Long-term impacts: (1) significant unplanned labour, overtime, and idle equipment costs; (2) increased or denied insurance; (3) degraded equipment performance and quality; (4) fees and lawsuits due to negligence or non-compliance; (5) loss of customers; and (6) redirection of organisational expenditure toward recovery efforts.

The Department of Homeland Security [16] in the United States identified the following ICS **attack methods**: (1) exploiting weak authentication; (2) brute force intrusion; (3) abuse of access authority; (4) network scanning/probing; (5) spear phishing; (6) removable media; (7) SQL injection.

Moving towards **cloud-computing** for ICSs

introduces new threats and vulnerabilities [17]:
(1) ICS managers have **limited security controls over the data,** resulting in loss of data privacy and opening up an easy point of illegal access to the assets;
(2) **loss of connection** with the remote components from the local devices or vice versa, resulting in a threat of loss of data, delays in the production process etc;
(3) **abuse of current flaws** in the local security controls by other remote cloud users, resulting in a threat of data breach, data theft, data manipulation, data exploitation, etc;
(4) lack of **security standardisation** for cloud-based ICSs.

2.1.2 Safety

Safety is a consideration related to but distinct from (cyber)security. In control systems, it may be considered to be of even greater significance than cybersecurity.

Whilst security is concerned with intentional harm (i.e. malicious acts), safety is focused on **unintentional harm** (i.e. accidents) [18]. The addition of new security defences in an attempt to mitigate security threats may actually introduce safety concerns. For example, a nuclear power plant in Georgia was shut down for 48 hours after a software update was installed on one of the computers on the plant's corporate network. The lack of data after the computer reset post-update was interpreted as a significant change in the physical process causing the emergency safety system to shut down the plant [19]. Security solutions should take these safety concerns into account when designing and deploying new security mechanisms [20].

A **safety-critical system** executes critical tasks, whose failure could endanger human life, lead to substantial economic loss, or cause extensive environmental damage [21]. In February 2021, a hacker infiltrated a computer at a Florida city's water treatment plant and briefly increased the amount of sodium hydroxide, also known as lye, by a factor of more than 100. In large quantities it can cause irritation, burns and other complications. A supervisor noticed the measurements of the chemical changing on his computer screen and stepped in to reverse the action, leaving the city's water supply unaffected [22]. The breach could potentially have led to mass poisoning, putting the lives of thousands of Florida residents at risk.

2.1.3 Data

2.1.3.1 Supply Chains

Supply chains rank amongst the most data-rich of all business environments. Creation of a flexible, responsive, reliable and resilient supply chain is not possible without the necessary volume and quality of associated data. That data unlocks the ability to: (1) accelerate inventory turnover; (2) reduce the number and frequency of defects; (3) increase responsiveness and efficiency within supply networks; (4) improve risk and loss management; and (5) reduce costs and increase business efficiency [23]. However, there are numerous data-related challenges that need to be addressed.

Confidentiality and Privacy

Confidentiality involves maintaining the privacy of the information flow throughout the horizontal and the vertical value chains of the manufacturing system. In digital supply chains there are many information flows which could be tapped by attackers. Confidentiality loss can be costly for a company; resulting in loss of customer's data, intellectual property, trade secrets, etc. Hence, proper mechanisms (such as end-to-end encryption and access control) need to be incorporated to ensure confidentiality of the system [24].

Data Integrity

Data integrity is defined as *the property that data has not been changed, destroyed, or lost in an unauthorised or accidental manner* [25]. An attack against data integrity can cause corruption, modification, and/or destruction of the data which ultimately results in a loss in trust in the data. Integrity is part of the CIA security triad of Confidentiality, Integrity, and Availability [26].

Ransomware, destructive malware, insider threats, and even honest user mistakes present ongoing threats to organisations. Organisations' data, such as database records, system files, configurations, user files, applications, and customer data, are all potential targets [26].

Data Sharing

A Delphi study exploring antecedents associated with information sharing across multiple supply chain tiers, identified 22 factors that pose challenges to information sharing beyond the dyadic relationships. They also found that certain factors, such as trust, are regarded as barriers i.e. too difficult to resolve for implementing multi-tier information sharing [27]. The 22 factors were grouped into 6 categories: information utilisation, technology utilisation, power structures, culture, business process, and legal. These are presented in Figure 2 1 and some key aspects of each category are summarised below.

