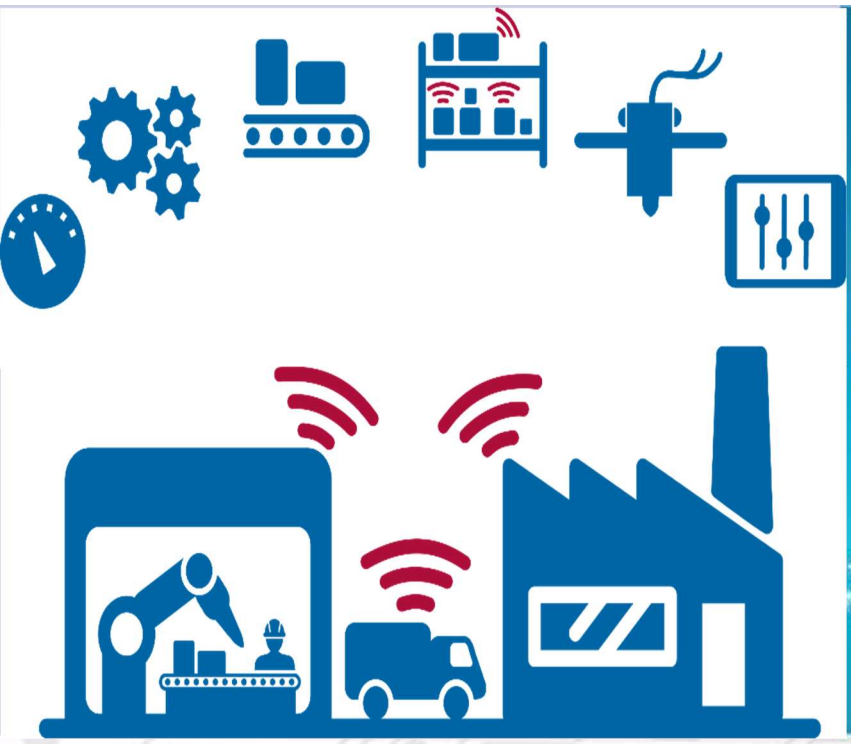

Good Practices for Security of Internet of Things

in the context of Smart Manufacturing

NOVEMBER 2018

www.enisa.europa.eu European Union Agency For Network and Information Security

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Contact

For queries in relation to this paper, please use iot-security@enisa.europa.eu
For media enquiries about this paper, please use press@enisa.europa.eu.

Acknowledgements

Over the course of this study, we have received valuable input and feedback from:

Ernie Hayden	443 Consulting
Adrien Becue	Airbus Cybersecurity
Jalal Bouhdada	Applied Risk
Hannes Tschofenig, Reed Hinkel	ARM Ltd.
Denis Justinek	BIOKODA D.O.O.
Alessandro Cosenza	Bticino S.p.A.
Cédric Lévy-Bencheton	Cetome
Jeff Schutt	CISCO
Mirko Ross	Digital Worx GmbH
Gianmarco Baldini	DG JRC
Georges-Henri Leclercq	Engie Laborelec
Brice Copy, Pascal Oser	European Organization for Nuclear Research (CERN)
Jens Mehrfeld	Federal agency for information security (BSI)
Rafal Leszczyna	Gdansk University of Technology
Carlos Valderrama	Geomantis Corporation Limited
Ian Smith	GSM Association (GSMA)
Konstantin Rogalas	Honeywell
Antonio J. Jara	HOP Ubiquitous S.L. (HOPU)
Vangelis Gazis	Huawei Technologies Co., Ltd.
Luca Bizzotto, Mike Edwards, Arndt Kohler, Ivan Reedman	IBM
Samuel Linares	

Victor Fidalgo Villar	INCIBE (The Spanish National Cybersecurity Institute)
Steve Olshansky, Andrei Robachevsky	Internet Society
Andrey Nikishin, Ekaterina Rudina, Vyacheslav Zolotnikov	Kaspersky Lab
Mahmoud Ghaddar	Legrand
Benedikt Abendroth, Kadri Umay	Microsoft Corporation
Vytautas Butrimas	NATO Energy Security Center of Excellence
Sergi Cuny Lafond	Nestle
Jacques Kruse-Brandao	NXP Semiconductors N.V.
Andrew Tierney, Mark Harrison	PenTestPartners
Stefano Zanero	Politecnico di Milano
Marcin Blasiak, Marcin Tarchalski	Pratt&Whitney
Pirmin Heinzer	MELANI
Jay Thoden van Velzen	SAP
Pierre Kobes, Wolfgang Klasen	SIEMENS AG
Sylvie Wuidart	STMicroelectronics N.V.
Yun Shen	Symantec Corporation
Steffen Zimmermann	Trade Association (VDMA)
Julio Hernández Castro	University of Kent
Antonio Raposo	Volkswagen AG
Filip Chytrý	
EC3/Europol	

ISBN: 978-92-9204-261-5, DOI:, DOI: 10.2824/851384

Table of Contents

Executive Summary

Industry 4.0 is rapidly becoming a reality, making use of intelligent, interconnected cyber-physical systems to automate all phases of industrial operations, spanning from design and manufacturing to operation, supply chain and service maintenance. With a great impact on citizens' safety, security and privacy due to its cyber-physical nature and the inherent autonomy, the threat landscape concerning Industry 4.0 and IoT is extremely wide.

Following a methodological approach, ENISA has developed this study on Good Practices for Security of the IoT in the context of Industry 4.0 and Smart Manufacturing. The study makes a series of contributions, most notably the following:

- Defines relevant terminology (i.e. terms such as Industry 4.0, Smart manufacturing, Industrial IoT) to promote common understanding of relevant cybersecurity scenarios.
- Categorizes in a comprehensive taxonomy the Industry 4.0 assets across the manufacturing process and value chain.
- Introduces a detailed Industry 4.0 threat taxonomy based on related risks and attack scenarios.
- Maps the identified threats to assets, thus facilitating the deployment of security measures based on the customized requirements of interested stakeholders.
- Lists security measures related to the use of IoT in Smart Manufacturing and Industry 4.0 and maps them against the aforementioned threats.

In conducting this study, ENISA identified and extensively analysed the current state of available documentation on security in IoT, Industrial IoT, Industry 4.0 and Smart Manufacturing. ENISA also collected input from a number of security experts through a structured questionnaire and a series of interviews.

ENISA considered the security of Industry 4.0 devices and services throughout their lifecycle (from conception to end-of-life and decommissioning) and paid close attention to issues that are particular to the requirements of Industry 4.0. Accordingly, the study highlights security measures in three dimensions:

- Policies
- Organisational measures
- Technical measures

One additional noteworthy element of this study is the mapping to existing security initiatives, standards and schemes. ENISA reviewed more than 150 resources on Industry 4.0 and IoT security and mapped them against the security measures proposed in this study. This mapping facilitates stakeholders, who are nowadays faced with a fragmented field, to have a common basis of understanding.

The guidelines and security measures listed in this study aim at improving the cybersecurity posture of Industry 4.0 organisations that have adopted or plan to adopt Industrial IoT devices and solutions that enhance automation in industrial operations. These security measures apply to a wide audience spanning Industrial IoT operators and manufacturers/vendors, which can utilise these measures and recommendations as a checklist against which to examine their Industry 4.0 security solutions.

The aim of the study is to serve as a reference point to promote collaboration on Industry 4.0 and Industrial IoT security across the European Union and raise awareness of the relevant threats and risks with a focus on "security for safety".

1. Introduction

In recent years, we have seen a significant and rapid decline in data transfer and storage costs due to the accelerating shift in the global economy driven by more connectivity, collaboration and sharing. This development, accompanied by a bimodal IT organisation, supports exponential growth in the smart connected world, especially in manufacturing. Recent trends include the emergence of Industry 4.0, a concept that is revolutionising traditional manufacturing and other industries by introducing new capabilities, such as digitisation, decision-making decentralisation and value chain integration. Industry 4.0 is tightly bound to cyber-physical systems that in turn are enabling intelligent and connected infrastructures – including Smart Manufacturing infrastructures – by enhancing their quality of service provisioning.

Transforming the industrial landscape, Industry 4.0 with the Internet of Things (IoT) at its core has already exerted an impact on society, transforming products, customer experience and the labour market. It is therefore playing a central role within the European Union's initiatives, becoming the subject of various studies, programs and regulations[1].

The fourth industrial revolution and exponential growth in the quantity of connected devices all over the world together with the rapidly increasing number of cyber security incidents further stress the need for strengthening cyber resilience, especially among the industrial operators who are beginning to utilise IoT solutions. Recent initiatives towards Industry 4.0 and Smart Manufacturing[2] are attracting more attention to aspects related to the security of technical solutions and the safety of citizens who rely on them. This subject is all the more important since the potential impact exerted by new threats ranges from compromising physical security to production downtime, spoilage of product, damage to equipment and the ensuing financial and reputational losses.

Industry 4.0 and Smart Manufacturing, in particular, accelerate the introduction of intelligence, automation and autonomy in manufacturing and supply chain environments. Accordingly and given the significant attention and prioritization that has been given to the digitisation of the EU industrial sector, this study has a focus on security of IoT in the context of Industry 4.0. The topic is of great importance as vendors' and users' / consumers' awareness of the threats related to the deployment of Smart Manufacturing and Industry 4.0 is usually limited. At the same time, cyberattacks focusing on industrial assets, such as Safety Instrumented Systems, using new attack vectors have been recently observed with an increasing frequency.

1.1 Objectives

This ENISA study aims at addressing the security and privacy challenges related to the evolution of industrial systems and services precipitated by the introduction of IoT innovations. The main objectives were to collect good practices to ensure security of IoT in the context of Industry 4.0/Smart Manufacturing, while mapping the relevant security and privacy challenges, threats, risks and attack scenarios.

The aim of the study is to serve as a reference point to promote collaboration on Industry 4.0 and Industrial IoT security across the European Union and raise awareness of the relevant threats and risks with a focus on "security for safety".

[1] See examples of EU initiatives related to Industry 4.0 concept: https://ec.europa.eu/growth/tools-databases/dem/monitor/tags/industry-40

[2] See examples of national initiatives for digitizing industry within the EU: https://ec.europa.eu/growth/tools-databases/dem/monitor/category/national-initiatives

An additional important element of the study is to define the notion of Industry 4.0 and Smart Manufacturing to set the perimeter of the work to be done and serve as the basis for future developments.

1.2 Scope

This study outlines good practices for cybersecurity in the IoT applied in an industrial environment. Due to the extensive landscape of IoT deployments, this study focuses on Industrial IoT (IIoT) and Smart Manufacturing because they are among the most representative elements of the overall Industry 4.0 landscape[3].

In this study ENISA identified and extensively analysed the current state of available documentation on security in IoT, IIoT, Industry 4.0 and Smart Manufacturing and other related subjects. ENISA also collected input from a number of security experts through a structured questionnaire and a series of interviews. Based on a thorough review of existing works, ENISA identified threats and developed possible critical attack scenarios targeting various domains of Industry 4.0 and Smart Manufacturing. This enabled the Agency to develop good practices and security measures to ensure security in IoT in Industry 4.0. In this respect, the study also made it possible to identify gaps in, and barriers to, security adoption.

The study highlights three groups of security measures to address security challenges in technologies, people and processes. A risk-based and holistic approach to security was undertaken. ENISA considered the security of IoT devices and services in industrial settings throughout their lifecycle (from conception to end-of-life) and paid particular attention to the overall supply chain and third party management, which constitute essential elements of Industry 4.0.

1.3 EU and International policy context

With a globally emerging trend of connected things and the increasingly common adoption of IoT concepts by organisations across the world, cybersecurity of IoT in recent years has become a matter of interest for the European Commission and other regulation bodies. IoT in Industry and Smart Manufacturing is a specific subset of IoT cybersecurity.

Being aware of the potential of IoT and the related cyber security challenges, the EU has been striving to ensure security in the IoT and accelerate development in this area through numerous policy actions that include the creation of alliances and centres of expertise, development of regulatory documents and launch of pilot projects. In March 2015, the European Commission launched the Alliance for Internet of Things Innovation (AIOTI)[4] with the objective to create an innovative European IoT ecosystem. It has become the largest IoT association in Europe illustrating the EU's intention to collaborate with stakeholders in order to establish a competitive European IoT market and develop new business models.

Two months later, in May 2015, the EU adopted the Digital Single Market (DSM) Strategy[5]. In terms of the IoT, which is one of its five main development areas, the DSM aims to address common issues that may lead to the deceleration of secure IoT adoption, such as fragmentation of guidelines and lack of interoperability. In April 2016, to fulfil DSM needs and ensure awareness of its upcoming policy, the European Commission published a staff working document related to the IoT[6]. It constitutes part of the "Digitising European

[3] See EC, Fourth Industrial Resolution: https://ec.europa.eu/digital-single-market/en/fourth-industrial-revolution
[4] See The Alliance for Internet of Things Innovation: https://ec.europa.eu/digital-single-market/en/alliance-internet-things-innovation-aioti
[5] See more about Digital Single Market: https://ec.europa.eu/commission/priorities/digital-single-market/
[6] See European Commission (2016) "Advancing the Internet of Things in Europe": https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016SC0110

Industry" initiative and outlines the EU's vision of IoT based on three pillars: a thriving IoT ecosystem, a human-centred IoT approach and a single market for IoT.

Like the Internet of Things, Cybersecurity is another DSM priority in terms of standards development. It is a broad concept that, among others, spans cybersecurity in the Internet of Things and cybersecurity in industrial systems. When it comes to IoT cybersecurity, ENISA developed a document entitled "Baseline Security Recommendations for IoT"[7] in 2017 to address systematically cybersecurity issues that emerged because of the introduction of IoT concepts[8].

Considering EU policy in terms of typical industrial initiatives, the DSM focuses on facilitating coordination of European, national and regional initiatives, such as the German *Industrie 4.0*[9], Dutch *Smart Industry*[10] and French *Industrie du Futur*[11]. In 2016, a relevant communication from the European Commission was issued[12]. Through these initiatives, the EU aims to boost innovation and prepare for new products and services.

As IoT and digitisation of industry rely on the exchange, processing and storage of large amounts of data, the recent General Data Protection Regulation (GDPR)[13] must be mentioned when discussing EU policy actions. Its objective is to protect privacy and personal information. It applies to all organisations, including Smart Manufacturing companies and the vendors and operators of IoT devices.

Moving from the EU policy landscape to the international context, in 2017 the US IoT Cybersecurity Improvement Act[14] was introduced to address IoT security issues. Even more recently, the governor of California signed the first IoT cybersecurity law in the United States that is planned to take effect in 2020. It requires manufacturers to equip connected devices with reasonable security features[15]. Apart from this example, the US Department of Homeland Security, NIST and other entities have also worked on addressing cybersecurity issues associated with IoT and Smart Manufacturing through development of guidelines, frameworks and other documents. Notable examples of these initiatives include the Department of Homeland Security's publication "Strategic Principles for Securing the Internet of Things"[16] or NIST's "Cybersecurity Framework Manufacturing Profile"[17].

---

[7] See ENISA (2017) "Baseline Security Recommendations for IoT": https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot/at_download/fullReport

[8] Relation of this document to ENISA Baseline Security Recommendations for IoT has been described in Annex A:.