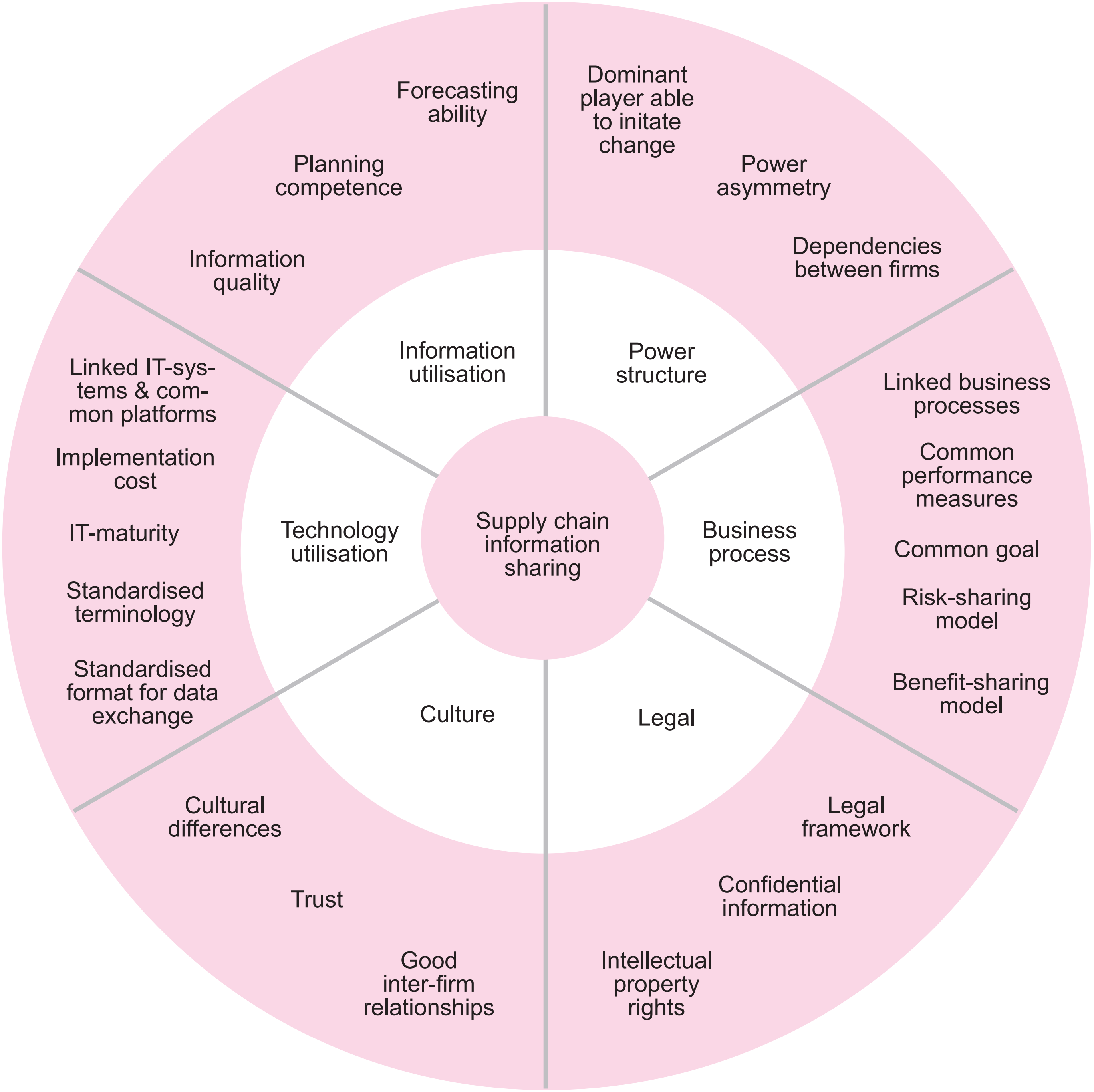

Figure 2 1: Factors that pose challenges to information sharing across multiple supply chain tiers (adapted from K. Timmermans, 2021)

Information Utilisation. Low information quality makes it difficult to plan logistics and production related activities. Low information quality also relates to (1) delayed information - decisions are made on “old” and potentially incorrect information; (2) misinterpreted information - receiver needs to understanding how the information was generated; and (3) difficulty in aggregating information.

Technology Utilisation. Refers to the various means for sharing, receiving and making sense of transmitted information. Even though the technology is available, the dynamics of networks pose a challenge for multi-tier information sharing. As companies are involved in numerous supply chains, the task of connecting suppliers and customers across multiple tiers becomes a cumbersome and costly undertaking over time.

Power Structures. Relates to inter-dependencies between firms and a company’s power/ ability to influence its business partners’ behaviours. Companies often fear unbalanced dependencies and the risk of being forced into information sharing arrangements. Power asymmetry, however, may aid the implementation of multi-tier information sharing. A dominant player may be able to bring multiple partners together and, if need be, enforce change with regards to, for example, adopted formats and platforms.

Culture. Represents the business relationships and the attitude and willingness toward collaborating and sharing information with supply chain partners. Lack of trust, which signifies a lack of cooperative and non-opportunistic behaviours, appears to be magnified when involving partners across three or more tiers.

Business Process. The task of linking business processes among three or more partners is considered difficult as: (1) there must be an overarching purpose and process so that all partners work toward the same goal, and (2) there must be standardised business processes in place.

Legal. In a multi-tier setting, suppliers and customers are generally embedded in multiple supply chains meaning that information can travel both vertically and horizontally across the network of business relationships. There is a need to formalise information sharing through a legal framework, including: (1) what information can be shared, (2) how to interpret the information, (3) how to use the information for decision making in production or similar, (4) how to store and treat the information, and (5) with whom information can be shared within and outside the company.

2.1.3.2 Control Systems

Data Integrity. A NIST report published in September 2021, titled *Protecting Information and System Integrity in Industrial Control System Environments: Cybersecurity for the Manufacturing Sector* highlights the importance of accounting for data integrity concerns. The integration of Informational Technology (IT) and Operational Technology (OT) networks are helping manufacturers boost productivity and gain efficiencies, it has also provided malicious actors - including nation states, common criminals, and insider threats - a fertile landscape in which they can exploit cybersecurity vulnerabilities to compromise the integrity of ICS and ICS data. Data integrity involves falsifying or exaggerating data. The motivations behind these attacks can range from degrading manufacturing capabilities and financial gain, to causing reputational harm. Whilst compromised data in the supply chain may affect the availability of products, compromised data at the control system level may lead to loss of reliability or integrity of the products themselves [28]–[30].

Confidentiality. There is difficulty in assessing and quantifying the perceived value of data. For example, code from a machine may seem unintelligible and therefore not very significant or valuable. However, in the hands of someone with domain knowledge, it may be incredibly valuable, providing, for example, highly significant and protected design details. As the volumes of data produced in manufacturing continue to increase, it is important to determine the value of the different data streams in order to understand the various levels of protection required.

2.1.4 Certification

Manufacturing processes are certified under certain operating conditions. If these processes are knowingly, or unknowingly, altered then that certification would no longer be valid. If through some malicious cyber-attack, the configuration of the process is changed such that it falls outside of the certification, the manufacturing operation would be in violation of the law. In order to cause such disruption and damage, the malicious actor would just have to understand the detail of the certification. Even if the final product is functional and safe, the operating company will still have broken the law by not complying with their certification.

2.1.5 Industry 4.0

ENISA published a report, titled *Industry 4.0 Cybersecurity: Challenges & Recommendations*, in May 2019 [6]. In this document, ENISA identified the main challenges to the adoption of the security measures and security of Industry 4.0 and Industrial IoT. The challenges were categorised as being related to people, processes or technology:

People

- **Need to Foster and Align IT/OT Security Expertise and Awareness**. People involved in deployments of new solutions usually have only knowledge of either IT or OT security, while Industry 4.0 and Smart Manufacturing require expertise over several areas.
- **Incomplete Organisational Policies and Reluctance to Fund Security**. Industry 4.0 operators, which are at various stages of Industry 4.0 adoption, often do not have appropriate governance structures in place for secure implementation of new technologies and secure maintenance of the existing ones.

Processes

- **Liability Over Industry 4.0 Products' Lifecycle is Poorly Defined**. There are a large number of stakeholders involved in the supply chain and in the use lifecycle of Industry 4.0, therefore apportioning liability in the aftermath of a security incident becomes challenging.
- **Fragmentation of Industry 4.0 Security Technical Standards**. Given the nascent nature of Industry 4.0, comprehensive initiatives to address security in a holistic manner are lagging behind.
- **Supply Chain Management Complexity**. Supply chains have become more dynamic, flexible, interdependent and demanding in terms of performance. However, increased interdependence of supply chains results in broader impact caused by existing security risks and the introduction of new ones.

Technology

- **Interoperability of Industry 4.0 Devices, Platforms and Frameworks**. Ensuring interoperability between devices/ platforms is not only about seamless operation, but also about security.
- **Technical Constraints Hampering Security in Industry 4.0 and Smart Manufacturing**. A particular issue is integration with legacy infrastructures. Patching and software updates over-the-air are in most cases not feasible solutions when it comes to low-end devices, as they do not support such functionality. Dedicated cybersecurity tools for Industry 4.0 systems are generally too few or too expensive.