[9] See more about Plattform Industrie 4.0: https://www.plattform-i40.de/I40/Navigation/EN/Home/home.html

[10] See more about Smart Industry: https://www.smartindustry.nl/

[11] See more about Alliance Industrie du Futur: http://www.industrie-dufutur.org/

[12] See European Commission (2016) "Digitizing European Industry. Reaping the full benefits of a Digital Single Market": https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016DC0180

[13] See European Parliament and Council of European Union (2016) "General Data Protection Regulation": https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679

[14] See United States Congress (2017) "Internet of Things (IoT) Cybersecurity Improvement Act of 2017": https://www.congress.gov/bill/115th-congress/senate-bill/1691/text?format=txt

[15] See more about the California's IoT cybersecurity law: https://www.cnet.com/news/california-governor-signs-countrys-first-iot-security-law/

[16] See U.S. Department of Homeland Security (2016) "Strategic Principles for Securing the Internet of Things": https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf

[17] See NIST (2017) "Cybersecurity Framework Manufacturing Profile": https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8183.pdf

Analysing EU and international initiatives makes it possible to highlight several policy initiatives related to the security of IoT. However, IoT security in the industrial environment is still regarded as a matter for consideration by regulatory bodies, as Industry 4.0 and Smart Manufacturing concepts utilising IoT are still in the process of being devised.

1.4 Target Audience

This study provides a set of guidelines and security measures to improve the IoT cybersecurity posture of Industry 4.0 and Smart Manufacturing organisations, namely organisations that have adopted or plan to adopt Industrial Internet of Things devices and solutions. These security measures apply to a wide audience spanning IIoT operators and manufacturers/vendors. The list of potentially targeted profiles includes (but is not limited to) the following:

- Industrial IoT experts, software developers and device manufacturers
- Industrial IoT operators and users
- OT and IT security experts and solution architects
- Persons in charge of security within Industry 4.0 organisations (e.g. CISOs)
- Members of international Industry 4.0 organisations and security communities
- Academic and Research Development Institutions.

In addition, this document may also support discussions at the policy-making level and therefore be of interest to the potential development of related regulations on Industrial IoT security.

1.5 Methodology

The methodology (as depicted in Figure 1) followed to conduct this study consists of the following five tasks.

Figure 1: Methodology adopted for the study

Task 1: Definition of the project scope and identification of experts – The first step consisted of establishing the scope of the project and selecting subject matter experts whose input and insights were considered for the development of the report. The members of the ENISA IoTSEC[18] (IoT Security) and EICS[19] (ENISA Industry 4.0 Cyber Security) Informal Expert Groups as well as selected additional stakeholders formed the pool of subject matter experts. In total experts from 42 different bodies contributed to the development and validation of the study.

Task 2: Desktop research – During this step, extensive search for relevant documents in the context of the project was conducted. The identified sources served as a reference to develop good practices and other parts of the report.

[18] See more about IoT Security Experts Group: https://resilience.enisa.europa.eu/iot-security-experts-group-1
[19] See more about EICS Experts Group: https://resilience.enisa.europa.eu/eics-experts-group

Task 3: Questionnaire and series of interviews with selected subject matter experts – ENISA developed a questionnaire covering various Industrial IoT and Industry 4.0 security aspects. The questionnaire was completed by a group of subject matter experts. Furthermore, a series of interviews with these experts took place, through which ENISA collected valuable input to prepare this report.

Task 4: Analysis of collected material and report development – The inputs collected from desktop research and collaboration with stakeholders were thoroughly analysed by ENISA's experts. Based on this analysis, the first draft of this report was developed.

Task 5: Review and validation – ENISA once again reached to its subject matter experts, this time to share the draft of the report with them to obtain comments and feedback. Taking into account the stakeholders' feedback, the final version of this report was developed and validated by the subject matter experts during the validation workshop held in The Hague, NL on the 26th of October 2018.

This methodology enabled ENISA to engage actively with the interested stakeholders and:

- define terminology (e.g. Industry 4.0, Smart manufacturing, Industrial IoT etc.),
- identify the corresponding assets (what kind of assets and where and how they are used across the manufacturing process and value chain, its path and evolution over time),
- identify possible threats, risks and attack scenarios posed against the Industrial IoT,
- map identified threats to assets,
- list security measures related to the use of IoT in Smart Manufacturing.

1.6 Structure

The study is structured as follows:

- Chapter 1: Introductory information on the objectives, scope, context, target audience, methodology and structure of the study.
- Chapter 2: Definition of Industry 4.0 and its components with an overview of the concepts discussed and the related security challenges.
- Chapter 3: Threat and risk analysis containing a taxonomy of the threats and examples of Industry 4.0/Smart Manufacturing attack scenarios.
- Chapter 4: Description of security measures and good practices mapped to threats, security domains, standards and other relevant documents.

2. Industrial IoT: Industry 4.0 and Smart Manufacturing

2.1 Definition

This report focuses on the IoT, Industry 4.0, Smart Manufacturing and IIoT, which are relatively new terms. There is a veritable plethora of definitions for these terms while commonly held definitions are lacking. Depending on the source and context, the descriptions of these terms may vary significantly. Thus, it is important to adopt specific definitions and clarify our understanding of those terms. In this study, ENISA defines IIoT as IoT (as defined in the ENISA Baseline IoT Security Recommendations[20]) applied in the industrial environment. Industry 4.0 is, in turn, a much broader concept that encompasses IIoT and Smart Manufacturing alike.

ENISA defines Industry 4.0 as **"a paradigm shift towards digitalised, integrated and smart value chains enabling distributed decision-making in production by incorporating new cyber-physical technologies such as IoT".**

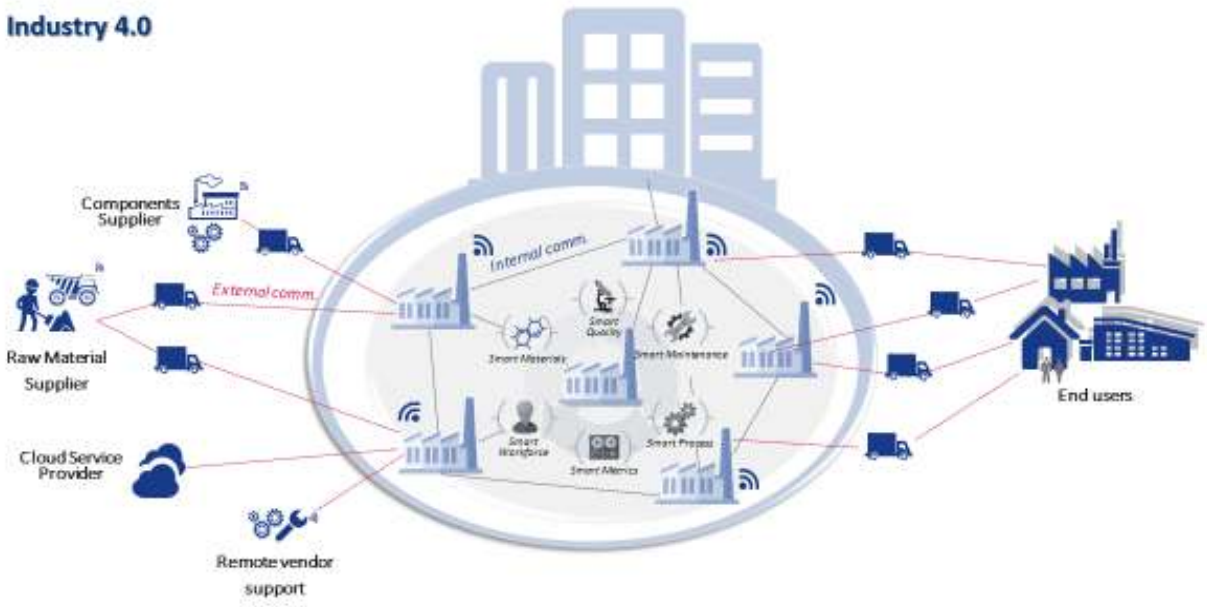

Figure 2: Communication relationships in Industry 4.0

Industry 4.0 design principles, often referred to as the fourth industrial revolution, include interoperability, autonomy, information transparency, technical assistance and distributed decisions[21]. Recent technological

[20] See ENISA (2017) "Baseline Security Recommendations for IoT": https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot/at_download/fullReport

[21] See Connected Factory Global (2016) "Manufacturing Control System Cybersecurity: Risk Assessment & Mitigation Strategies": http://www.connectedfactoryglobal.com/resources/cybersecurity-report/

advances that resulted in reversal of the traditional production process logic led to the formation of this concept, representing a shift towards decentralised production. With the advent of Industry 4.0, a product is not merely processed by machines – it communicates with its environment providing relevant information and instructions (referring to the notion of digital twin). No longer isolated, products and production lines have become integral parts of the overall network.

Contrary to the traditional approach to industry in which a hardware-based structure with a clear communication hierarchy was prevalent, Industry 4.0 introduced flexible systems whose functions are not bound to hardware but distributed throughout the network. In these new systems internal communication can now be observed across an organisation's hierarchical levels. New types of interactions have been introduced (see Figure 2) and external interactions between organisations have changed significantly and become more flexible.[22]

Industry 4.0 connects production to information and communication technologies. It merges end user data with machine data and enables machines to communicate with each other. As a result, it has become possible for components and machines to manage production autonomously in a flexible, efficient and resource-saving manner. Its benefits include, among others, higher product quality, greater flexibility, shorter product launch times, new services and business models.[23] It is important to note that the flows depicted in the figure refer to physical goods and data (e.g. exchange of digital twins). Data flows are bidirectional at least, e.g. customers may provide feedback to the production/manufacturing process.

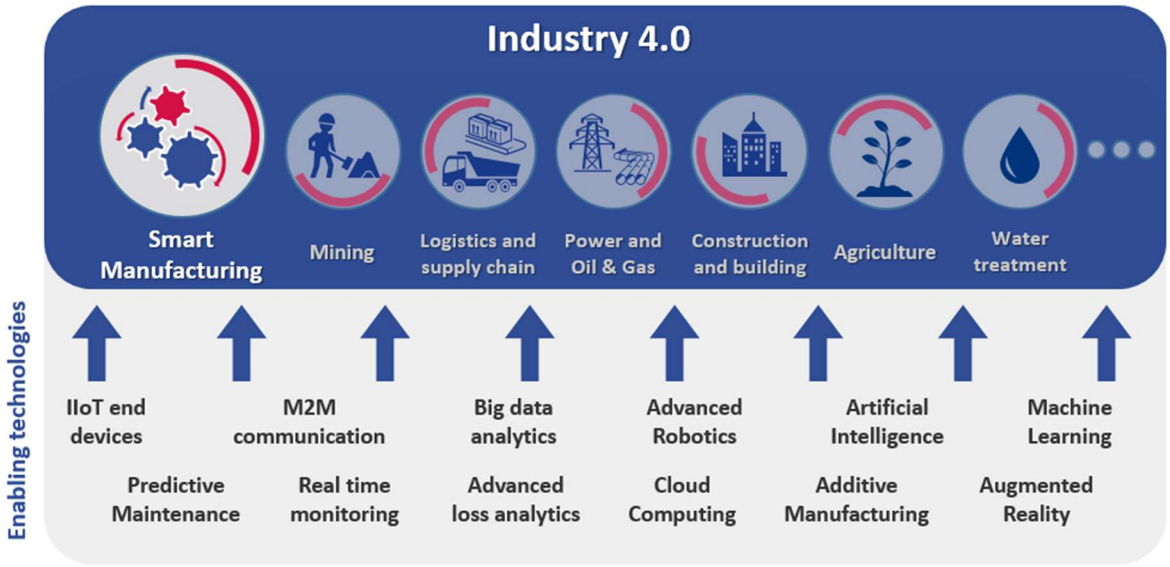

Figure 3: Smart Manufacturing in Industry 4.0

By introducing a wide array of new capabilities, Industry 4.0 acts as an enabler for a new approach to manufacturing, namely Smart Manufacturing. This particular concept, focusing on product manufacturing using new technologies, constitutes only a small part of Industry 4.0, which may be regarded as a superset

[22] See Plattform Industrie 4.0 (2016) "Technical Overview: Secure Identities": https://www.plattform-i40.de/I40/Redaktion/EN/Downloads/Publikation/secure-identities.pdf?__blob=publicationFile&v=9
[23] See Plattform Industrie 4.0 (2018) "RAMI4.0 – a reference framework for digitalisation": https://www.plattform-i40.de/I40/Redaktion/EN/Downloads/Publikation/rami40-an-introduction.pdf?__blob=publicationFile&v=4

encompassing a variety of industrial areas. Figure 3 illustrates how Smart Manufacturing is related to Industry 4.0 and other technologies in use.

ENISA defines Smart Manufacturing as **"next-generation industrial manufacturing processes and systems built on emerging information and communication technologies in line with Industry 4.0, such as additive manufacturing, advanced analytics and IT/OT integration"**. This new term describes systems that – by using connected devices and sensors – attempt to maximise capabilities such as cost, delivery, flexibility and quality by using advanced technologies that promote rapid flow and widespread use of digital information[24]. Smart Manufacturing combines some of the functionalities of earlier manufacturing models, while introducing its own new capabilities included advanced decision-making. Together with collaborative supply chains, organisations may quickly adapt to market changes and disruptions.

To achieve innovation and the desired enhanced capabilities, Industry 4.0 and Smart Manufacturing benefit from various technologies (see Figure 4), such as:

- IIoT end devices
  Devices that have various capabilities, such as sensing, actuating, storing and/or processing data and that exchange data over the network.
- Machine-to-machine (M2M) communication
  Technologies that facilitate direct communication between devices in the network without human assistance.
- Big data analytics
  Process of examining vast amounts of various types of data sets generated in real time by smart sensors, devices, log files, video and audio.
- Advanced Robotics
  Advanced industrial robots designed for complex tasks with smart capabilities, such as the ability to learn from their errors and improve their performance.
- Artificial Intelligence (AI)
  Algorithms that enable computers and digital machines to perform tasks typically associated with intelligent human beings.
- Machine Learning (ML)
  Algorithms that enable computers to act and improve their ability to predict without being explicitly programmed.
- Predictive Maintenance
  Solutions that monitor the condition of equipment predicting when the failure may occur to perform maintenance effectively at the lowest possible frequency.
- Real time monitoring
  Technologies that enable collection and aggregation of security data from system components and monitoring and analysis of events that occur in the network.
- Advanced loss analytics
  Methods for analysis of various types of losses that may occur in a Smart Manufacturing environment with the objective to eliminate or reduce them.
- Cloud Computing
  Solutions enabling access to shared sets of resources such as networks, servers and applications with minimal requirements concerning managerial effort and service provider interaction.

[24] See NIST (2016) "Current Standards Landscape for Smart Manufacturing Systems": https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8107.pdf

- Additive Manufacturing
  Technologies that enable the creation of objects of various geometric shapes by adding material, e.g. 3D printing or rapid prototyping.
- Augmented reality
  Technologies that modify the perception of the real-world environment, for example technologies used in Smart Manufacturing to improve the efficiency of manual assembly tasks.

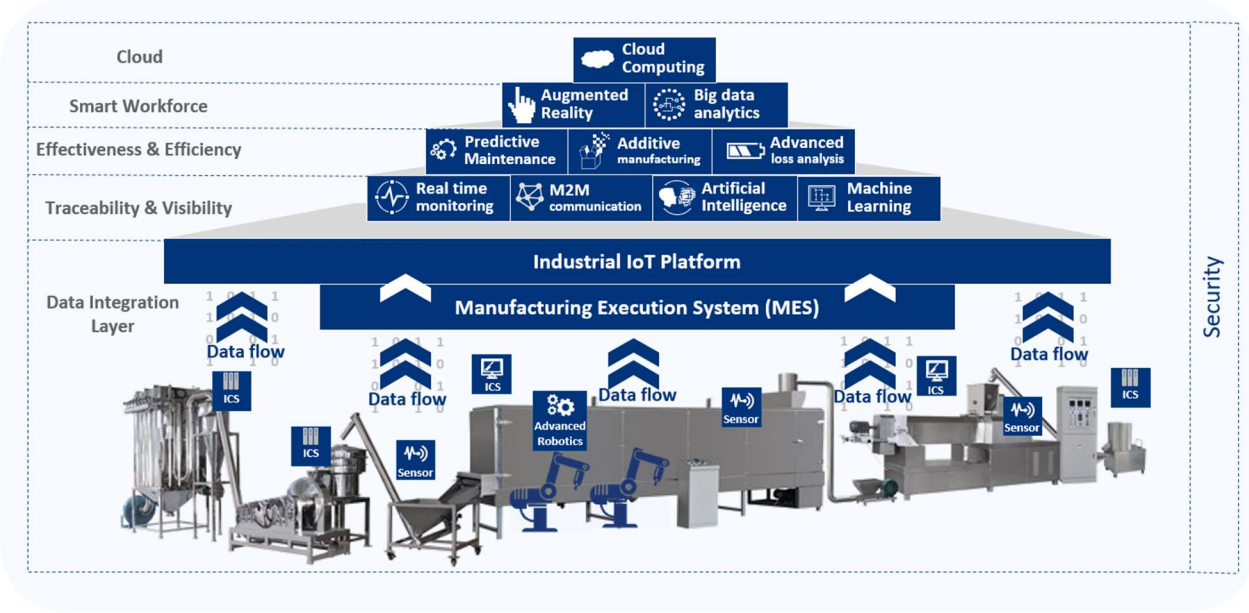

Figure 4: Industry 4.0 and Smart Manufacturing capabilities

The notions of Industry 4.0 and Smart Manufacturing are rather complex. Based on the responses received by the subject matter experts in interviews and analysis of relevant publications, ENISA has identified the following main elements:

- **ICS (Industrial Control Systems)** – This group consists of control systems, such as SCADA (supervisory control and data acquisition) and DCS (distributed control systems), as well as other control system elements and devices, such as PLCs (programmable logic controllers) and HMIs (human machine interfaces). Various control components within the system cooperate with each other to achieve a specified control objective, e.g. manufacturing a product or desired state that is within pre-set parameters such as keeping the flow of a liquid in a pipe within the bounds of the desired flow rate, pressure or temperature, respectively. Additionally, ICSs may contain remote diagnostics and maintenance tools.
- **IIoT End Devices** – These devices have various capabilities, such as sensing, actuating, storing and/or processing information. What distinguishes them from traditional devices such as sensors and actuators that have been used in industrial applications for years is the fact that IIoT End Devices exchange data over the network. In Smart Manufacturing environments, by making large amounts of new types of data available, they contribute to streamlining production.
- **Manufacturing and business processes** – This group consists of activities that lead to achieving a certain goal, in this case obtaining a final product from raw materials or components. These processes include technological procedures that may vary considerably depending on the characteristics of the company, as well as organisational processes, which enable the whole company to operate successfully.

- **Artificial Intelligence and Machine Learning** – In Smart Manufacturing, due to the collection of enormous amounts of data from industrial process, various ML and AI algorithms are utilised for analysis. Artificial Intelligence transforms manufacturing by making it easily adaptable without having to spend long hours to reprogram industrial robots, enabling predictive maintenance and increasing flexibility.[25]
- **Control systems communication networks and their components** – This group includes networks, network devices and industrial protocols. Networks play a significant role in a Smart Manufacturing ecosystem since they allow different nodes to exchange data and information with each other via a data link. Networks in control systems communication include serial and digital links to transfer inputs and outputs to/from end devices. Network devices include gateways, routers, switches, etc. Typical examples of industrial communication protocols include (but are not limited to): e.g. HART[26], Modbus TCP/IP[27], OPC[28] and OPC-UA[29].

2.2 Security Challenges

The numerous benefits of adopting Industry 4.0 technologies and making manufacturing *Smart* go hand in hand with significant security challenges. A recent survey revealed that stakeholders are becoming aware of this problem, as 65% of companies believe that OT/ICS cybersecurity risks are more likely with IoT technologies[30]. The following detail the generic security challenges that Smart Manufacturing and Industry 4.0 face:

- Vulnerable components – Along with the fourth industrial revolution, the new Internet of Things (IoT) landscape has emerged with millions of connected devices globally. That is why securing IoT in Smart Manufacturing entails affording protection to an enormous number of connected assets. What is more, IoT cybersecurity is not an isolated concept; it is interconnected with a number of security disciplines, e.g. IT security, OT security and physical safety making this landscape even broader. As a result of shifting from closed to connected cyber-physical systems, Smart Manufacturing companies need to handle the issue of the typical vulnerabilities in those systems. In industrial environments this may pose a considerable challenge since most systems of this type were not designed with cybersecurity in mind[31] and thus vulnerabilities in this hardware are becoming more and more common[32].
- Management of processes – In addition to the large attack surface in terms of connected devices, a multitude of complex processes involved in Smart Manufacturing should also be considered. Management of processes with cybersecurity in mind poses a challenge for Industry 4.0 companies, especially since functionality and production efficiency are usually seen as having a higher priority than cybersecurity.
- Increased connectivity – Manufacturing processes need to interact with objects and environments on a global scale and systems used in Smart Manufacturing need to enable collaboration across multiple

[25] See TOPBOTS (2017) "Future Factories: How AI enables smart manufacturing": https://medium.com/topbots/future-factories-how-ai-enables-smart-manufacturing-c1405f4ec0e6
[26] See HART (Highway Addressable Remote Transducer Protocol): https://www.fieldcommgroup.org/technologies/hart
[27] See MODBUS TCP/IP Specification: http://www.modbus.org/specs.php
[28] See OPC (Open Platform Communications): https://opcfoundation.org/about/what-is-opc/
[29] See OPC Unified Architecture (OPC UA): https://opcfoundation.org/about/opc-technologies/opc-ua/
[30] See Kaspersky Lab (2018) "Worried about IoT, but hit by malware: Kaspersky Lab reveals industrial organization pain points": https://www.kaspersky.com/about/press-releases/2018_ics-cybersecurity
[31] See Hongmei He (2017) "Security Challenges on the Way Towards Smart Manufacturing": https://www.iotsecurityfoundation.org/security-challenges-on-the-way-towards-smart-manufacturing/
[32] See Positive Technologies (2018) "ICS SECURITY: 2017 IN REVIEW": https://www.ptsecurity.com/upload/corporate/ww-en/analytics/ICS-Security-2017-eng.pdf

organisations. One of the biggest challenges for higher connectivity is that security can exert a direct impact on safety.

- IT/OT convergence – Industrial control systems ceased to be isolated once the incorporation of IT components in the ICS domain become a common practice. Converging with IT network-enabled organisations simplified the management of complex environments while also introducing new security risks. Managing IT/OT integration is a significant challenge. The contributing factors include insecure network connections (internal and external), utilisation of technologies with known vulnerabilities that introduce previously unknown risks into the OT environment, and insufficient understanding of requirements for ICS environments. Holistic security must cover digital twin and physical implementation.
- Supply chain complexity – Companies that manufacture products or solutions are very rarely able to produce every part of the product itself and usually need to rely on third parties' components. Developing technologically sophisticated products results in an extremely complex supply chain with a large number of people and organisations involved, thereby making it highly demanding in terms of management. Not being able to track every component to its source means not being able to ensure product security, which is only as secure as its weakest link.
- Legacy industrial control systems – Legacy hardware is a significant barrier to adoption of the Industrial Internet of Things by over a third of the respondents according to a recent survey[33]. Manufacturers build new systems on top of legacy systems, and this may result in outdated protection measures and contain unknown vulnerabilities that have been inactive for years. Adding new IoT devices to outdated hardware raises concerns that it may allow attackers to find a new way to compromise systems.
- Insecure protocols – Manufacturing components communicate over private industrial networks using specific protocols. In modern network environments, these protocols often fail to ensure proper protection against cyber-threats. According to a recent report, 4 of the 5 least secure protocols are ICS-specific[34].
- Human factors – Adopting new technologies means that factory workers and engineers have to work with new types of data, networks and systems in novel ways. They are unaware of the risks associated with gathering, handling and analysing that data and can thus become an easy target for attackers. This is becoming all the more disturbing given that the industry most targeted by phishing emails in 2016 was Manufacturing[35].
- Unused functionalities – Industrial machines are designed to offer a large number of functions and services, many of which may not be necessary for operation. In industrial environments, machines or their selected components often have access to unused functionalities that may considerably expand the potential attack area and become gateways for the attackers.
- Safety aspects – The presence of actuators that act on the physical world makes safety aspects very relevant in IoT and Smart Manufacturing. Security for safety emerges as an objective of paramount importance.
- Security updates – Applying security updates to IoT is extremely challenging, since the particularity of the user interfaces available to users does not allow traditional update mechanisms. Securing those mechanisms is in itself a daunting task, especially considering Over-The-Air updates. In OT environments in particular, applying updates may be challenging since this operation needs to be scheduled and performed during downtime.

[33] See World Economic Forum (2015) "Industrial Internet of Things: Unleashing the Potential of Connected Products and Services": http://www3.weforum.org/docs/WEFUSA_IndustrialInternet_Report2015.pdf
[34] See Synopsys (2017) "State of Fuzzing 2017": https://www.synopsys.com/content/dam/synopsys/sig-assets/reports/state-of-fuzzing-2017.pdf
[35] See NTT Security (2017) "Global Threat Intelligence Report 2017": https://www.nttsecurity.com/en-us/gtir-2017

- Secure product lifecycle – Device security should be a subject of consideration through the product's entire lifecycle, even end-of-life/end-of-support of the machine.

2.3 High-level reference model

Smart Manufacturing environments consisting of a large number of elements can seem unduly complicated. To provide a better explanation of this concept, a high-level reference model based on the Purdue Model (i.e. the Purdue Enterprise Reference Architecture[36] developed by Theodore J. Williams and members of the Industry-Purdue University Consortium for Computer Integrated Manufacturing, as referenced in ISA-95[37]) tailored to the scope of this project has been proposed (see Figure 5).

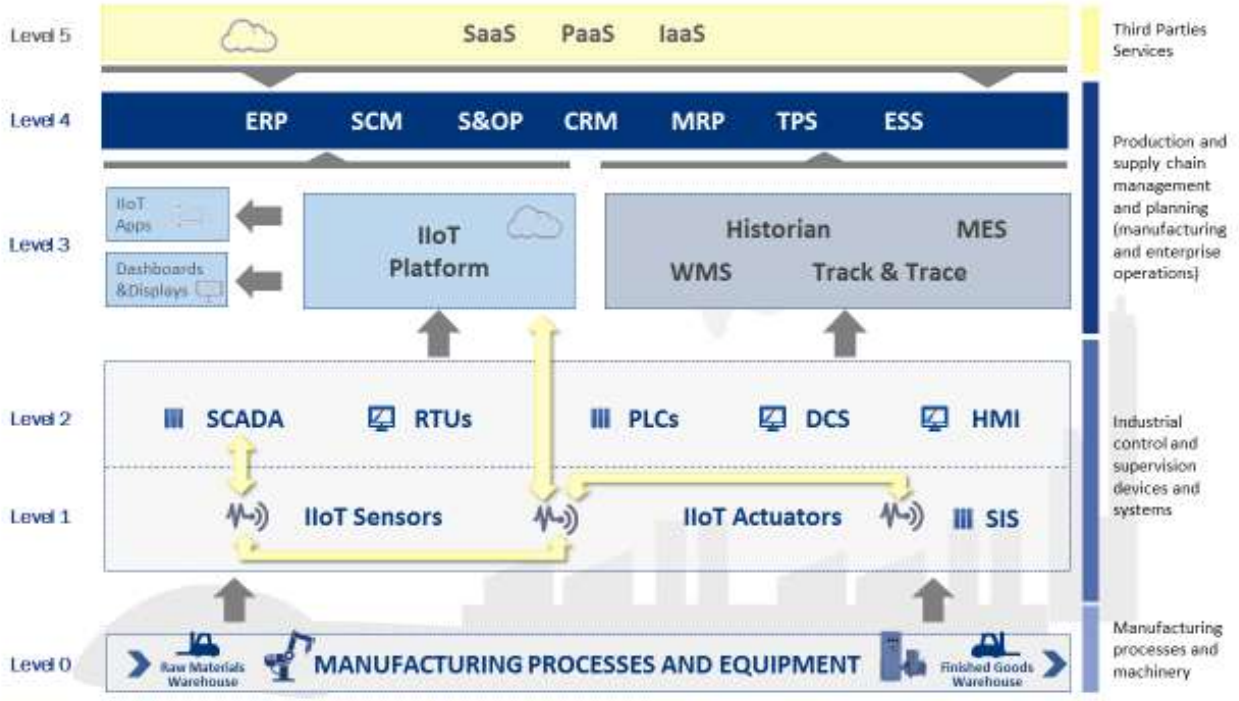

Figure 5: High-level reference model

The presented concept divides Smart Manufacturing environment into 6 layers. These layers are arranged in order, with the lowest one being the manufacturing processes (Layer 0), followed by devices, systems and services (Layers 1-5). Levels 1 and 2 represent OT layers. IIoT devices fall into the Layer 1 of this model. Layer 4 corresponds to the IT part of a corporation, while Layer 3 is an intermediate layer with systems classified in-between IT and OT. IIoT Platform utilisation was included as part of the Layer 3. The highest layer, which did not appear in the Purdue Model, is specific for Smart Manufacturing, where external services are commonly used.

The objective of the reference model is to provide a general overview of relationships between the most important assets (see section 2.4) and components (see section 2.1). Grey arrows represent simplified communication paths between larger groups in the model (i.e. on the left of the picture). Additionally, new

[36] See The Purdue Enterprise Reference Architecture by T.J. Williams: https://www.sciencedirect.com/science/article/pii/0166361594900175
[37] See ISA95: https://www.isa.org/isa95/

communication paths introduced by Industry 4.0 and enabled by the incorporation of IIoT devices into the network, e.g. communication between IIoT devices and direct connection of IIoT devices to IIoT platform, have been added on top of the model with yellow arrows to emphasise their criticality in terms of security and privacy. In what follows, we briefly described the levels of the reference model.

Level 0: Manufacturing processes and equipment (machines, robots)

This is the lowest level of the IIoT environment where manufacturing processes executed by smart machines and robots take place. These processes are measured and controlled by devices and systems in higher layers of the reference model.

Level 1: IIoT devices – sensors and actuators

This layer comprises IIoT devices that measure system parameters (IIoT sensors) and execute specific actions (IIoT actuators). Data is transmitted between IIoT devices and control systems (Level 2) as well as IIoT platform (Level 3). Level 1 also includes SIS.

Level 2: Industrial control devices and systems

These are devices and systems that control the industrial processes (Layer 0) based on information from IIoT devices (Level 1). They include controllers (PLCs, RTUs), distributed control systems (DCS), operator panels (HMI) and supervision and control systems (SCADA).

Level 3: Manufacturing operations systems and IIoT Platform

This is an intermediate layer between OT and IT environment. It comprises systems that are used to manage manufacturing processes, e.g. Manufacturing Execution Systems (MES), Historian, Warehouse Management System (WMS) and Track & Trace systems. These systems communicate with both OT and IT environments. Distinguishing this layer makes it possible to control this communication and prevents direct communication between the OT and IT layers. Level 3 of the model also includes an IIoT platform that analyses and manages data from the manufacturing and control processes provided by IIoT devices. It is closely related to the OT environment and provides information to the systems in the layer above.

Level 4: Enterprise operations systems

These IT systems support a company's operations at an enterprise level. They include supply chain and production management and planning. In contrary to level 2 systems, they do not operate in real-time. This layer includes the following systems (this list is not meant to be exhaustive): Enterprise Resource Planning (ERP), Supply Chain Management (SCM), Sales & Operations Planning (S&OP), Customer Relationship Management (CRM), Material Requirements Planning (MRP), Transaction Processing System (TPS) and Executive Support System (ESS).