3. Policy and Legislation

3.1 UK

3.1.1 Supply Chains

DCMS Call for Views. In May 2021, the UK Government put out a call for views on cyber security in supply chains and Managed Service Providers (MSP) [31]. The Call for Views focuses on understanding two aspects of supply chain cybersecurity: Part 1 seeks input on how organisations across the market manage supply chain cyber risk and what additional government intervention would enable organisations to do this more effectively; and Part 2 seeks input on the suitability of a proposed framework for MSP security and how this framework could most appropriately be implemented to ensure adequate baseline security to manage the risks associated with MSPs. The information collected and analysed through this Call for Views will contribute to the development of policy solutions.

Cyber Assessment Framework. The National Cyber Security Centre (NCSC) developed the Cyber Assessment Framework (CAF) in 2019, a collection of a set of 14 cyber security & resilience principles, together with guidance on using and applying the principles. It is designed for organisations that play a vital role in the day-to-day life of the UK, and is supported by technical guidance and references, constantly evolving to address emerging issues and threats [31]. One of the 14 principles focuses on supply chains - A.4 Supply Chain – and stipulates: *the organisation understands and manages security risks to networks and information systems supporting the operation of essential functions that arise as a result of dependencies on external suppliers. This includes ensuring that appropriate measures are employed where third party services are used* [32]. The principle states a number of specific supply chain related security considerations that should be addressed, where relevant to the provision of the essential function, including ensuring the protection of data shared with a third party and effective specification of the security properties of products or services procured from a third party that are important for the protection of the essential function.

NCSC Supply Chain Security Guidance. The NCSC has also developed a series of 12 principles, designed to help businesses establish effective control and oversight of their supply chains. The 12 principles are divided into four stages: understand the risks; establish control; check your arrangements; and continuous improvement.

PAS 555:2013. The Standard - *Cyber Security Risk. Governance and Management. Specification* - provides a business-led, holistic approach to cyber security. It applies to the whole organisation and its supply chain. it considers not only the technical aspects of cybersecurity, but also the physical, cultural and behavioural aspects, alongside effective leadership and governance [33].

Minimum Cyber Security Standard (MCSS). Launched by the UK government in June 2018, the MCSS sets out a series of mandatory cyber resilience outcomes that all government departments must achieve. The Standard can also be used by any other organisation to benchmark its cyber resilience efforts. The standards are presented as an absolute minimum and, ideally, should be exceeded [34]. MCSS states that: *Departments shall understand and manage security issues that arise because of dependencies on external suppliers or through their supply chain. This includes ensuring that the standards defined in this document are met by the suppliers of 3rd party services"* [35].

3.1.2 Control Systems

BS 6739:2009. *Code of Practice for Instrumentation in Process Control Systems: Installation Design and Practice* provides recommendations for, and guidance on, the design for the installation of instrumentation of measurement and control systems in the process industry, and the implementation and commissioning of this installation [36].

BS EN 61508-1:2010. *Functional Safety of Electrical/Electronic/ Programmable Electronic Safety-Related Systems - General Requirements* covers the safety systems of electrical equipment and their components that could have an impact on the safety of people and the environment if they fail. It also applies to protection and control systems [37].

BS EN 61511:2017. *Functional Safety. Safety Instrumented Systems for the Process Industry Sector.* The second edition of the Standard (the first was released in 2003) acknowledges that as functional safety related control systems become more complex - with programmable logic and the use of networks to monitor and control such systems - there is a growing need to identify and manage threats to the ongoing safe operation of the safety system from cyber-attacks. Thus, the Standard includes cybersecurity, with an emphasis on the threat to ongoing operations that a cyber-attack can pose and the importance of early identification [39] [40].

3.2 International

3.2.1 Supply Chains

Executive Order 14017. In February 2021, President Biden signed Executive Order 14017, titled *America's Supply Chains*. The EO directed a whole-of-government approach to assessing vulnerabilities in, and strengthening the resilience of, critical supply chains. It called for a comprehensive review to figure out exactly where the risks are, including explicit mention of cyber-attacks [40]–[42]. On May 12, Executive Order 14028 on *Improving the Nation's Cyber Security* was issued. The EO charged multiple agencies with enhancing cybersecurity through a variety of initiatives related to the security and integrity of the software supply chain [43]. On 30 September, NIST published the draft version of *SP 800-218 (Draft) Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities*. The SSDF is a set of fundamental, sound practices for secure software development based on established standards and guidelines produced by various organisations [44]. In accordance with EO 14028, (1) by February 6, 2022, after consulting heads of various agencies, NIST will issue guidance that identifies practices that enhance software supply chain security, with references to standards, procedures, and criteria, and (2) by May 8, 2022, NIST will publish additional guidelines, including procedures for periodically reviewing and updating guidelines [43].

NIS 2.0. In December 2020, the European Commission unveiled its new Cybersecurity Strategy to bolster Europe's collective resilience against cyber threats. Included in the strategy was the proposal to revise The Network and Information Security (NIS) Directive, producing NIS2. Amongst the proposed changes, the key sections of NIS2 impacting supply chains are under Chapter IV ‘Cybersecurity Risk Management and Reporting Obligations’ and Articles 18 and 19 in particular [46] [47]. Article 18, *Cybersecurity Risk Management Measures, asserts that “member States shall ensure that essential and important entities shall take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which those entities use in the provision of their services. Having regard to the state of the art, those measures shall ensure a level of security of network and information systems appropriate to the risk presented.” The measures referred to are specified to include, amongst others: “supply chain security including security-related aspects concerning the relationships between each entity and its suppliers or service providers such as providers of data storage and processing services or managed security services”* [47]. Article 19, EU Coordinated Risk Assessments of Critical Supply Chains, states that *“the Cooperation Group, in cooperation with the Commission and ENISA, may carry out coordinated security risk assessments of specific critical ICT services, systems or products supply chains, taking into account technical and, where relevant, nontechnical risk factors”* [47].

Data Act. The Communication on a European strategy for data adopted by the European Commission in February 2020 stressed that further EU actions could be taken forward in a Data Act. Among other things, the new Act is intended to support data sharing between businesses, targeting in particular issues relating to rights of use in jointly generated information, including IoT data generated in an industrial environment [23] [49]. In May 2021, the Commission published its Inception Impact Assessments on the forthcoming Data Act. This legislative initiative will aim at facilitating data access and use and review the rules on the legal protection of databases. The initiative is about ensuring fairness in the allocation of data value among actors of the data economy, including in business-to-business and business-to-government situations. Further development and fine tuning of the initiative is tabled for Q3-Q4 2021 [48].

ISO 28000:2007. *Specification for Security Management Systems for the Supply Chain* specifies the requirements for a security management system, including those aspects critical to security assurance of the supply chain. It is applicable to all sizes of organisations, from small to multinational, in manufacturing, service, storage or transportation at any stage of the production or supply chain [49].