Level 5: Third Parties' services

As mentioned before, reliance on Third Parties' services is an inherent characteristic of Smart Manufacturing. For this reason, to better reflect Industry 4.0 and Smart Manufacturing specifics, we decided to place an additional layer on top of the ISA 95 model to include Third Parties services. These services may take different forms, e.g. Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS).

2.4 Asset taxonomy

To focus on the details of IoT security in Smart Manufacturing it is essential to start from identification and decomposition of assets of such vast and complex environments. Here we provide an overview of the key asset groups and assets that need to be protected. Industry 4.0/Smart manufacturing assets are classified into key groups depicted in Figure 6 and described in Table 1. The levels assigned to each asset group in the table correspond to the levels defined in section 2.3, i.e. High-level reference model depicted in Figure 5. It

should be noted that the lowest level of the taxonomy is indicative and not exhaustive. For instance, not all sensor types or network protocols are listed, just some representative ones.

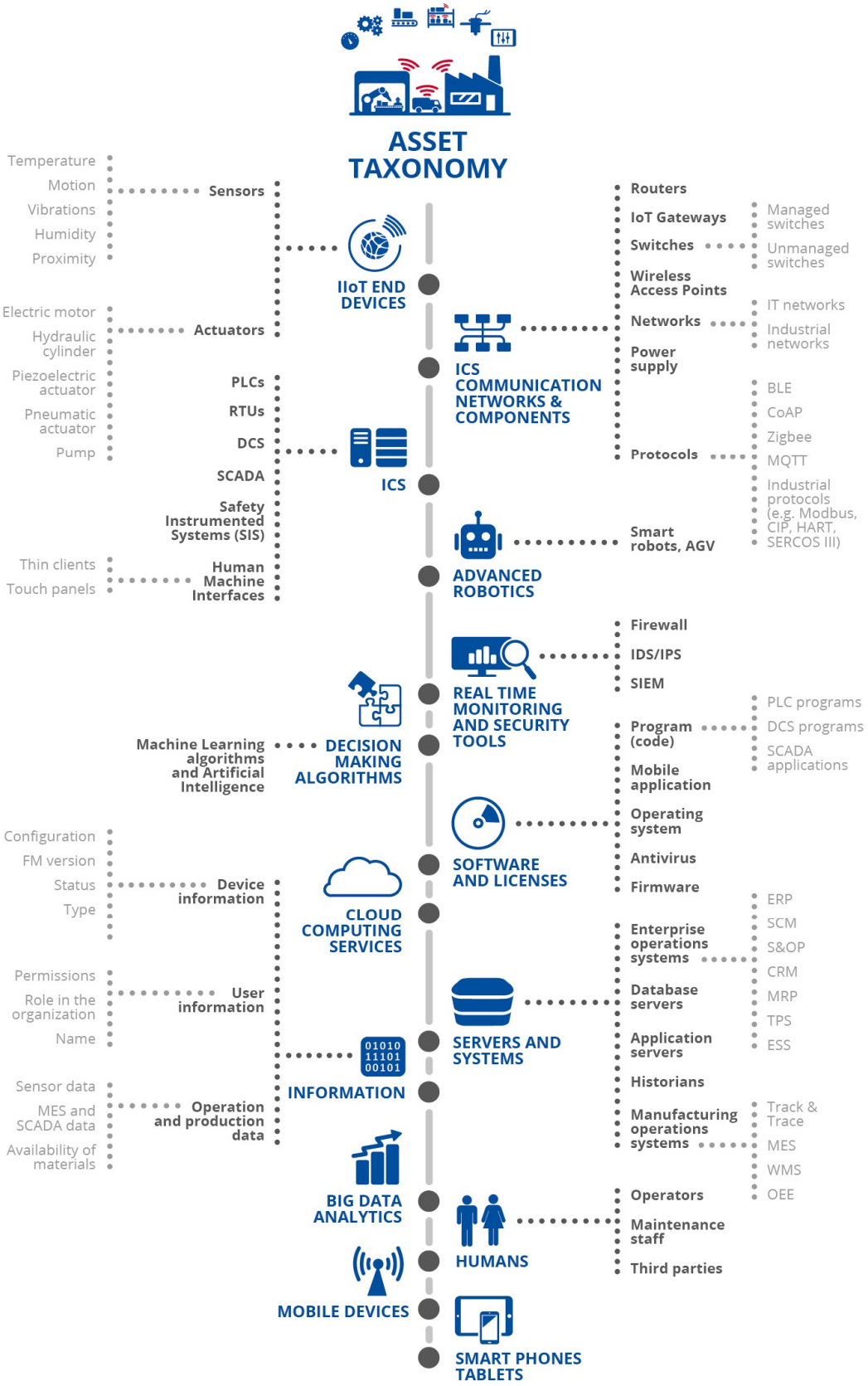

Figure 6: Industry 4.0 asset taxonomy

ASSET GROUP	ASSETS	DESCRIPTION
IIoT End Devices Level 1	Sensors	These devices detect and/or measure events in their environment and transmit information to other electronic systems to be processed. There are sensors for many purposes, such as to measure temperature, motion, vibration etc.
	Safety Instrumented Systems (SIS)	These systems consist of sensors, logic solvers, and final control elements (actuators) whose objective is to bring the process to a safe state in case of a violation of predetermined conditions.
	Actuators	These devices interact with the environment by moving or controlling a mechanism or system. In order to do so, they convert energy (e.g. electrical, hydraulic or pneumatic) into motion.
ICS Level 2	PLCs	These specialised industrial computers are used to automate control functions within the industrial network. Typically, they are equipped with additional plug-in modules, such as Input / Output modules to connect sensors and actuators.
	RTUs	These devices are used typically in substations or remote locations. Their objective, similar to PLCs, is to monitor field parameters and send data to the central station.
	DCS	These control systems distribute intelligence, i.e. management logic, about the controlled process instead of relying on a single central unit.
	SCADA	These systems are used to collect data from industrial assets and processes, their visualisation, supervision and control. Such workstations usually operate on the Windows operating system.
	Human Machine Interfaces	These control panels and dashboards allow the operators to monitor and control PLCs, RTUs and other electronic devices.
ICS communication networks & components Levels 1 - 3	Routers	These networking devices forward data packets between different networks in industrial environments and IoT ecosystems.
	IIoT Gateways	These network nodes are used to interface with another network from an IoT environment using different protocols. Gateways may provide protocol translators, fault isolators, etc., to provide system interoperability.
	Switches	These network components filter and forward packets within the local area network.
	Wireless Access Points	These components enable wireless devices to connect to a wired network using Wi-Fi, or related standards.
	Firewall	These network security devices or systems control network traffic between networks or between a host and a network based on predetermined rules.
	Networks	They allow the different nodes of an IoT ecosystem to exchange data and information with one another, via a data link. There are different kinds of networks related to their spatial coverage, including e.g. (W)LANs, (W)PANs, PANs and (W)WANs, among others.

ASSET GROUP	ASSETS	DESCRIPTION
	Protocols	They define the set of rules on how two or more IoT devices communicate over a given channel. There are many communication protocols, which can be either wired or wireless.
	Power Supply	It supplies electric power to an IoT device and its internal components. The power source can be external and wired or a battery integrated in the device itself.
Information All levels	Operation and production data	This includes information about IIoT system operation and production data, such as sensor data, MES and SCADA data, etc.
	Device Information	This includes information such as model, type, configuration, firmware version, status, etc. IP address, physical location, etc. The asset inventory contains this information about all system devices.
	User Information	This includes information such as name, role, permissions, etc.
Decision Making Algorithms Levels 2-5	Artificial Intelligence and Machine Learning	These terms describe the ability of a machine (e.g. computer, robot, etc.) to perform tasks typical for intelligent beings. In Smart Manufacturing, where enormous amounts of data is collected from industrial process, various ML and AI algorithms can be utilised for analysis.
Cloud Computing Services[38] Levels 3-5	These services enable swift universal network access to a shared set of resources such as networks, servers and applications with minimal requirement of management effort and service provider interaction.	
Big Data Analytics Levels 3-5	In Smart Manufacturing, this term describes the process of examining vast amounts of various data sets generated in real time by smart sensors, devices, log files, video and audio. This data is created on all automation levels including manufacturing plant, transaction applications, etc. Big Data is analysed to uncover hidden patterns, unknown correlations, trends and other useful information that can help make more-informed and deliberate decisions.	
Advanced Robotics Level 0	Smart Robots, Automated guided vehicles	These sophisticated industrial robots are designed to perform complex tasks with smart capabilities, such as the ability to learn from errors and improve their performance.
Real time monitoring and security tools Levels 3-5	SIEM	These applications are utilised to collect and aggregate security data from various system components and render them in the form of meaningful information via a single interface.
	IDS/IPS	These systems enable automatic monitoring of the events that occur in a computer system or network and their analysis for signs of possible incidents. In addition, IPS may execute actions in an attempt to stop detected incidents.
Software and Licenses Levels 2-5	Program (code)	These programs are written for devices within an IIoT ecosystem to achieve specific technological objectives, including PLC logic, SCADA applications, HMI applications, industrial robot programs, etc.

[38] See ENISA's study on Cloud Computing, "Towards secure convergence of Cloud and IoT":
https://www.enisa.europa.eu/publications/towards-secure-convergence-of-cloud-and-iot

ASSET GROUP	ASSETS	DESCRIPTION
	Operating System	This term refers to a system that manages computer hardware resources and provides common services for other computer programs to run.
	Mobile application	These programs run on mobile devices, such as tablets and smartphones, which are used for remote supervision and control of a process (e.g. mobile SCADA client applications), equipment maintenance and other tasks (e.g. warehouse inventory).
	Antivirus	This term refers to a software that monitors a computer or network to identify malware, prevent it from infecting devices and clean infected devices.
	Firmware	This term refers to a class of software stored on a device's read-only memory and provides instructions on how the device should operate. During execution, it cannot be dynamically written or modified.
Servers and Systems Levels 3-5	Historians	These software systems gather data from industrial devices and store them in specialized databases.
	Application Servers	These computers host applications, e.g. user workstations' applications.
	Database Servers	These servers are used as repositories for event information provided by sensors, agents, and management servers.
	Enterprise operations systems (e.g. ERP, CRM)	These systems integrate information from various parts of an organization (i.e. manufacturing, distribution, financials, human resources, etc.). They also provide a connection between organization and its customers and suppliers.
	Manufacturing operations systems (e.g. MES)	These systems automate production control and process automation using network computing, bridging the gap between business and plant-floor. These systems are used for downloading instructions, scheduling and uploading information on production results.
Mobile devices Level 3	Tablets, smartphones	These portable devices can be operated by hand. They run mobile applications enabling operators to perform various tasks.
Personnel All levels[39]	Operators, maintenance staff, third parties	This asset group refers to all the individuals who have physical or remote access to the OT system. People are inseparable elements of manufacturing environments and hence must be taken into consideration when defining critical assets in terms of security. All the people with access to an OT environment can introduce malware to the system (intentionally or unintentionally), become targets of phishing or cause damage to the system and compromise its security in a variety of ways. On the other hand, people require particular protection, as their privacy and physical safety may be endangered in the event of security incident.

Table 1: Asset taxonomy

Figure 7 provides a view of the criticality of the main assets described in the asset taxonomy, based on the responses provided by subject matter experts during their interviews. These interviews involved a structured

[39] Indicated levels correspond to the concept of layers as explained in subchapter 2.3 High-level reference model.

questionnaire in which one of the questions referred to an in-depth evaluation of the main IIoT / Smart Manufacturing assets according to their criticality. The experts could select any number of assets they considered the most important in terms of cybersecurity of the IIoT ecosystem. The figures presented below correspond to the percentage of experts who selected a given option.

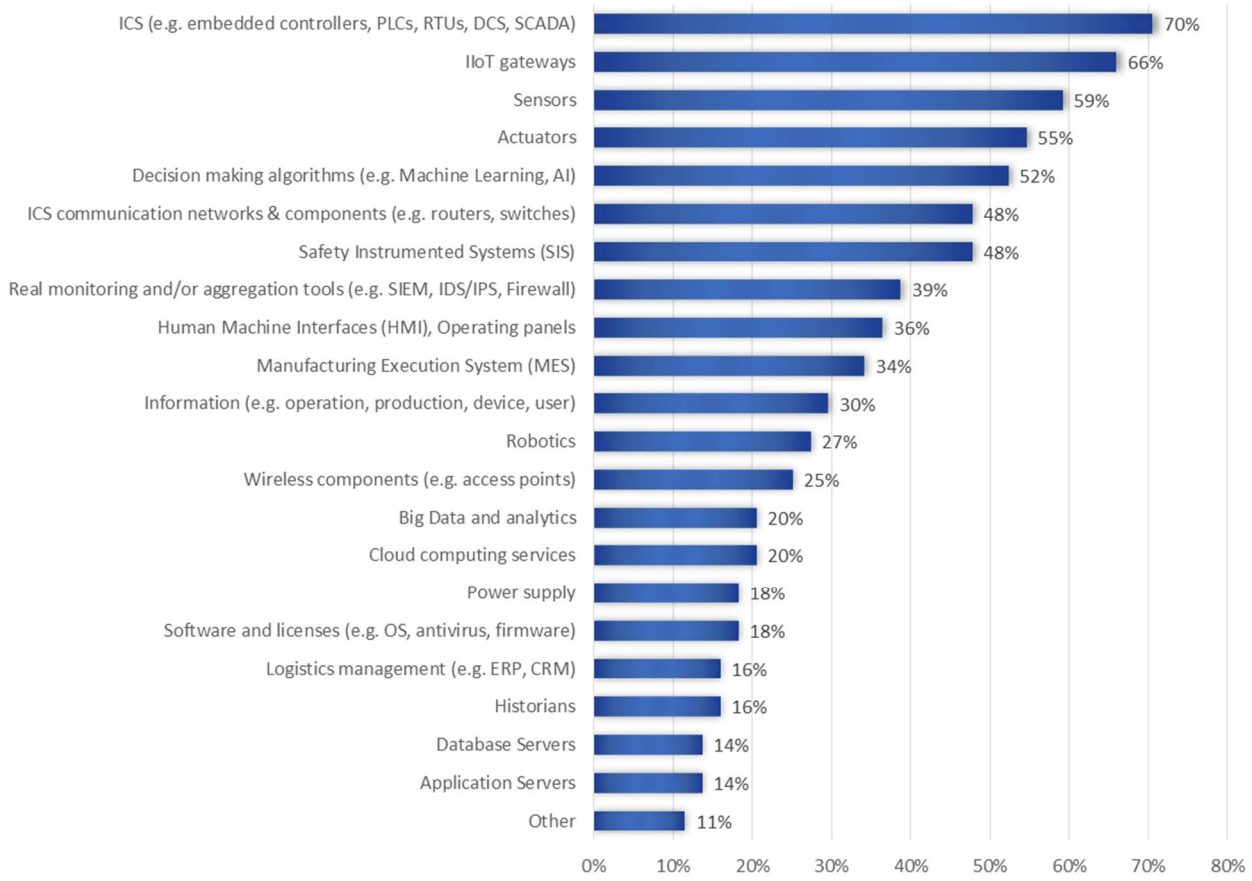

Figure 7: Asset criticality

The figure shows that stakeholders consider ICS, i.e. PLCs, RTUs, DCS and SCADA systems to be the most critical assets for Smart Manufacturing and Industry 4.0. Such a choice comes as no surprise as these systems control and supervise industrial processes and their functioning is therefore indispensable for proper execution and safety of production. As the study revealed, in terms of criticality, industrial control systems are followed by IoT devices, notably IIoT gateways, sensors and actuators. Over half of the respondents selected each of these types of assets confirming that the introduction of new connected devices to OT environments is in fact a security challenge and generates a need for additional protection.