ISO/IEC 27036. A multi-part standard offering guidance on the evaluation and treatment of information risks involved in the acquisition of goods and services from suppliers [50]. *ISO/IEC 27036-1:2021 Cybersecurity - Supplier Relationships - Part 1: Overview and Concepts* provides an overview of the guidance intended to assist organisations in securing their information and information systems within the context of supplier relationships [51]. *ISO/IEC 27036-2:2014 Information technology - Security Techniques - Information Security for Supplier Relationships - Part 2: Requirements* specifies fundamental information security requirements for defining, implementing, operating, monitoring, reviewing, maintaining and improving supplier and acquirer relationships [52]. *ISO/IEC 27036-3:2013 Information Technology - Security Techniques - Information Security for Supplier Relationships - Part 3: Guidelines for Information and Communication Technology Supply Chain Security* provides product and service acquirers and suppliers in the information and communication technology (ICT) supply chain with guidance on: (1) gaining visibility into and managing the information security risks caused by physically dispersed and multi-layered ICT supply chains; (2) responding to risks stemming from the global ICT supply chain to ICT products/ services that can have an information security impact on the organisations using these products and services.; and (3) integrating information security processes and practices into the system and software lifecycle processes (ISO, 2013). *ISO/IEC 27036-4:2016 Information Technology - Security Techniques - Information Security for Supplier Relationships - Part 4: Guidelines for Security of Cloud Services* provides cloud service customers and cloud service providers with guidance on (1) gaining visibility into the information security risks associated with the use of cloud services and managing those risks effectively, and (2) responding to risks specific to the acquisition or provision of cloud services that can have an information security impact on organisations using these services [53].

3.2.2 Control Systems

BS EN / IEC 62443. The *Security for Industrial Automation and Control Systems* series of Standards was developed to secure IACS throughout their lifecycle. It currently includes nine standards, technical reports and technical specifications [54]. The Standard addresses not only the technology that comprises a control system, but also the work processes, countermeasures, and employees. IEC 62443 takes a risk-based approach to cybersecurity, in which users must identify what is most valuable and requires the greatest protection and identify vulnerabilities. They must then erect defence-in-depth architecture that ensures business continuity [54].

ISA TR84.00.09-2013. *Security Countermeasures Related to Safety Instrumented Systems (SIS)* provides guidance on the countermeasures used to reduce the likelihood of a security breach of the SIS that degrades its ability to perform its function(s). This relates to cybersecurity from both inside and outside the plant boundary. The scope does not address physical plant protection (for example, fences, cameras, and grounding), but does address physical issues related to cybersecurity of the SIS [55].

ISO/IEC 27000. There are more than a dozen standards in the ISO/IEC 27000 family, providing a globally recognised framework for best practice in information security management. *ISO 27001* is a specification that sets out specific requirements, all of which must be followed, and against which an organisation's Information Security Management System (ISMS) can be audited and certified. *ISO/IEC TR 27019* provides guiding principles based on ISO/IEC 27002 for information security management applied to process control systems as used in the energy utility industry. The scope of ISO/IEC TR 27019:2013 covers process control systems used by the energy utility industry for controlling and monitoring the generation, transmission, storage and distribution of electric power, gas and heat in combination with the control of supporting processes. Outside the scope of ISO/IEC TR 27019:2013 is the conventional or classic control equipment that is non-digital [57] [58].

ANSI/ISA-18.2-2016. *Management of Alarms Systems for the Process Industries* specifies general principles and processes for the lifecycle management of alarm systems based on programmable electronic controller and computer-based human-machine interface (HMI) technology for facilities in the process industries. It covers all alarms presented to the operator through the control system [58].

SP 800-82 Rev. 2. *Guide to Industrial Control Systems (ICS) Security* was produced by NIST in 2015. It provides guidance on how to secure ICS, including Supervisory Control and Data Acquisition (SCADA) systems and Distributed Control Systems (DCS), while addressing their unique performance, reliability, and safety requirements. The document provides an overview of ICS and typical system topologies, identifies typical threats and vulnerabilities to these systems (including cybersecurity), and provides recommended security countermeasures to mitigate the associated risks [59].

ICS-CERT Recommended Practices. The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), part of CISA in the US Department of Homeland Security, have published a series of guidance documents for best practice. The publications include: updating antivirus in an industrial control system; improving industrial control systems cybersecurity with defence-in-depth strategies; and remote access for industrial control systems [60].

VCSS-CSO. The Voluntary Cyber Security Standards for Industrial Control Systems Operators (VCSS-CSO) were developed by the New Zealand National Cyber Security Centre (NCSC) in partnership with the New Zealand Control Systems Security Information Exchange (CSSIE) in 2019. VCSS-CSO is intended to support New Zealand's control systems operators in building resilient cyber security defences and practices [62] [63].

4. Opportunities

4.1.1 Supply Chains

A review paper published in August 2021 outline five key challenges faced by supply chains built on large and complex IoT systems [63]:

- **Need for end-to-end solutions for vulnerabilities and risks management**. There is a lack of effective methods to characterise, detect, classify, forecast, and estimate threats, risks, vulnerabilities, and suspicious activities. The challenge extends beyond detecting the vulnerability itself, to include building innovative solutions to manage the whole vulnerabilities lifecycle and the propagation of vulnerabilities within the entire end-to-end supply chain. Cybersecurity and privacy risks must also be accurately estimated within the entire supply chain to meet performance expectations through an appropriate data sharing mechanism, as well as to enable dynamic updates through real-time awareness of ICT systems' actual states.
- **Lack of evidence-based metrics for security assurance and trust guarantees**. Security and trust assurance should not only be inferred from an observed absence of security incidents; this may be an indication of the inability of the system to detect attacks or simply an absence of attacks during the monitored period. Similarly, security assurance must not only leverage on trust, but on evidence supporting specific security claims. However, there is a lack of effective metrics to characterise ICT systems performance with regards to cybersecurity and privacy. It is necessary to define both the security claims and the set of metrics used to characterise these claims, and choose the proper evidence for each specific claim.
- **Cumbersome coordination in multi-actor and multi-vendor supply chains of ICT systems**. Given such a heterogeneous and complex cybersecurity ecosystem, the process of coordinating and orchestrating the management of security appliances to provide trusted supply chains becomes a challenging endeavour. One of the challenges is that security policies are often specified by people who are different from the software developers actually implementing them, which leads to misconfigurations and improper responses to threats and attacks. Gartner estimates that 70% - 99% of data breaches result not from external, concerted attacks, but from misconfigurations of the affected IT systems. In supply chains, there is not a single allocated individual controlling the whole system; therefore, there is a lack of strict identity management and accountability mechanisms.
- **Static cybersecurity networked configurations and dynamic systems audit**. Even when a security policy is

successfully developed and implemented, the security systems in use are relatively static with respect to the highly dynamic threat prevention and mitigation techniques needed. In most cases, neither the network elements nor the security appliances support a reconfiguration framework to meet the dynamically changing nature of cyber threats.