Among the other answers provided by the respondents, the human factor (e.g. operators, maintenance staff and third parties) was highlighted. People were identified as critical assets as they may become targets of phishing campaigns and their errors can allow malware to penetrate a system. Moreover, stakeholders noted that, apart from the assets themselves, asset management is of great importance. To secure the assets properly, companies should be aware of the devices and solutions they have, where they are located and how secure they are, i.e. what type of protection mechanisms/security measures have been applied.

3. Threats and risk analysis

3.1 Threats taxonomy

Industry 4.0 environments face numerous security challenges caused by a large number of factors and hence they need to be prepared to handle a wide variety of cybersecurity threats. In addition to threats related to IoT technologies, Industry 4.0 and Smart Manufacturing companies are likely to be affected by additional threats, which are typical in OT and IT environments. A good illustration of this is the recent large-scale ransomware attack called NotPetya[40], as more that 50% of the companies hit by this attack were industrial companies[41].

In accordance with with ENISA Threat Taxonomy[42], we have developed a threat taxonomy focused on Industry 4.0, which is depicted in Figure 8 and described in detail in Table 2.

[40] See the list of indicative incidents in Annex A:D.
[41] See Kaspersky Lab (2017) "More than 50% of organizations attacked by ExPetr (Petya) cryptolocker are industrial companies": https://ics-cert.kaspersky.com/alerts/2017/06/29/more-than-50-percent-of-organizations-attacked-by-expetr-petya-cryptolocker-are-industrial-companies/
[42] See ENISA (2016) "ENISA Threat Taxonomy A tool for structuring threat information": https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape/etl2015/enisa-threat-taxonomy-a-tool-for-structuring-threat-information

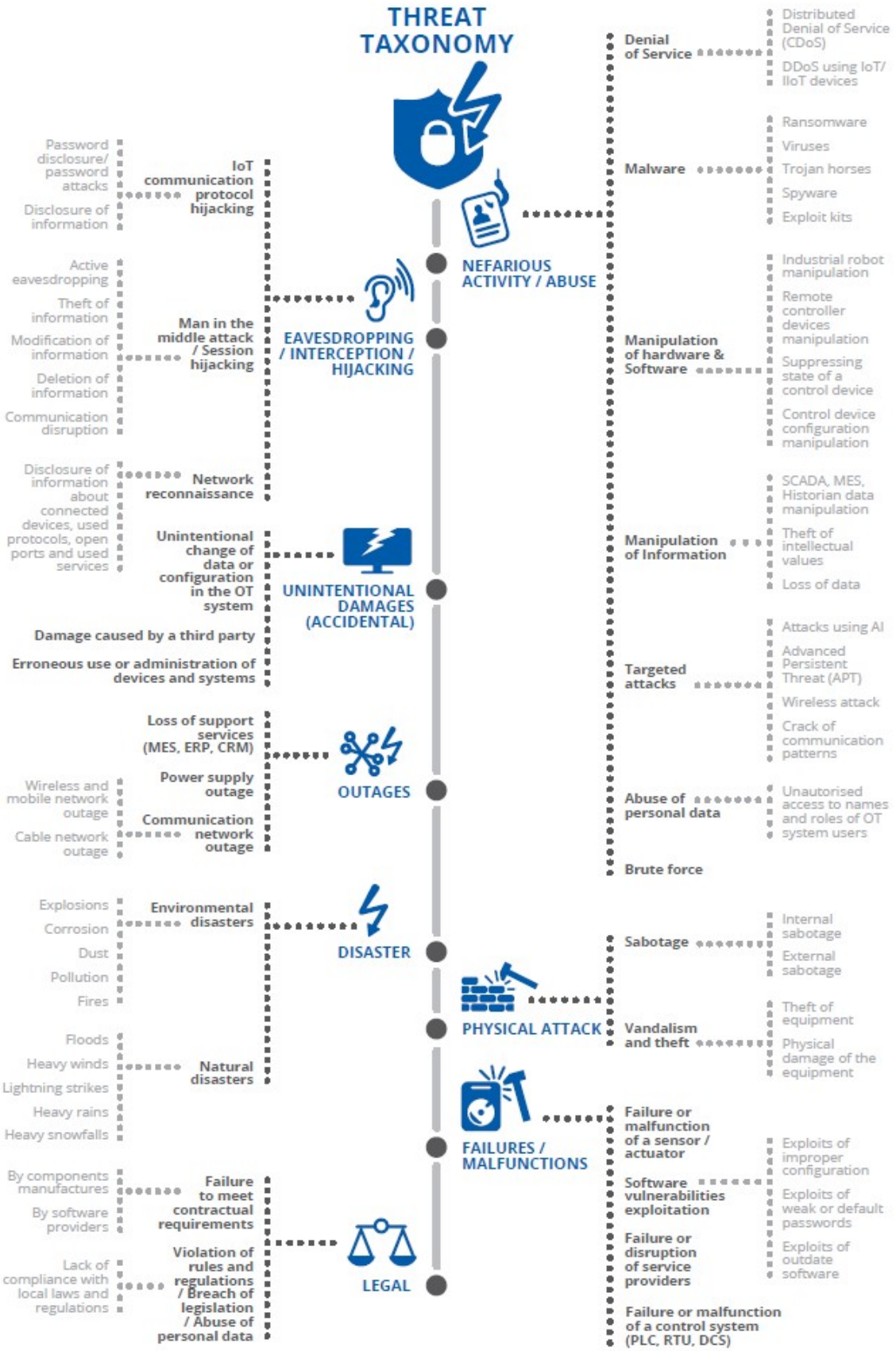
THREAT TAXONOMY
NEFARIOUS ACTIVITY / ABUSE
EAVESDROPPING / INTERCEPTION / HIJACKING
UNINTENTIONAL DAMAGES (ACCIDENTAL)
OUTAGES
DISASTER
PHYSICAL ATTACK
FAILURES / MALFUNCTIONS
LEGAL
Denial of Service
Distributed Denial of Service (CDoS)
DDoS using IoT/ IIoT devices
Malware
Ransomware
Viruses
Trojan horses
Spyware
Exploit kits
Manipulation of hardware & Software
Industrial robot manipulation
Remote controller devices manipulation
Suppressing state of a control device
Control device configuration manipulation
Manipulation of Information
SCADA, MES, Historian data manipulation
Theft of intellectual values
Loss of data
Targeted attacks
Attacks using AI
Advanced Persistent Threat (APT)
Wireless attack
Crack of communication patterns
Abuse of personal data
Unautorised access to names and roles of OT system users
Brute force
Sabotage
Internal sabotage
External sabotage
Vandalism and theft
Theft of equipment
Physical damage of the equipment
Failure or malfunction of a sensor / actuator
Software vulnerabilities exploitation
Exploits of improper configuration
Exploits of weak or default passwords
Exploits of outdate software
Failure or disruption of service providers
Failure or malfunction of a control system (PLC, RTU, DCS)
Password disclosure/ password attacks
Disclosure of information
IoT communication protocol hijacking
Active eavesdropping
Theft of information
Modification of information
Deletion of information
Communication disruption
Man in the middle attack / Session hijacking
Disclosure of information about connected devices, used protocols, open ports and used services
Network reconnaissance
Unintentional change of data or configuration in the OT system
Damage caused by a third party
Erroneous use or administration of devices and systems
Loss of support services (MES, ERP, CRM)
Wireless and mobile network outage
Power supply outage
Cable network outage
Communication network outage
Explosions
Corrosion
Dust
Pollution
Fires
Environmental disasters
Floods
Heavy winds
Lightning strikes
Heavy rains
Heavy snowfalls
Natural disasters
By components manufactures
By software providers
Failure to meet contractual requirements
Lack of compliance with local laws and regulations
Violation of rules and regulations / Breach of legislation / Abuse of personal data

Figure 8: Industry 4.0 threat taxonomy

CATEGORY	THREAT	DESCRIPTION	ASSETS AFFECTED
Nefarious activity / Abuse	Denial of Service	A Denial of Service attack can be bi-directional: It can target an IIoT system resulting in system unavailability and production disruption caused by a massive number of requests sent to the system. On the other hand, an attacker may take advantage of a large number of IIoT devices in an industrial environment and create an army of IoT botnets as a platform to attack some other system.	- IIoT end devices - ICS - ICS communication networks & components - Information - Cloud computing services - Mobile devices - Servers and systems - Software
	Malware	The penetration of malicious software in an IIoT aimed at performing unwanted and unauthorised actions, which may cause damage to an OT system, operational processes and related data. Ransomware, viruses, Trojan horses and spyware are common examples of this threat.	- IIoT end devices - ICS - Servers and systems - Real time monitoring and security tools - Information - Cloud computing services - Software
	Manipulation of hardware & software	Threat of unauthorized manipulation of devices software or applications within an OT system by an attacker. In terms of industrial IoT systems, an attacker's actions may include manipulation of an industrial robot, manipulation of remote controller devices suppressing state of a control device and modification of its configuration.	- IIoT end devices - ICS - ICS communication networks & components - Software - Real time monitoring and security tools - Advanced robotics - Personnel
	Manipulation of Information	The threat of unwanted and unauthorized data modification by an attacker. This may apply to compromising OT or production supporting systems, such as SCADA, MES, Historian and manipulation of process data. Possible consequences may include inappropriate decisions based on falsified data.	- IIoT end devices - ICS - Information - Cloud computing services - Big data analytics - Real time monitoring and security tools - Servers and systems - Software and Licenses
	Targeted attacks	The threat of a cyberattack targeting a specific organisation (or a specific person in this organisation). Such attack aims at harming an organisation possibly to take control over the system using various technical means such as compromising key devices and falsifying telemetry deceiving unaware operators. Other impacts include damage of reputation or theft of company secrets. When the target is a manufacturing company, the attacker may, for instance, attempt to steal formulas or recipes and sell them to the competition. An attacker may use Artificial Intelligence to execute a highly personalised attack, tailored to selected group or individual employees. This attack is different from wider scale attacks whose objective is to	- IIoT end devices - ICS - Information

CATEGORY	THREAT	DESCRIPTION	ASSETS AFFECTED
		infect any company that connects to a certain website prepared by an attacker or any company that uses a device or software with a certain vulnerability.	
	Abuse of personal data	The threat of compromising personal / sensitive information stored on devices or in the cloud. The attacker's goal is to gain unauthorised access to this kind of data and use it in an illicit manner. In manufacturing companies this may apply to names and roles of OT system users. Production data is not considered to be subject to privacy but it may also pose problems if it can be linked to the performance of individual employees.	- IIoT end devices - Information - Cloud computing services - Personnel
	Brute force	The threat of gaining unauthorised access to an organisation's resources (i.e. data, systems, devices, etc.) through a large number of attempts to guess the correct key or password. Industry 4.0 organisations that allow the utilisation of uncomplicated or default passwords for industrial devices and systems may be especially vulnerable to such attacks.	- IIoT end devices - ICS - Mobile devices - ICS communication networks & components - Real time monitoring and security tools
Eavesdropping / Interception / Hijacking	Man-in-the-Middle attack / Session hijacking	The threat of active eavesdropping, where messages exchanged between unaware affected parties are relayed by an attacker. The attacker may just listen to the exchanged messages (e.g. to steal a company's sensitive or confidential information) or modify or delete transmitted information, leading to communication disruption.	- Information - ICS communication networks and their components - IIoT end devices - Mobile devices
	IoT communication protocol hijacking	The threat of an attacker taking control of an existing communication session between two network components, which may lead to the disclosure of passwords and other confidential information.	- Information - ICS communication networks and their components - IIoT end devices - Decision making algorithms
	Network reconnaissance	The threat of revealing internal network information (e.g. connected devices, used protocols, open ports and used services, etc.) to an attacker who manages to scan a network passively. With this knowledge, the attacker can plan which actions to take next to compromise system operation.	- Information - IIoT end devices - ICS communication networks & components
Physical attack	Vandalism and theft	The threat of causing physical damage to the device by a saboteur who gains physical access to the OT environment - either an outsider who has managed to bypass insufficient physical security measures or an insider, e.g. a disgruntled employee who, for some reasons, wants to harm the organisation. This threat also includes theft. The necessity to replace a damaged or stolen device may result in unplanned production	- IIoT end devices - ICS - Mobile devices - ICS communication networks & components - Advanced robotics - Personnel

CATEGORY	THREAT	DESCRIPTION	ASSETS AFFECTED
		downtime related to the delivery time of spare parts.	
	Sabotage	The threat of tampering with a device by a saboteur who gains physical access to the OT environment - either an outsider who manages to bypass insufficient physical security measures or an insider, e.g. a disgruntled employee who, for some reasons, wants to harm the organisation. The attacker may take advantage of improper configuration of ports and possibility exploit open ports. The attacker may also use access to execute unauthorised operator actions.	- IIoT end devices - ICS - Mobile devices
Unintentional damages (accidental)	Unintentional change of data or configuration in the OT system	The threat of disrupting an operational process by unintentional data or configuration change in the OT system performed by an insufficiently trained employee. Even with good intentions, an unskilled employee, unaware of the consequences, may introduce improper changes to the system, especially if he or she receives higher than necessary privileges.	- IIoT end devices - ICS - ICS communication networks & components - Advanced robotics - Information - Cloud computing services - Big data analytics - Software and licenses - Servers and systems - Personnel
	Erroneous use or administration of devices and systems	The threat of disrupting an operational process or causing physical damage to the device by unintentional misuse of an IIoT/OT device by an insufficiently trained employee. Even with good intentions, an unskilled employee may inadvertently fail to use a device in accordance with the manuals and guidelines thereby disrupting the operation of the device or causing physical damage to it.	- IIoT end devices - ICS - Mobile devices - ICS communication networks & components - Advanced robotics - Information - Personnel
	Damage caused by a third party	The threat of damaging OT assets caused by a third party. In Industry 4.0, third parties may have access to the OT system, for example, for maintenance or software update purposes. If this access is not controlled in a sufficient way, security breaches of a third party organisation may affect the company that receives the service.	- IIoT end devices - ICS - ICS communication networks & components - Advanced robotics - Cloud computing services - Information
Failures / Malfunctions	Failure or malfunction of a sensor / actuator	The threat of failure or malfunction of IIoT end devices. This can occasionally happen, especially if proper maintenance and compliance with the devices' manuals and instructions during the exploitation is not ensured.	- IIoT end devices - ICS
	Failure or malfunction of a control system (PLC, RTU, DCS)	The threat of failure or malfunction of control system. This can occasionally happen, especially if proper maintenance and compliance with the devices' manuals and instructions during the exploitation is not ensured.	- IIoT end devices - ICS - ICS communication networks & components

CATEGORY	THREAT	DESCRIPTION	ASSETS AFFECTED
	Software vulnerabilities exploitation	The threat that an attacker takes advantage of IIoT end device firmware or software vulnerabilities. Such devices are often vulnerable due to lack of updates, usage of weak or default passwords and improper configuration.	- IIoT end devices - Information - Software and Licenses
	Failure or disruption of service providers	The threat of disruption of processes that rely on third party services in case of failure or malfunction of these services.	- IIoT end devices - ICS - ICS communication networks & components - Information - Cloud computing services - Big data analytics
Outages	Communication network outage	The threat of unavailability of communication links related to problems with cable, wireless or mobile network.	- ICS communication networks & components
	Power supply outage	The threat of failure or malfunction of the power supply. If no emergency power supply exists for critical systems, any power supply disruption may result in serious consequences due to a sudden shutdown of production processes.	- IIoT end devices - ICS - ICS communication networks & components - Advanced robotics
	Loss of support services (MES, ERP, CRM)	The threat of failure or malfunctions of systems supporting production or logistics, i.e. MES, ERP and CRM.	- Servers and systems
Legal	Violation of rules and regulations / Breach of legislation / Abuse of personal data	The threat of legal issues and financial losses related to personal data processing, e.g. related to the usage of IIoT end devices without complying with local laws or regulations. In operations within the European Union, these requirements are imposed on companies by the GDPR.	- IIoT end devices - Information
	Failure to meet contractual requirements	The threat of violating contractual requirements by components manufacturers and software providers in case of failure to ensure the required security measures.	- IIoT end devices - Cloud computing services - Information - ICS - Software & licences
Disaster	Natural disasters	The threat of natural disasters such as floods, lightning strikes, heavy winds, rain and snowfall, which may cause physical damage to the OT environment components.	- IIoT end devices - ICS - ICS communication networks & components - Advanced robotics - Personnel
	Environmental disasters	The threat of incidents and unfavourable conditions such as fires, pollution, dust, corrosion, explosions, which may cause physical damage to OT environment components.	- IIoT end devices - ICS - ICS communication networks & components - Advanced robotics - Personnel

Table 2: Industry 4.0 threat taxonomy

3.2 Examples of Industry 4.0/Smart Manufacturing cyber security attack scenarios

Subject matter experts have assessed attack scenarios based on these threats during the interview process to identify critical attack scenarios for Smart Manufacturing organisations. For each proposed attack scenario, experts selected their perceived criticality level (not important, of low, medium or high importance or as crucial). Analysis of the experts' answers is the source of the results presented in Table 3.