- **Unlikely wide adoption of integrated cybersecurity solutions for composed ICT systems**. New approaches are needed to facilitate a coordinated, rather than integrated, deployment of cybersecurity solutions, accounting for the complexity of supply chains bringing together systems from different stakeholders, handled by human resources with different skill levels in ICT management.

Challenges may be categorised into those that are logistical, those that are technical, and those related to decision-making and policy [64].

Logistical Challenges

- **Lack of control over upstream supply chain**
- **Disclosure of supply chain information**: suppliers' willingness to disclose their cyber security practices, partly due to privacy reasons and competitor-sensitive information
- **Awareness of vulnerabilities**: the suppliers of IoT equipment may not be fully aware of all the possible vulnerabilities in their products
- **Centralised database of vulnerabilities**: there is no centralised database of known vulnerabilities and attacks that can serve as a guideline to identify risks and possible attacks
- **Heterogeneous supply chain management practices**

Technical Challenges

- **Lack of management controls**: centralised network management may not be available for the IoT
- **Inflexible hardware**: IoT device hardware may not be serviceable, meaning it cannot be repaired, customised, or inspected internally
- **Heterogeneous ownership**: devices are owned and operated by separate entities resulting in less control over policy implementation

Decision Making and Policy Challenges

- **Risk informed procurement and deployment**
- **Contingency planning**: IoT network requires arrangement of contingencies as suppliers may end security updates or discontinue support for the equipment
- **Risk-conscious supplier contracts**

4.1.2 Control Systems

Four broad areas have been identified as the most significant challenges requiring further research with regards to control systems:

Value of Data. In manufacturing, understanding/deciphering the real value of data is a complex task. Some data will have clear financial value, whereas other data will not have obvious apparent value but when combined with domain knowledge or other data sources, may have significant value. Need to be able to distinguish between valuable data and otherwise in order to determine what needs to be protected. Development of a matrix or method of determining value of manufacturing data is important.

Safer Connectivity. What are the right ways of addressing connectivity on the shop floor, and how do you ensure connectivity is not coming at a cost? Need to understand how to increase connectivity whilst ensuring that both control systems and data are sufficiently protected.

Certification and Standards. On the one hand, you have cybersecurity concerns, and on the other, certification requirements which are primarily concerned with processes. Need to map the two and ensure that any measures that are in place meet both sets of requirements. Need to understand whether compliance with cybersecurity standards satisfies requirement of certification, or whether within regulated industries more needs to be done to ensure that the process is certified.

Architecture Configuration. We are producing exponentially increasing amounts of data. In-process monitoring involves analysing this data, as it is produced in real-time, to control the process. This makes up-stream and down-stream inspections redundant, streamlining the manufacturing process and identifying issues as (or even before) they occur. Such processing requires (at least some of) the analytics to be undertaken at the edge, rather than at a central server. Having such edge devices has many advantages from a manufacturing perspective, however, the cybersecurity risks need to be understood and mitigated for. The constant flows of data in and out of the machines and the control systems need to be protected. Thus, with regards to edge devices, need to better understand optimal architecture, in terms of what needs to be processed locally versus at the central server.

PETRAS in the UK Research Landscape

There are numerous research centres focused on IoT and cybersecurity related issues in the Supply Chain and Control Systems sector. A few notable ones include:

1. The **High Value Manufacturing Catapult** which is the UK's innovation accelerator for advanced manufacturing technologies. The Catapult looks to (1) grow businesses and the contribution of the manufacturing sector to the UK economy; (2) investigate innovative technologies or scale up new products and processes to prove they have achieved manufacturing readiness; (3) work with academic partners to build on research at Universities and Research establishments in the UK and beyond; (4) use its expertise to help shape UK manufacturing policy; and (5) work with UK Government and others to develop high quality training provision to meet industry needs;
2. The new **Made Smarter Innovation Digital Supply Chain Innovation Hub** was announced in July 2021. It will be delivered by Digital Catapult, collaborating with large and small businesses, as well as universities, research technology organisations, and catapults. Breakthrough technology development will be delivered through large scale test beds. The hub will create an effective and integrated innovation ecosystem to develop new solutions to transform UK manufacturing;
3. Funding and plans for **five university-led research centres**, who will receive a share of £25 million from UK Research and Innovation (UKRI) and Made Smarter, was announced in July 2021. The research centres will help the UK's manufacturing industry become more productive and competitive through innovation and adoption of digital technologies. As well as being at the forefront and driving developments in their areas of expertise, these research centres will connect across the challenge to help bridge the gap between basic research and its application in manufacturing. This will provide a pipeline of digital technologies for the future.

PETRAS has a strong, and expanding, research focus in Supply Chains and Control Systems. There are 19 projects within the sector, either completed or ongoing, some of which are detailed in Table 2. Further details on all of the projects can be found at:
https://petras-iot.org/projects/?_sft_sector=supply-chains-and-control-systems

PETRAS has a dedicated Business Development team who connect the public and private sectors with a network of transdisciplinary academic experts, to enable research collaborations that address social and technical issues relating to the cybersecurity of IoT devices, systems and networks.

If you are a research institution, private or public sector organisation interested in collaborating with PETRAS, please contact petras@ucl.ac.uk.

Table 2: A selection of completed PETRAS projects in cybersecurity in the Supply Chain and Control Systems sector

Project	Description	Partners	Status
Identifying Attack Vectors for Network Intrusion to Determine Impact Across Threat Surfaces (IoT-Depends)	Looked to enhance the Supervisory Control And Data Acquisition (SCADA) testbed at Airbus using IoT devices to enhance Airbus' knowledge and expertise in IoT risks to SCADA, and to test the utility of Dependency Modelling to incorporate goal success probability data derived from 'canned attacks' on IoT devices into a risk model of a SCADA system to simulate failure.	Airbus	Completed
EBIS+: Extending BIM Level 2 to support IoT & Security Demonstrator	Explored the use of a secured distributed Digital Object Management System (DOMS) to represent deployments including security, data description and access process information with the relevant security metadata and extensive use of templates.	BRE	Completed
Power Grid IoT System Protection and Resilience using Intelligent Edge (Power-SPRINT)	Investigates the cybersecurity risks posed by the growing integration of IoT-enabled smart-home appliances on power grid operations. By analysing network traffic from IoT-smart-home appliances, Power-SPRINT will perform threat analysis and identify the devices that are most likely to be targeted by the attacker. Using a control theoretic-approach, Power-SPRINT will investigate the impact of compromising a large number of smart-home appliances (in a Botnet-type attack) on power grid operations and shed light on how the grid's resilience can be enhanced by the optimal deployment of security reinforcements and back-up devices to mitigate these attacks. Power-SPRINT will investigate how to detect such attacks if they occur using the power grid's physical signals and deep learning along with implementing a privacy-preserving mechanism that can be deployed at the edge devices.	Schneider Electric; Global Cyber Alliance	Ongoing

Cognitive and Socio-Technical Cybersecurity in Modern Railway System (CoSTC-MoRS)	Developing a hybrid and adaptive approach to combining AI and a socio-technical model to identify and detect cyberattacks and create a holistic & fast response to cyber incidents to ensure the security, safety, and functionality of a Modern Railway System (MRS). The project focuses on the Signalling and Control System (SCS), on which an attack tree analysis will be given. The project also aims to provide a socio-technical security roadmap and IoT plan for business continuity to mitigate the potential impact of cyber incidents on MRSs, considering the operations, human-factors, organisational structures, regulation and policies.	National Skills Academy for Rail (NSAR);
		Birmingham Centre for Railway Research and Education (BCRRE);
		East West Rail Co (EWR);
		COSTAIN; Vega Systems UK;
		CERBERUS Security Laboratories (CSL)
			Ongoing

Table 2 cont. A selection of completed PETRAS projects in cybersecurity in the Supply Chain and Control Systems sector

Project	Description	Partners	Status
Early Anomaly Detection for Securing IoT in Industrial Automation (ELLIOTT)	Investigates deep learning along with conventional machine learning models to develop a fast, reliable and robust detection model that can be applied to various industrial processes. The project has previously developed an AI-approach which uses evolutionary algorithms as a mechanism to generate attack examples to identify weaknesses in the detection. To test the performance of the detection models, ELLIOTT will test the developed AI-approach in conjunction with manual random attacks and off the shelf tools. To show the work in a wider context, ELLIOT will work with user partners to test the developed approaches in two real cyber physical systems within industrial control systems: i) electronic servo motors in factories and ii) building management systems.	Cube Controls; Rockwell Automation	Ongoing
Integrity Checking at the Edge (ICE)	Assesses the potential threats involved in interactions between edge devices, cloud platforms and legacy systems used in the manufacturing and water treatment sectors. It provides security and resilience for emerging technologies in critical infrastructures. considers human-machine interaction in conversation around pathways and interactions, taking inspiration from Explainable AI.	Cardiff University; University of Bristol	Ongoing

Logistics 4.0: Securing High Value Goods using Self-Protecting Edge Computer	Aims to create, design and develop tiny sensor-tracking systems that attach directly to objects. The project aims to advance IoT technologies to better protect high-value goods by providing environment, transit behaviours, and wide-area real-time location data. These devices protect the object and can also protect themselves. Research is conducted through 3 themes: “Design for Trust”, “Technical Co-Design” and “Law, Ethics and Risk” covering security from different angles. Though the focus is on high value goods, specifically art, the AI/systems/algorithms/protocols that operate at the Edge not only apply to other goods, but their advances will provide a step-change to the security/reliability of IoT and Cyber-Physical Systems generally.	Tate;
		Ordnance Survey;
		Constantine Ltd;
		Momart Ltd;
		Arm Holdings
			Ongoing

Glossary

AI (Artificial Intelligence) is *“the theory and development of computer systems able to perform tasks normally requiring human intelligence, such as visual perception, speech recognition, decision-making, and translation between languages”* [65]

A Managed Service Provider (MSP) *“delivers services, such as network, application, infrastructure and security, via ongoing and regular support and active administration on customers’ premises, in their MSP’s data centre (hosting), or in a third-party data centre”* [66]

References

1. K. Timmermans, “Can you see what the future holds for the supply chain?,” WordPressBlog, Sep. 2021. https://www.accenture.com/us-en/blogs/business-functions-blog/business-futures-supply-chain (accessed Nov. 17, 2021).

2. M. Govil and J.-M. Proth, “2 - DEFINITION OF A SUPPLY CHAIN,” in Supply Chain Design and Management, M. Govil and J.-M. Proth, Eds. San Diego: Academic Press, 2002, pp. 7–16. doi: 10.1016/B978-012294151-1/50002-3.

3. CIPS, “What is a Supply Chain?,” CIPS, n.d. https://www.cips.org/knowledge/procurement-topics-and-skills/supply-chain-management/what-is-a-supply-chain/ (accessed Aug. 13, 2021).

4. W. Bolton, “1 - Control systems,” in Control Systems, W. Bolton, Ed. Oxford: Newnes, 2002, pp. 1–36. doi: 10.1016/B978-075065461-6/50001-5.

5. A. Shahzad, Y.-G. Kim, and A. Elgamoudi, “Secure IoT Platform for Industrial Control Systems,” in 2017 International Conference on Platform Technology and Service (PlatCon), Feb. 2017, pp. 1–6. doi: 10.1109/PlatCon.2017.7883726.

6. ENISA, Industry 4.0 Cybersecurity Challenges & Recommendations. Greece: ENISA, 2019. Accessed: Sep. 06, 2021. [Online]. Available: https://www.enisa.europa.eu/publications/industry-4-0-cybersecurity-challenges-and-recommendations

7. A. G. Frank, L. S. Dalenogare, and N. F. Ayala, “Industry 4.0 technologies: Implementation patterns in manufacturing companies,” International Journal of Production Economics, vol. 210, pp. 15–26, 2019, doi: https://doi.org/10.1016/j.ijpe.2019.01.004.

8. R. Lineberger, A. Hussain, T. Hanley, V. Rutgers, and B. Sniderman, Aerospace & Defense 4.0: Capturing the value of Industry 4.0 technologies. Deloitte Insights, 2019. Accessed: Aug. 18, 2021. [Online]. Available: https://www2.deloitte.com/us/en/insights/focus/industry-4-0/aerospace-defense-companies-digital-transformation.html

9. ENISA, “Threat Landscape for Supply Chain Attacks — ENISA,” Jul. 2021. https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks (accessed Oct. 29, 2021).

10. Kaspersky, “Threat landscape for industrial automation systems. Statistics for H1 2021,” Kaspersky ICS CERT | Kaspersky Industrial Control Systems Cyber Emergency Response Team, Sep. 09, 2021. https://ics-cert.kaspersky.com/media/Kaspersky-ICS-CERT-Threat-landscape-for-industrial-automation-systems-statistics-for-H1-2021-En.pdf (accessed Oct. 29, 2021).

11. CNBC, “Colonial Pipeline restarts after hack, but supply chain won’t return to normal for a few days,” May 12, 2021. https://www.cnbc.com/2021/05/12/colonial-pipeline-restarts-after-hack-but-supply-chain-wont-return-to-normal-for-a-few-days.html (accessed Oct. 29, 2021).

12. The New York Times, “Colonial Pipeline Hack Reveals Weaknesses in US Cybersecurity - The New York Times,” May 14, 2021. https://www.nytimes.com/2021/05/14/us/politics/pipeline-hack.html (accessed Oct. 29, 2021).