ATTACK SCENARIOS	SEVERITY
1. Against the connection between the controller (e.g. DCS, PLC) and the actuators	**High**
2. Against sensors (modification of measured values / states, their reconfiguration, etc.)	**High**
3. Against actuators (suppressing their state, modifying the configuration)	**High** - **Crucial**
4. Against the information transmitted via the network	**High** - **Crucial**
5. Against IIoT gateways	**High** - **Crucial**
6. Manipulation of remote controller devices (e.g. operating panels, smartphones)	**High**
7. Against the Safety Instrumented Systems (SIS)	**Crucial**
8. Malware	**High**
9. DDoS attack using (IoT) botnets	**Medium** - **High**
10. Stepping stones attacks (e.g. against the Cloud)	**Medium**
11. Human error-based and social engineering attacks	**High**
12. Highly personalised attacks using Artificial Intelligence Technologies	**Medium** - **High**

Table 3: IIoT attack scenarios

For each attack scenario, a brief description detailing the potential impact and related threats based on the Threats taxonomy (section 3.1) can be found below.

1. Against the connection between the controller (e.g. DCS, PLC) and the actuators

This type of attack takes place when an attacker injects and executes code or sends (manipulated) data by a compromised system using a line that is not monitored.

- Impact: Manipulation or loss of control, damage of the batch/product and infrastructure.
- Related threats: Internal and external sabotage, manipulation of hardware & software, control device configuration manipulation.

2. Against sensors (modification of measured values / states, their reconfiguration, etc.)

The measurement data is manipulated in the end devices, e.g. by breaking into the sensor and modifying its firmware or configuration, such as measurements adjustment etc.

- Impact: Making the wrong operator decisions based on manipulated data. Conducting the process based on incorrect measurements. Measurements covered by the regulations will not be evaluated properly.
- Related threats: Modification of information, sabotage, manipulation of hardware & software, manipulation of transmitted sensor data.

3. Against actuators (suppressing their state, modifying their configuration)

Manipulation of the actuators' configuration/parameters making them use wrong configurations, thresholds or data, and therefore affecting their normal behaviour by sabotaging their normal operation settings.

- Impact: It varies depending on the actuators affected. It can affect production processes.
- Related threats: Manipulation of hardware & software, failure or malfunction of a sensor / actuator, failure or malfunction of a control system (PLC, RTU, DCS).

4. Against the information being transmitted via the network

The attack aims to manipulate the data at the network layer (layer 2,3,4 model OSI). At the level of layer 5,6,7 of the OSI model, i.e. controller and control system (DCS, SCADA), data values seem to be correct. Manipulation can be detected by network layer traffic monitoring.

- Impact: It varies depending on the data manipulated. It can affect production process or cause damage to the process, e.g. manipulation of furnace temperature that can cause explosion.
- Related threats: APT, Man-in-the-Middle attack, sabotage, malware.

5. Against IIoT gateways

An attacker tries to compromise an IIoT gateway, potentially compromising the entire environment. It can be quite successful if weak/vulnerable protocols or default passwords or protocols are used. This type of attack comprises different stages/phases and it is usually launched in a covert manner. It should be noted that this type of attack should be taken into account over a device's entire lifecycle.

- Impact: An attacker gains access to the network and data including access to the devices, systems and network equipment. It can be the first stage of exploitation of the whole system and its components.
- Related threats: Password attacks, exploit kits, abuse of personal data, malware and DDoS.

6. Manipulation of remote controller devices (e.g. operating panels, smartphones)

An attacker can break into a device that is far away from the control system (distributed environment). Often such devices are intended for local control and are not monitored on an ongoing basis. The acquisition of such a device is a great threat to the possibility of infiltration of the entire network as well as causing damage to the equipment, where it will take a long time to obtain this information and could therefore magnify the damage.

- Impact: Gaining access to the system and full access to the control layer as well as engineering tools and changes. It can cause dangerous changes to the IoT environment.
- Related threats: Password attacks, software vulnerabilities exploitation, session hijacking, disclosure of information.

7. Against the Safety Instrumented Systems (SIS)

One of the most dangerous attacks is against systems that are ultimately supposed to protect the environment, human life and/or companies against large financial losses. Taking over the control system or any manipulation of this system can lead to the destruction of the installation or in the least dangerous case to the unplanned interruption of the process. An example of such attack is the recent Triton attack[43].

- Impact: Compromise of SIS, manipulation or interruption of SIS may affect many people, cause environmental issues and even extend to other systems, affecting their operations or even disabling them.
- Related threats: Malware, sabotage, remote controller devices manipulation, APT.

8. Malware

These attacks are carried out by a malicious code that spreads over the network. It can give access to the victim's data. Since these attacks are malware-based, they can be avoided by updating/patching vulnerable devices. This can also be done outside the IIoT ecosystem. The problem regarding IIoT is the difficulty to update/patch the different devices - some of them do not offer the ability to be updated or patched.

- Impact: There are many possible targets for malware within IIoT – an attacker could take control of a smart thermostat in the middle of winter and not turn on the heat, or he or she could hold power grids or hospitals systems, etc., putting people's safety at risk.
- Related threats: Exploit kits, malware, DDoS, password attacks.

9. DDoS attack with (IoT) botnets

This type of attack does not target IIoT devices themselves, but instead uses them to attack other devices, not necessarily IIoT devices. Firstly, malware automatically finds vulnerable Internet of Things devices, infecting and conscripting them into a botnet, which then can be used to mount DDoS attacks, flooding the target's servers with malicious traffic.

- Impact: The target device or service is flooded with malicious traffic, taking it down.
- Related threats: Exploit kits, DDoS and malware.

10. Stepping stones attacks (e.g. against the Cloud)

This type of attack is a common way to launch anonymous attacks. They are often used by network intruders to hide their identities, since they launch attacks not from their own computer but from intermediary hosts they have previously compromised.

- Impact: If an attacker launches a stepping stone attack, he or she could compromise a collection of hosts, using them as stepping stones to relay attack commands.
- Related threats: APT, DDoS, malware.

11. Human error-based and social engineering attacks

[43] FireEye (2017) "Attackers Deploy New ICS Attack Framework "TRITON" and Cause Operational Disruption to Critical Infrastructure": https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html

This type of attack is usually the gateway to launch other types of attacks; it is a means to an end. Attacks or human-errors are used to gain unauthorised privileged access to a system, which can lead to the installation of other malicious content or backdoors or even physical access to the devices. It is used as part of an attack, regardless of whether the target is a single system/device or a whole network or facility. It is difficult to detect these attacks due to non-technical character, and it is much easier to detect the suspicious actions in the environment based on very good awareness trainings for employees.

- Impact: If successful, the social engineering attack creates an entry point to a system or facilities, in some cases with elevated privileges. A human error-based attack could cause the system to crash or become unstable. This attack is commonly used as part of a larger, sophisticated attack, which could be simple data theft or a complex APT.
- Related threats: Erroneous use or administration of devices and systems, unintentional change of data or configuration in the OT system, physical damage to equipment, theft of intellectual values.

12. Highly personalised attacks using Artificial Intelligence Technologies (AIT)

Attacks to identify patterns for reconciliation or direct attack on IIoT systems. Their main threat is the use of often potentially insignificant information. With the application of AIT attackers can combine specific data obtained from the Internet and explicit data to find a hole in the security.

- Impact: These attacks can be very personalised and target particular people, e.g. system administrators. The development of communication throughout the IIoT ecosystem could also be a target. Such an attack may be the first attack or one of the subsequent phases of an attack.
- Related threats: Loss of data, network reconnaissance.

4. Security measures and good practices

4.1 Security Measure categorisation

Development of Security Measures for IoT in Smart Manufacturing was one of the focal points of this study. The idea behind it was to provide guidelines and recommendations for Operators, Manufacturers and Users of Industrial IoT that, if applied, can help prevent or properly respond to potential cyberattacks and ensure overall security and safety of the industrial IoT environment. As part of this study, a considerable effort was expended to identify all the relevant aspects related to this issue.

Firstly, extensive desktop research was conducted. Thorough analysis of relevant sources (listed in Annex C) allowed distinguishing frequently mentioned topics in IIoT security. These topics were then aggregated to create an initial list of security domains. Final set of domains was clarified and adapted based on the interviews conducted with the stakeholders resulting in a list of 20 domains that provide a comprehensive view of the Industry 4.0 landscape and indicate areas that require protection.

To organise the domains in a logical manner, they were classified into three main groups:

- Policies
- Organisational practices
- Technical practices

These groups provide a high-level division and are in line with the classification of the ENISA "Baseline Security Recommendations for IoT" study.

Figure 9: Good practices overview

4.2 Policies

This first group of Security Measures mostly refers to policies and procedures that should be established within organisations to help ensure a good level of cybersecurity, especially where IIoT solutions are concerned. In addition, privacy issues have been covered in the context of manufacturers who should ensure that their solutions do not violate privacy regulations, and operators, who should be sensitised to privacy related risks and made aware of how to utilise IIoT devices without exposing users' personal information.

4.2.1 Security by design

Security measures which should be applied from the very beginning of product development.

- PS-01: Treat IoT cybersecurity as a cycle, not as an end-to-end process, adopting a security by design approach from the perspective of the devices and infrastructure at every step of a smart manufacturing system development lifecycle (SDLC).
- PS-02: Address cybersecurity through embedded features of endpoints rather than only at the network level.
- PS-03: Equip, as deemed appropriate after a security and safety assessment, even the most basic connected devices holding very limited processing capabilities (e.g. actuators, converters) with identification and authentication features and ensure compatibility with IAM class solutions.
- PS-04: Perform risk and threat analysis involving cybersecurity experts from the very early stages of the design process of the device to find out which security features will be necessary.
- PS-05: In each design document include a chapter addressing the security of all the information and control systems in the industrial environment.

4.2.2 Privacy by design

Security measures related to privacy and protection of personal data. These measures should be applied from the first stages of product development.

- PS-06: Address privacy related issues based on applicable local and international regulations, such as the General Data Protection Regulation (GDPR)[44].
- PS-07: Define the scope of the data that will be processed by the device as well as the objective of this processing during the design phase, avoiding collecting or unnecessarily providing sensitive data.
- PS-08: Establish a physical location of data storage and define between which organisations data will be transferred restricting access to collected personal data only to authorised individuals.
- PS-09: Conduct a Privacy Impact Analysis (PIA) for the data that will be processed by the device.
- PS-10: Separate data that can be used to identify an individual from other information and ensure its security, e.g. through encryption of any personal data transferred within the IIoT environment.

4.2.3 Asset Management

Security measures regarding asset discovery, administration, monitoring and maintenance.

- PS-11: Utilise tools supporting asset management that are able dynamically to discover, identify and enumerate assets specific to the organisation and industrial environment.
- PS-12: Ensure that your company has a consistent and up-to-date asset inventory.

[44] General Data Protection Regulation, https://eur-lex.europa.eu/eli/reg/2016/679/2016-05-04

- PS-13: In complex industrial environments with legacy systems, use passive monitoring devices wherever feasible or precede the implementation with a testing phase if you consider active monitoring tools.
- PS-14: Use a centralised asset inventory for the entire computerised environment inside a manufacturing plant.
- PS-15: Consider secure administration of assets with management of the infrastructure and security devices via a dedicated management network.
- PS-16: Introduce a new device into the system only according to an established, accepted and communicated change management process.
- PS-17: Avoid the usage of removable devices disabling the USB ports if there is no accepted business requirement.

4.2.4 Risk and Threat Management

Security measures regarding the recommended approach to the process of risk and threat management adapted to Industry 4.0 environment.

- PS-18: Adopt an approach to risk management dedicated to Industry 4.0 and Smart Manufacturing considering new parameters, threats and attack scenarios.
- PS-19: For critical infrastructures in manufacturing environments, establish a number of risk management areas completely aligned with corporate, safety and environmental sides. Assess and characterise threats, vulnerabilities and protection measures against those risk management areas.
- PS-20: Establish risk and threat management process according to the individual needs and security requirements of your company.
- PS-21: Perform risk analysis which includes cybersecurity aspects at least annually. Also, integrate it with other processes, such as change management, incident handling and vulnerability management. The risk assessment should cover technical and procedural testing of effectiveness of the security policies and process.
- PS-22: Consider incorporating threat intelligence process within the threat management approach of your company relying on various sources of information and sharing information with trusted industry partners, ISACs and CERTs.
- PS-23: From an organisational perspective, monitor selected threats and determine their impact on systems by performing a risk analysis.
- PS-24: Regarding the Risk Management process, adopt two different approaches at the same time: top-down, addressing cybersecurity from the organisation-wide perspective, and bottom-up[45], providing a very granular and detailed view on the company's situation.

4.3 Organisational practices

Organisation principles and governance are indispensable factors that are usually critical in terms of company security. The following Security Measures explain how Smart Manufacturing and other Industry 4.0 companies should operate, what organisational rules and responsibilities they should establish and follow and what approach they should adopt towards their employees and third party contractors to handle effectively cybersecurity incidents, manage vulnerabilities and ensure security of IIoT solutions throughout their lifecycle.

[45] See more information on the top-down and bottom-up approach in Annex B:.

4.3.1 Endpoints lifecycle

Security measures related to security at different stages of product (including end devices and infrastructure) lifecycle, including the procurement process, supply chain, handover phase, exploitation and end-of-life.

- OP-01: Focus on the security of software and hardware during every stage of the endpoint lifecycle.
- OP-02: Take into account security considerations throughout the supply chain.
- OP-03: Consider security aspects during the overall procurement process defining security measures and requirements tailored to particular devices/solutions.
- OP-04: Conduct cybersecurity acceptance tests against technical specification during different validation activities or stages of the product lifecycle.
- OP-05: During the handover phase of the project implementation process, properly build and transfer all cybersecurity documentation, processes and procedures.

4.3.2 Security Architecture

Security measures regarding the architectural-based approach and establishment of security architecture.

- OP-06: To ensure security in a computerised ecosystem, adopt a holistic architectural-based approach and develop a risk-aligned security architecture based on business requirements.
- OP-07: While defining security architecture, ensure that it comprises all relevant security aspects – from organisational to physical implementation issues.
- OP-08: Within the security architecture, allocate clear roles and responsibilities for security. Clearly define and communicate roles for both OT systems and security processes.
- OP-09: Integrate compliance enforcement controls to the established Security Architecture and ensure that all products meet the requirements defined within it.