13. DCMS, “Cyber Security Breaches Survey 2021 - GOV.UK,” GOV.UK, Mar. 2021. https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2021/cyber-security-breaches-survey-2021 (accessed Nov. 10, 2021).

14. NPR, “A ‘Worst Nightmare’ Cyberattack: The Untold Story Of The SolarWinds Hack,” Apr. 2021. https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack (accessed Oct. 29, 2021).

15. CISA, DOE, and NCSC, “Recommended Cybersecurity Practices for Industrial Control Systems,” p. 2, 2020.

16. Department of Homeland Security, Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies. 2016. Accessed: Oct. 29, 2021. [Online]. Available: https://us-cert.cisa.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf

17. D. Bhamare, M. Zolanvari, A. Erbad, R. Jain, K. Khan, and N. Meskin, “Cybersecurity for industrial control systems: A survey,” Computers & Security, vol. 89, p. 101677, Feb. 2020, doi: 10.1016/j.cose.2019.101677.

18. M. Boholm, N. Möller, and S. O. Hansson, “The Concepts of Risk, Safety, and Security: Applications in Everyday Language,” Aug. 2015. https://onlinelibrary.wiley.com/doi/epdf/10.1111/risa.12464 (accessed Oct. 29, 2021).

19. B. Krebs, “Cyber Incident Blamed for Nuclear Power Plant Shutdown,” Jun. 2008. https://www.washingtonpost.com/wp-dyn/content/article/2008/06/05/AR2008060501958.html (accessed Oct. 29, 2021).

20. A. Cardenas, Cyber-Physical Systems Security Knowledge Area Issue 1.0. 2019. Accessed: Oct. 29, 2021. [Online]. Available: https://www.cybok.org/media/downloads/Cyber-Physical_Systems_Security_issue_1.0.pdf

21. J. C. Knight, “Safety critical systems: challenges and directions,” in Proceedings of the 24th International Conference on Software Engineering. ICSE 2002, May 2002, pp. 547–550.

22. “Hacker attempted to poison water supply of Florida city, officials say,” The Guardian, Feb. 08, 2021. Accessed: Oct. 29, 2021. [Online]. Available: https://www.theguardian.com/us-news/2021/feb/08/hacker-water-supply-oldsmar-florida

23. M. Godfrey-Faussett, “The role of data in smart supply chains,” Pinsent Masons, Oct. 2020. https://www.pinsentmasons.com/out-law/analysis/role-of-data-smart-supply-chains (accessed Nov. 12, 2021).

24. S. R. Chhetri, S. Faezi, N. Rashid, and M. A. Al Faruque, “Manufacturing Supply Chain and Product Lifecycle Security in the Era of Industry 4.0,” J Hardw Syst Secur, vol. 2, no. 1, pp. 51–68, Mar. 2018, doi: 10.1007/s41635-017-0031-0.

25. CNSS, Committee on National Security Systems (CNSS) Glossary. 2015. Accessed: Nov. 12, 2021. [Online]. Available: https://rmf.org/wp-content/uploads/2017/10/CNSSI-4009.pdf

26. NIST, Securing Data Integrity Against Ransomware Attacks: Using the NIST Cybersecurity Framework and NIST Cybersecurity Practice Guides. 2020. Accessed: Nov. 12, 2021.

[Online]. Available: https://nvlpubs.nist.gov/nistpubs/cswp/NIST.CSWP.10012020-draft.pdf

27. J. Kembro, D. Näslund, and J. Olhager, “Information sharing across multiple supply chain tiers: A Delphi study on antecedents,” International Journal of Production Economics, vol. 193, pp. 77–86, Nov. 2017, doi: 10.1016/j.ijpe.2017.06.032.

28. S. Smith, “Building Management in The Cybersecurity Age,” ASHRAE Journal, vol. 60, no. 11, pp. 84–86, Nov. 2018.

29. N. Krayem, “Global cybersecurity risks in the manufacturing industry,” Willis Towers Watson, Aug. 2019. https://www.willistowerswatson.com/en-US/Insights/2019/07/decode-cyber-brief-global-cybersecurity-risks-in-the-manufacturing-industry (accessed Nov. 14, 2021).

30. NIST, Protecting Information and System Integrity in Industrial Control System Environments: Cybersecurity for the Manufacturing Sector. 2021. Accessed: Nov. 14, 2021. [Online]. Available: https://www.nccoe.nist.gov/sites/default/files/2021-09/mf-ics-nist-sp1800-10-draft.pdf

31. DCMS, “Call for views on cyber security in supply chains and managed service providers - GOV.UK,” GOV.UK, May 2021. https://www.gov.uk/government/publications/call-for-views-on-supply-chain-cyber-security/call-for-views-on-cyber-security-in-supply-chains-and-managed-service-providers (accessed Nov. 10, 2021).

32. NCSC, “A.4 Supply chain,” GOV.UK, Sep. 2019. https://www.ncsc.gov.uk/collection/caf/caf-principles-and-guidance/a-4-supply-chain (accessed Nov. 10, 2021).

33. BSI, “PAS 555:2013 Cyber security risk. Governance and management. Specification,” May 2013. https://shop.bsigroup.com/products/cyber-security-risk-governance-and-management-specification (accessed Nov. 10, 2021).

34. IT Governance, “UK Government Minimum Cyber Security Standard | IT Governance Ltd,” n.d. https://www.itgovernance.co.uk/uk-government-minimum-cyber-security-standard (accessed Nov. 10, 2021).

35. Cabinet Office, Minimum Cyber Security Standard. 2018. Accessed: Nov. 11, 2021. [Online]. Available: https://www.gov.uk/government/publications/the-minimum-cyber-security-standard/the-minimum-cyber-security-standard

36. BSI, “Code of practice for instrumentation in process control systems: installation design and practice,” Jan. 2009. https://shop.bsigroup.com/products/code-of-practice-for-instrumentation-in-process-control-systems-installation-design-and-practice (accessed Nov. 11, 2021).

37. BSI, “Functional safety of electrical/electronic/ programmable electronic safety-related systems - General requirements,” Jun. 2010. https://shop.bsigroup.com/products/functional-safety-of-electrical-electronic-programmable-electronic-safety-related-systems-general-requirements (accessed Nov. 11, 2021).

38. A. Derbyshire, The long awaited IEC 61511 edition 2 and what it means for the process industry. IChemE, 2016. Accessed: Nov. 11, 2021. [Online]. Available: https://www.icheme.org/media/11752/hazards-26-paper-15-iec-61511-functional-safety-in-the-process-industry-the-long-awaited-iec-61511-edition-2-and-what-it-means-for-the-process-industry.pdf

39. BSI, “Functional safety. Safety instrumented systems for the process industry sector - Framework, definitions, system, hardware and application programming requirements,” 2017. https://shop.bsigroup.com/products/functional-safety-safety-instrumented-systems-for-the-process-industry-sector-framework-definitions-system-hardware-and-application-programming-requirements (accessed Nov. 11, 2021).