4.3.3 Incident handling

Security measures regarding the detection and response to incidents that may occur in Industry 4.0 environments.

- OP-10: Define cyber incidents relevant for your organisation based on the company's area and range of operation and classify them according to applicable standards.
- OP-11: Consider creation of a Cybersecurity Operations Centre (SOC) consisting of OT and IT cybersecurity specialists to support cybersecurity incidents dividing them into specific lines of support with appropriate roles and responsibilities.
- OP-12: Establish a process for incidents handling that consists of identification of affected assets, identification and classification of vulnerabilities, escalation and notification.
- OP-13: Detect and investigate promptly every unusual security related event.

4.3.4 Vulnerabilities management

Security measures on the vulnerability management process, related activities and vulnerability disclosure.

- OP-14: Define a comprehensive vulnerability management process within the organisation that covers utilisation of automatic and manual tools resulting from risk analysis.
- OP-15: While eliminating vulnerabilities, begin from the most critical ones taking into account criticality of assets and systems.
- OP-16: Establish a comprehensive and well-defined process for disclosure of vulnerabilities.
- OP-17: Conduct penetration tests of new IIoT solutions in a controlled environment or before / during commissioning phase, and also regularly and after an important update of the system.

- OP-18: Establish tight collaboration of OT and IT departments ensuring that their collaboration with systems business owners, decision-making authorities and other stakeholders is effective as well.

4.3.5 Training and Awareness

Security measures regarding the recommended approach related to security training and raising awareness of employees working with IIoT devices and systems.

- OP-19: Adopt a holistic approach to security training and awareness of the employees, covering employees on all levels of the organisation and addressing new Industry 4.0 related threats.
- OP-20: Provide all newly hired employees with cybersecurity training before the start of the job.
- OP-21: Ensure that security training is continuous, regular and frequently updated.
- OP-22: Train users of IIoT on the secure usage of their devices explaining to them the technologies deployed to protect IIoT devices and the ecosystem.
- OP-23: Consider communicating with other companies on a sector level including the supply chain and participate in international security infrastructures formed to enable discussion, cooperation and intelligence sharing across organisations to improve security awareness.

4.3.6 Third Party Management

Security measures related to third party management and control of third party access.

- OP-24: Strictly control access of third parties to a control or production layer only granting access on-demand, in a specified time window, for a specific purpose, and in a least privileged way.
- OP-25: Do not provide a direct connection for the vendor to a system in a control or production layer. Allow access only to the necessary selected functions and parts of the network.
- OP-26: Prompt the suppliers for information on security of their processes and commitments to their product and develop dedicated security requirements for vendors and service providers.
- OP-27: Clearly define all relevant aspects of the partnership with third parties, including security, within the appropriate agreements and contracts.

4.4 Technical practices

Apart from implementing policies and organisational practices, security also needs to be addressed through the appropriate technical capabilities of IIoT solutions and the environments where they are deployed. The Technical Security Measures listed below constitute a last piece of the puzzle enabling Industry 4.0 and Smart Manufacturing companies to improve their level of security. This section provides an overview of what technical security measures should be implemented in the devices, as well as corresponding solutions and how they should be implemented. We also discuss recommended methods for Smart Manufacturing companies to ensure resilience of their infrastructure and continuity of production processes.

4.4.1 Trust and Integrity Management

Security measures that can help ensure the integrity and trustfulness of data and devices.

- TM-01: Verify the integrity of the software before starting to run it ensuring that it comes from a reliable source (signed by the vendor) and that it is obtained in a secure manner.
- TM-02: Authorise all IIoT devices within the OT network utilising appropriate methods, e.g. digital certificates/PKI.
- TM-03: Define data exchange channels between IIoT devices in the form of a whitelist and choose only secure channels whenever possible.
- TM-04: Implement application whitelists and review the list at least annually and in case of a change to the system.

- TM-05: Ensure production data integrity through utilisation of appropriate cryptographic mechanisms and key storage tailored to processing capabilities of the implemented solutions.
- TM-06: Monitor the production data at rest and in transit to identify potential unauthorised data modification.

4.4.2 Cloud security

Security measures regarding various security aspects of cloud computing.

- TM-07: Base your decisions regarding the choice of the type of cloud on a business and privacy impact assessment taking also into consideration laws and regulations applicable to the cloud security provider's country and points of presence.
- TM-08: Include security and availability aspects in agreements with cloud security providers, if applicable.
- TM-09: In the context of cloud-based application and centralised systems, avoid single points of failure.
- TM-10: Locate critical systems and applications within the private or at least hybrid deployment models and precede implementation with a risk analysis if you consider utilisation of a public cloud.
- TM-11: To mitigate the risk related to cloud attacks, adopt a zero-knowledge security approach and protect all data within the cloud and in transfer.

4.4.3 Business continuity and recovery

Security measures regarding the development, testing and reviewing of company's plan to ensure resilience and continuity of operations in the event of security incidents.

- TM-12: Focus on ensuring resilience of Industry 4.0 systems by creating a business continuity plan (BCP) and disaster recovery plan (DRP). Test the plans periodically and adapt them according to lessons learnt from tests and actual security incidents.
- TM-13: Define critical business and technological processes and determine to what extent they influence business continuity.
- TM-14: Perform threat and risk assessment and develop written procedures on how to return to the normal – well-defined – state of operation tailored to the assessment's results.
- TM-15: Consider contingency planning preceded by risk analysis. Define contingency plans and test them executing controlled exercises. Regularly review the plan and adjust it appropriately.
- TM-16: In business continuity and recovery plans, include third party aspects.
- TM-17: Define important parameters for your company's business continuity, such as a recovery time objective (RTO), recovery point objective (RPO), maximum tolerable outage (MTO) and minimum business continuity objective (MBCO).

4.4.4 Machine-to-Machine security

Security measures regarding key storage, encryption, input validation and protection in Machine-to-Machine communications security.

- TM-18: Store long-term service-layer keys (other than public keys) in a server-HSM residing in infrastructure equipment.
- TM-19: Establish a security association with proven and secure cryptographic algorithms between the communicating entities to provide mutual authentication, integrity and confidentiality.
- TM-20: Use communication protocols that include the functionality to detect if all or part of a message is an unauthorised repeat of an earlier message.
- TM-21: Use positive / whitelist input validation to protect against cross-site scripting and command injection.

4.4.5 Data Protection

Security measures regarding protection of confidential data on various levels of an organisation and management of access to data.

- TM-22: Protect data at rest (both in volatile and non-volatile memory), in transit and in use.
- TM-23: Categorise data related to the OT system based on risk analysis, assess its criticality and define required security measures that will ensure proper level of security.
- TM-24: Grant access to certain categories of data to Third Parties with least privilege and need-to-know principles in mind and document this access.
- TM-25: For data of high confidentiality implement encryption and key management so that the information can be read only by authorised users and use data loss prevention solutions.
- TM-26: Anonymise and secure any direct or indirect personal data processed within the company, e.g. through role-based access control and encryption, having considered all relevant legal requirements.

4.4.6 Software/Firmware updates

Security measures regarding verification, testing and execution of patches.

- TM-27: Verify endpoints' software/firmware authenticity and integrity and ensure tight control over the update.
- TM-28: Verify the source of the update and execute automatic update procedures only if they are based on the risk analysis.
- TM-29: Perform deployment of patches for the IIoT devices only after proving that no negative consequences exist and test the patches in a test environment before implementing them in production.
- TM-30: Allow Third Parties to perform patching only if they guarantee and are able to prove that the patch has been tested and will not lead to any adverse consequences on the device or if they accept liability for the update according to an applicable agreement.
- TM-31: For control systems that cannot be updated, apply compensating measures.

4.4.7 Access Control

Security measures regarding the control of remote access, authentication, privileges, accounts and physical access.

- TM-32: Segregate remote access, i.e. develop a set of rules for control of the remote communication.
- TM-33: Ensure minimal level of authentication for the IIoT devices and systems and ensure that authorisation allows only for access to a certain segment of the system.
- TM-34: Implement / Use multi-factor authentication capability in the IIoT solutions.
- TM-35: Change default passwords and usernames during the commissioning / first use. Use strong passwords and require the setting of a new password after a defined period.
- TM-36: Apply the least privilege principle and ensure that in an environment with multiple users, roles are properly segregated and approved by a proper person.
- TM-37: Create individual accounts for every user whenever possible.
- TM-38: Implement / Use an account lockout functionality in IIoT devices.
- TM-39: In case of extensive and diversified networks with a large number of devices, adopt a Privilege Access Management (PAM) solution.
- TM-40: Within access control, consider aspects of physical access to buildings, areas, rooms and cabinets.

4.4.8 Networks, protocols and encryption

Security measures can help ensure security of communications through proper protocols implementation, encryption and network segmentation.

- TM-41: Secure communication channels related to IIoT solutions and encrypt communication in case of important data, where technically possible.
- TM-42: Segment industrial plants networks based on a pre-defined zoning model that includes establishment of De-Militarised Zones (DMZ) and control of traffic between zones, e.g. according to the Purdue Model.
- TM-43: Follow the micro segmentation approach, i.e. build small islands of components within a single network that communicate only with each other and control the network traffic between segments.
- TM-44: If possible, isolate safety networks from business and control networks.
- TM-45: For IIoT solutions implement proven-in-use protocols with known security capabilities, based on standards and technical recommendations. Choose solutions that use protocols that have been proved secure or tackle previous security issues (e.g. TLS 1.3) and avoid the ones with known vulnerabilities (e.g. Telnet, SNMP v1 or v2).
- TM-46: Ensure security capabilities and interoperability between protocols when implementing different protocols for various devices within the same system.
- TM-47: If possible, limit the number of protocols implemented within a given environment and disable default network services that are unused.
- TM-48: Ensure a secure environment for key exchange and key management avoiding sharing cryptographic keys across multiple devices.
- TM-49: Ensure the proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of data and information (including control messages), in transit and at rest. Ensure the proper selection of standard and strong encryption algorithms and strong keys, and disable insecure protocols. Verify the robustness of the implementation.

4.4.9 Monitoring and auditing

Security measures regarding the network traffic and availability monitoring, logs collection and reviews.

- TM-50: Implement a passive monitoring solution in the IT and OT environments to create an industrial network traffic baseline and monitor anomalies and adherence to the baseline.
- TM-51: Collect security logs and analyse them in real-time using dedicated tools, e.g. SIEM class solutions, for example within a Security Operation Centre (SOC).
- TM-52: Perform periodic reviews of network logs, access control privileges and asset configurations.
- TM-53: Monitor availability of the IIoT devices in real time, where technically feasible.

4.4.10 Configuration Management

Security measures regarding security configuration, management of changes in configuration, devices hardening and backup verification.

- TM-54: Establish baseline security configurations tailored to different types of assets.
- TM-55: Implement a mechanism and supporting tools that enable configuration management.
- TM-56: Implement and document changes in configuration according to a change management policy developed by the organisation based on risk analysis.
- TM-57: Develop a dedicated procedure for impact analysis and perform it before implementation of change to the system.
- TM-58: Harden IIoT solutions and include this in change management policy.
- TM-59: Create and apply a comprehensive backup plan, including provisions for periodic testing, tailored to different types of assets.

Glossary

APT	Advanced Persistent Threat
BCP	Business Continuity Plan
BLE	Bluetooth Low Energy
CRM	Customer Relationship Management
CERT	Computer Emergency Readiness Team
(D)DoS	(Distributed) Denial of Service
DCS	Distributed Control System
DRP	Disaster Recovery Plan
ERP	Enterprise Resource Planning
ESS	Executive Support System
HMI	Human Machine Interface
ICS	Industrial Control System
IDS	Intrusion Detection System
IP	Internet Protocol
IPS	Intrusion Prevention System
ISAC	Information Sharing and Analysis Centre
M2M	Machine to Machine
MES	Manufacturing Execution System
ML	Machine Learning
MQTT	Message Queuing Telemetry Transport
PLC	Programmable Logic Controller
QC	Quality Control
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition
SIEM	Security Information and Event Management
SIS	Safety Instrumented System
SOC	Security Operations Centre
TCP	Transmission Control Protocol
WMS	Warehouse Management System

Annex A: Relation to ENISA Baseline IoT Security Recommendations

Baseline Security Recommendations for IoT is a previous study conducted by ENISA, which aimed at developing guidelines for IoT security in critical information infrastructures. It serves as a foundation and point of reference for the current study, which focuses on the in-depth exploration of cybersecurity aspects within the specific area of IIoT and Industry 4.0.

Because this study relies on *Baseline Security Recommendations for IoT*, the adopted definitions and connection with IoT are in line with ENISA's general approach. Hereafter, the relation of IIoT to IoT is explained. ENISA defines the Internet of Things (IoT) as **"a cyber-physical ecosystem of interconnected physical and potentially virtual sensors and actuators, which enable intelligent decision making. Information lies at the heart of IoT, feeding into a continuous cycle of sensing, decision making, and actions"**.

Based on the criteria of business function, as illustrated in Figure 10, the Internet of Things can be divided into *Consumer IoT* – which includes smart connected product platforms that add value to an individual customer and, *Industrial IoT* - which corresponds to machine connectivity that increases asset performance, product quality as well as traceability and accountability.

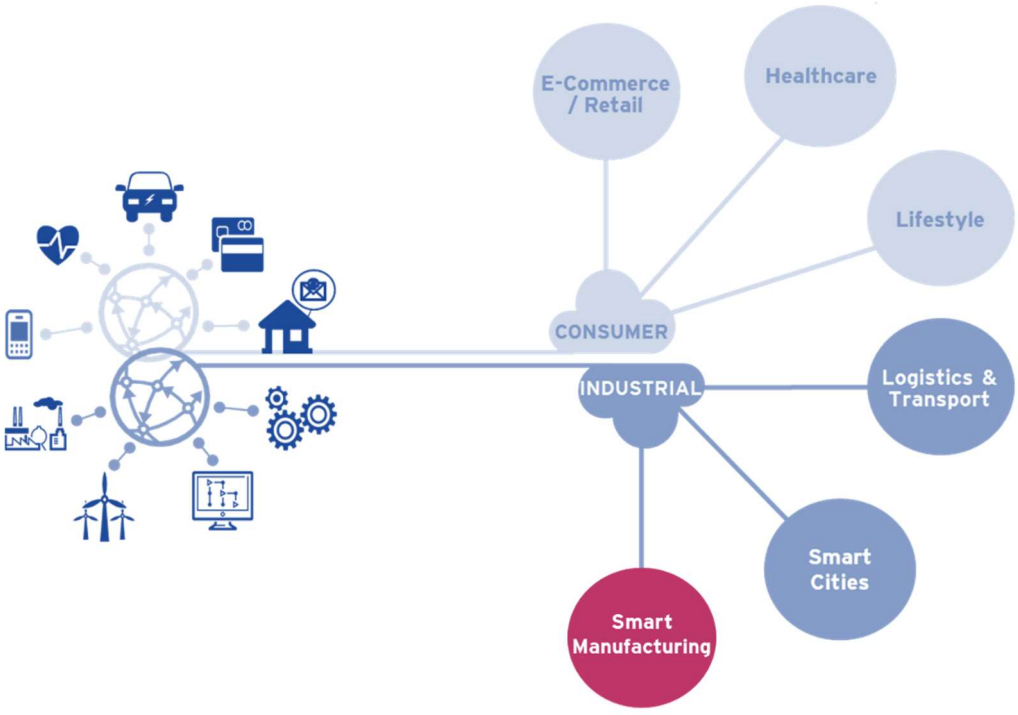

Figure 10: Consumer and Industrial IoT devices

The Industrial Internet of Things (IIoT) concept is associated with IoT focusing on digitising industries. IoT in general is a much wider concept that includes a variety of consumer products, while IIoT is specific for IoT used in OT (Operational Technology) environments. Characterised by similarities in terms of technology, IoT systems are usually more focused on usability than safety. IIoT systems however need to meet the security

requirements specific to the OT environments resulting in differences in terms of business drivers and characteristics[46], as described in Table 4.