40. Federal Register, “Executive Order 14017: America’s Supply Chains,” Feb. 24, 2021. https://www.federalregister.gov/documents/2021/03/01/2021-04280/americas-supply-chains (accessed Nov. 12, 2021).

41. F. Oliver, “Biden’s Supply Chain Intentions Depend on Cybersecurity,” May 2021. https://supplychaindigital.com/supply-chain-risk-management/bidens-supply-chain-intentions-depend-cybersecurity (accessed Nov. 12, 2021).

42. The White House, “FACT SHEET: Biden-Harris Administration Announces Supply Chain Disruptions Task Force to Address Short-Term Supply Chain Discontinuities | The White House,” Jun. 2021. https://www.whitehouse.gov/briefing-room/statements-releases/2021/06/08/fact-sheet-biden-harris-administration-announces-supply-chain-disruptions-task-force-to-address-short-term-supply-chain-discontinuities/ (accessed Nov. 12, 2021).

43. NIST, “Executive Order 14028, Improving the Nation’s Cybersecurity | NIST,” n.d. https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity (accessed Nov. 12, 2021).

44. NIST, “Executive Order 14028: Guidelines for Enhancing Software Supply Chain Security,” Nov. 2021. https://www.nist.gov/news-events/events/2021/11/executive-order-14028-guidelines-%03enhancing-software-supply-chain (accessed Nov. 12, 2021).

45. European Commission, “New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient,” European Commission - European Commission, Dec. 2020. https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2391 (accessed Nov. 12, 2021).

46. CyberSec4Europe, Cyber Security for Europe - D9.12 Supply Chain Security Recommendations 1. 2021. Accessed: Nov. 12, 2021. [Online]. Available: https://cybersec4europe.eu/wp-content/uploads/2021/05/D9.12-Supply-chain-security-recommendations-1-v1.0-submitted.pdf

47. European Commission, “Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148,” European Commission - European Commission, Dec. 2020. https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2391 (accessed Nov. 12, 2021).

48. European Parliament, “Legislative Train Schedule - A EUROPE FIT FOR THE DIGITAL AGE,” European Parliament, Oct. 2021. https://www.europarl.europa.eu/legislative-train (accessed Nov. 12, 2021).

49. ISO, “ISO 28000:2007,” ISO, 2007. https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/04/46/44641.html (accessed Nov. 12, 2021).

50. Joinup, “ISO/IEC 27036-1:2014 - Information technology -- Security techniques -- Information security for supplier relationships -- Part 1: Overview and concepts | Joinup,” n.d. https://joinup.ec.europa.eu/collection/ict-standards-procurement/solution/isoiec-27036-12014-information-technology-security-techniques-information-security-supplier/distribution/isoiec-27036-12014-information-technology-security-techniques-information-security-supplier (accessed

Nov. 12, 2021).

51. ISO, “ISO/IEC 27036-1:2021 Cybersecurity - Supplier relationships - Part 1: Overview and concepts,” ISO, 2021. https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/08/29/82905.html (accessed Nov. 12, 2021).

52. ISO, “ISO/IEC 27036-2:2014 Information technology - Security techniques - Information security for supplier relationships - Part 2: Requirements,” ISO, 2014. https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/05/96/59680.html (accessed Nov. 12, 2021).

53. ISO, “ISO/IEC 27036-4:2016 Information technology - Security techniques - Information security for supplier relationships - Part 4: Guidelines for security of cloud services,” ISO, 2016. https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/05/96/59689.html (accessed Nov. 12, 2021).

54. IEC, “Understanding IEC 62443 | IEC,” 2021. https://www.iec.ch/blog/understanding-iec-62443 (accessed Nov. 11, 2021).

55. ANSI, “ISA TR84.00.09-2013 - Security Countermeasures Related to Safety Instrumented Systems (SIS),” 2013. https://webstore.ansi.org/standards/isa/isatr8400092013 (accessed Nov. 11, 2021).

56. ISO, “ISO - ISO/IEC 27001 — Information security management,” ISO, n.d. https://www.iso.org/isoiec-27001-information-security.html (accessed Nov. 11, 2021).

57. Joinup, “About ISO/IEC TR 27019:2013 - Information technology -- Security techniques -- Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry,” n.d. https://joinup.ec.europa.eu/collection/ict-standards-procurement/solution/isoiec-tr-270192013-information-technology-security-techniques-information-security-management/about (accessed Nov. 11, 2021).

58. ISA, “ANSI/ISA-18.2-2016, Management of Alarm Systems for the Process Industries,” 2016. https://www.isa.org/products/ansi-isa-18-2-2016-management-of-alarm-systems-for (accessed Nov. 11, 2021).

59. K. Stouffer, S. Lightman, V. Pillitteri, M. Abrams, and A. Hahn, “Guide to Industrial Control Systems (ICS) Security,” National Institute of Standards and Technology, NIST Special Publication (SP) 800-82 Rev. 2, Jun. 2015. doi: 10.6028/NIST.SP.800-82r2.

60. CISA, “Recommended Practices | CISA,” n.d. https://us-cert.cisa.gov/ics/Recommended-Practices (accessed Nov. 12, 2021).

61. NCSC and CSSIE, “Voluntary Cyber Security Standards for Control Systems Operators,” 2019, Accessed: Nov. 12, 2021. [Online]. Available: https://www.ncsc.govt.nz/assets/NCSC-Documents/VCSS-CSO-Final-Oct-2019.pdf

62. NCSC, “NCSC - Voluntary Cyber Security Standards for Industrial Control Systems Operators (VCSS-CSO),” n.d. https://www.ncsc.govt.nz/resources/vcss-cso/ (accessed Nov. 12, 2021).

63. X. Masip-Bruin et al., “Cybersecurity in ICT Supply Chains: Key Challenges and a Relevant Architecture,” Sensors, vol. 21, no. 18, Art. no. 18, Jan. 2021, doi: 10.3390/s21186057.

64. M. J. Farooq and Q. Zhu, “IoT Supply Chain Security: Overview, Challenges, and the Road Ahead,” arXiv:1908.07828 [cs], Jul. 2019, Accessed: Nov. 04, 2021. [Online]. Available: http://arxiv.org/abs/1908.07828

65. Lexico, “Artificial Intelligence,” Lexico, n.d. https://www.lexico.com/definition/artificial_intelligence (accessed Feb. 14, 2021).

66. Gartner, “Definition of Managed Service Provider (MSP) - Gartner Information Technology Glossary,” Gartner, n.d. https://www.gartner.com/en/information-technology/glossary/msp-management-service-provider (accessed Nov. 18, 2021).

TWITTER
@PETRASiot

LINKEDIN
linkedin.com/
school/petrasiot

WEBSITE
petras-iot.org

EMAIL
petras@ucl.ac.uk