SELECTED CHARACTERISTICS	INTERNET OF THINGS	INDUSTRIAL INTERNET OF THINGS
Focus	Protection of personal data and assets.	Prevention of process interruption, safety
Priorities	Confidentiality, Integrity, Availability	Availability, Integrity, Confidentiality
Device Failure Implications	No critical consequences	Interruption of processes, Impact on production, Potential physical threats
Reaction to threat	Possible shut down and remediation	Maintenance of operation
Upgrades and Patch Management	Possible during operation time, no reasons for significant delays.	Need to be scheduled and performed during down time, which may postpone the upgrade for a considerable amount of time.
Lifecycle of the device	Relatively frequent upgrades of equipment	Long lifespan of the devices (over 15 years[47])
Conditions of deployment	Regular	Harsh environments (temperature, vibration, etc.)

Table 4: Indicative differences in terms of selected aspects between IoT and IIoT

[46] See Industrial Internet Consortium (2016) "Industrial Internet of Things Volume G4: Security Framework": https://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB.pdf

[47] See CISCO (2017) "Cybersecurity for Industry 4.0": https://i40.hkpc.org/CyberSec/pdf/Day%201_1110-1150_Mr.%20Garrick%20Ng%20(new).pdf

Annex B: Detailed list of security measures/good practices

DOMAIN	SECURITY MEASURE/GOOD PRACTICE	THREAT GROUPS	REFERENCE
Security by design	PS-01: Treat IoT cybersecurity as a cycle - not as an end-to-end process. Take into consideration cybersecurity aspects in any activity of the development of the solution from the very beginning. Adopt security by design approach both from the devices as well as from the infrastructure perspective. In a "Security by design" concept, this relates to Continuous Security Improvement cycles at every step of a smart manufacturing system development lifecycle (Secure SDLC), that is analysis, design, implementation, testing, operations & maintenance.	• Nefarious activity / Abuse • Eavesdropping / Interception / Hijacking • Physical attack • Unintentional damages (accidental) • Failures / Malfunctions • Outages • Legal • Disaster	• Auto ISAC - Automotive Cybersecurity Best Practices - Executive Summary • Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things • GSMA (Global System for Mobile Communications) - GSMA CLP.11 IoT Security Guidelines Overview Document • Huawei - IoT Security White Paper 2017 • IIC (Industrial Internet Consortium) - IIC Endpoint Security Best Practices • IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework • IoT Alliance Australia - Internet of Things Security Guidelines v1.2 • OpenAI and others - The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation • Symantec - Smarter Security for Manufacturing in The Industry 4.0 Era: Industry 4.0 Cyber Resilience for the Manufacturing of the Future • VDC - Industry 4.0: Secure by design
Security by design	PS-02: Address cybersecurity through embedded features of endpoints rather than only on the network level, if it is possible considering constraints such as limited computing power. Embed cybersecurity in automation systems by	• Nefarious activity / Abuse • Failures / Malfunctions	• Auto ISAC - Automotive Cybersecurity Best Practices - Executive Summary • Cloud Security Alliance - Identity and Access Management for the Internet of Things - Summary Guidance • Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things • GSMA (Global System for Mobile Communications) - GSMA CLP.11 IoT Security Guidelines Overview Document • Huawei - IoT Security White Paper 2017 • IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework • Symantec - An Internet of Things Reference Architecture • VDC - Industry 4.0: Secure by design

DOMAIN	SECURITY MEASURE/GOOD PRACTICE	THREAT GROUPS	REFERENCE
	introducing fail-safe and fail-secure mechanisms from design.		
Security by design	PS-03: Equip, as deemed appropriate after a security and safety assessment, even the most basic connected devices of very limited processing capabilities (e.g. actuators, converters) with identification and authentication features and ensure compatibility with IAM class solutions. This especially applies to protection against unauthorized re-calibration or re-configuration, e.g. of measuring devices, through: a) principle of least privilege for accessing device configuration and calibration engineering tools b) authorization and authentication for engineers accessing engineering tools c) strong physical security for L0/L1 devices d) disabling of vulnerable wireless protocols e) disabling of test/debug features	• Nefarious activity / Abuse • Physical attack • Unintentional damages (accidental)	• Auto ISAC - Automotive Cybersecurity Best Practices - Executive Summary • Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things • GSMA (Global System for Mobile Communications) - GSMA CLP.13 IoT Security Guidelines for Endpoint Ecosystems • Huawei - IoT Security White Paper 2017 • IIC (Industrial Internet Consortium) - IIC Endpoint Security Best Practices • IoT Alliance Australia - Internet of Things Security Guidelines v1.2 • ISO - ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls • NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security • NIST - NISTIR 8183: Cybersecurity Framework Manufacturing Profile • NIST - Draft NISTIR 8228: Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks • Symantec - Smarter Security for Manufacturing in The Industry 4.0 Era: Industry 4.0 Cyber Resilience for the Manufacturing of the Future

DOMAIN	SECURITY MEASURE/GOOD PRACTICE	THREAT GROUPS	REFERENCE
Security by design	PS-04: Perform risk and threat analysis involving cybersecurity experts from the very early stages of the design process of the device to find out which security features will be necessary. The analysis should include possible and tailored use cases that the device may encounter. It is recommended to develop threat modelling for the IIoT systems and attack trees to consider resilience to various attack scenarios. Cybersecurity experts should be involved in the process to provide insights on threats and risks that the control systems are facing based on the experience and knowledge of current threat and risk landscape.	• Nefarious activity / Abuse • Eavesdropping / Interception / Hijacking • Physical attack • Unintentional damages (accidental) • Failures / Malfunctions • Outages • Legal • Disaster	• Auto ISAC - Automotive Cybersecurity Best Practices - Executive Summary • Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things • ETSI (European Telecommunications Standards Institute) - ETSI GR QSC 004 V1.1.1 (2017-03) Quantum Safe Cryptography; Quantum-Safe threat assessment • GSMA (Global System for Mobile Communications) - GSMA CLP.11 IoT Security Guidelines Overview Document • IIC (Industrial Internet Consortium) - IoT Security Maturity Model: Description and Intended Use • IoT Security Foundation - Connected Consumer Products. Best Practice Guidelines • ISA - ANSI/ISA-95 Part 1: Models and Terminology • NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations
Security by design	PS-05: In each design document include a chapter addressing security of all information and control systems in industrial environment. The functional and/or technical specification should at least include information on security measures used, including but not limited to:	• Nefarious activity / Abuse • Eavesdropping / Interception / Hijacking • Physical attack • Unintentional damages (accidental) • Failures / Malfunctions	• Cloud Security Alliance - Identity and Access Management for the Internet of Things - Summary Guidance • Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things • European Parliament and Council of the European Union - General Data Protection Regulation (GDPR) (EU) 2016/679 • GSMA (Global System for Mobile Communications) - GSMA CLP.11 IoT Security Guidelines Overview Document • Huawei - IoT Security White Paper 2017 • IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program • IEEE - Internet of Things (IoT) Security Best Practices • IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework • IoT Security Foundation - Connected Consumer Products. Best Practice Guidelines

DOMAIN	SECURITY MEASURE/GOOD PRACTICE	THREAT GROUPS	REFERENCE
	a) system architecture b) access control c) interfaces and communication security d) policy enforcement e) mobile security f) cloud security g) backup/disaster recovery	• Outages • Legal • Disaster	• ISO - ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls • NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations • World Economic Forum - Industrial Internet of Things: Unleashing the Potential of Connected Products and Services
Privacy by design	PS-06: Address privacy related issues based on applicable local and international regulations, such as The General Data Protection Regulation (GDPR). A compliance function in the organization should ensure that all new systems comply with regulatory requirements. This involves having written requirements in technical specifications during tendering/procurement process. Organizations should also take into account accountability aspect of privacy protection and implement measures that will enable them to demonstrate their relevant actions and their effectiveness.	• Legal	• Cloud Security Alliance - Identity and Access Management for the Internet of Things - Summary Guidance • Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things • GSMA (Global System for Mobile Communications) - GSMA CLP.11 IoT Security Guidelines Overview Document • IIC (Industrial Internet Consortium) - IoT Security Maturity Model: Description and Intended Use • IoT Security Foundation - Connected Consumer Products. Best Practice Guidelines • IoT Security Foundation - Security Challenges on the Way Towards Smart Manufacturing • ISA - ANSI/ISA-95 Part 1: Models and Terminology • LNS - Putting Industrial Cyber Security at the top of the CEO agenda • NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations • OWASP (Open Web Application Security Project) - IoT Security Guidance • VDC - Industry 4.0: Secure by design

DOMAIN	SECURITY MEASURE/GOOD PRACTICE	THREAT GROUPS	REFERENCE
Privacy by design	PS-07: Define the scope of the data that will be processed by the device as well as the objective of this processing during the design phase. Ensure that only minimal amount of personal data is collected by the device. Avoid collecting sensitive data. If you are a user of an IIoT system, do not provide any personal or sensitive information if it is not necessary.	• Nefarious activity / Abuse • Legal	• Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things • Cloud Security Alliance - Identity and Access Management for the Internet of Things - Summary Guidance • GSMA (Global System for Mobile Communications) - GSMA CLP.11 IoT Security Guidelines Overview Document • ETSI (European Telecommunications Standards Institute) - ETSI TR 103 375 SmartM2M; IoT Standards landscape and future evolutions • IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program • IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework • ISA - ANSI/ISA-95 Part 1: Models and Terminology • NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations • NIST - NISTIR 8183: Cybersecurity Framework Manufacturing Profile • OWASP (Open Web Application Security Project) - IoT Security Guidance
Privacy by design	PS-08: Establish the physical location of data stored by the organization and define between which organizations data will be transferred. Restrict access to collected personal data only to authorized individuals. Periodically revise access rights and terminate them as soon as possible after employee's change of position/leaving company.	• Nefarious activity / Abuse • Physical attack • Legal	• Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things • ENISA - Baseline Security Recommendations for IoT • GSMA (Global System for Mobile Communications) - GSMA CLP.11 IoT Security Guidelines Overview Document • IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework • IoT Alliance Australia - Internet of Things Security Guidelines v1.2 • NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations • World Economic Forum - Industrial Internet of Things: Unleashing the Potential of Connected Products and Services
Privacy by design	PS-09: Conduct a Privacy Impact Analysis (PIA) –in line with GDPR requirements- for the data that will be processed by the device. It may be integrated with the overall risk management process.	• Nefarious activity / Abuse • Legal	• Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things • ETSI (European Telecommunications Standards Institute) - ETSI TR 103 375 SmartM2M; IoT Standards landscape and future evolutions • GSMA (Global System for Mobile Communications) - GSMA CLP.11 IoT Security Guidelines Overview Document • Huawei - IoT Security White Paper 2017 • IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework • IoT Alliance Australia - Internet of Things Security Guidelines v1.2

DOMAIN	SECURITY MEASURE/GOOD PRACTICE	THREAT GROUPS	REFERENCE
			• IoT Security Foundation - Connected Consumer Products. Best Practice Guidelines
Privacy by design	PS-10: Separate data that can be used to identify an individual from other information and ensure its security (for storing and retrieving information, communication services, cryptography, etc.). Any personal data transferred within the IIoT environment shall be encrypted in the traffic.	• Nefarious activity / Abuse • Eavesdropping / Interception / Hijacking • Legal	• Cloud Security Alliance - Identity and Access Management for the Internet of Things - Summary Guidance • Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things • GSMA (Global System for Mobile Communications) - GSMA CLP.11 IoT Security Guidelines Overview Document • IEC - IEC 62443-3-3:2013 System security requirements and security levels • IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework • NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations • NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security • World Economic Forum - Industrial Internet of Things: Unleashing the Potential of Connected Products and Services
Asset Management	PS-11: Utilize tools supporting asset management (i.e. automatic asset discovery). Asset management systems should be solid and robust. Choose asset management tools that are able dynamically to discover, identify and enumerate assets specific to the organization and industrial environment (including those using proprietary protocols).	• Nefarious activity / Abuse • Eavesdropping / Interception / Hijacking • Failures / Malfunctions	• Cloud Security Alliance - Identity and Access Management for the Internet of Things - Summary Guidance • Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things • IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program • IEC - IEC 62443-3-3:2013 System security requirements and security levels • ISO - ISO/IEC 27001:2013 Information technology -- Security techniques – Information security management systems -- Requirements • ISO - ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls • NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations • NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security • NIST - NISTIR 8183: Cybersecurity Framework Manufacturing Profile • SANS Institute - The 2018 SANS Industrial IoT Security Survey: Shaping IIoT Security Concerns • SANS Institute - Vulnerability Management: Tools, Challenges and Best Practices
Asset Management	PS-12: Ensure that your company has a consistent and up-to-date asset inventory. This inventory should include, among others, IP addresses, physical location, host, current firmware / OS version, used communication	• Eavesdropping / Interception / Hijacking • Physical attack • Failures / Malfunctions	• Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things • Huawei - IoT Security White Paper 2017 • IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program • IEC - IEC 62443-3-3:2013 System security requirements and security levels • IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework • NIST - Draft NISTIR 8228: Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks

DOMAIN	SECURITY MEASURE/GOOD PRACTICE	THREAT GROUPS	REFERENCE
	protocols, etc. Asset inventory should also include gathered known vulnerabilities related to particular assets. Clearly define and communicate the responsibility for maintaining an up-to-date asset inventory to the system owner/administrator.		• NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security
Asset Management	PS-13: In complex industrial environments with legacy system asset discovery, use passive monitoring devices instead of active monitoring solutions. It is advisable to utilize passive automatic tools whenever it is feasible, as they do not disrupt systems operation. Utilization of active monitoring devices can cause adverse effects on the OT environment and disrupt the production process. If you consider implementation of active monitoring tools, precede it with a testing phase in a laboratory/testing environment to verify whether it will exert an adverse impact on the system, i.e. whether it will not considerably increase the network load.	• Nefarious activity / Abuse • Eavesdropping / Interception / Hijacking	• Cloud Security Alliance - Identity and Access Management for the Internet of Things - Summary Guidance • Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things • IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program • IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework • NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations • SANS Institute - Vulnerability Management: Tools, Challenges and Best Practices

DOMAIN	SECURITY MEASURE/GOOD PRACTICE	THREAT GROUPS	REFERENCE
Asset Management	PS-14: Use a centralized asset inventory for the entire computerized environment inside a manufacturing plant. While implementing change to a system, update the inventory. Store the latest version of software after implementation and after every change. Periodic reviews, e.g. annual, are also recommended. It is also advisable to use security tools that enable configuration management and change detection.	• Nefarious activity / Abuse • Physical attack • Unintentional damages (accidental)	• BITAG (Broadband Internet Technical Advisory Group) - Internet of Things (IoT) Security and Privacy Recommendations • Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things • IEC - IEC 62443-3-3:2013 System security requirements and security levels • IoT Alliance Australia - Internet of Things Security Guidelines v1.2 • IoT Security Foundation - Connected Consumer Products. Best Practice Guidelines • NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security
Asset Management	PS-15: Consider secure administration of assets, e.g. utilize secure/encrypted methods for administration of IoT devices (e.g. HTTPS, SSH) and associated key management. Management of the infrastructure and security devices should occur via a dedicated management network.	• Nefarious activity / Abuse	• GSMA (Global System for Mobile Communications) - GSMA CLP.13 IoT Security Guidelines for Endpoint Ecosystems • IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program • IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework • IIC (Industrial Internet Consortium) - IoT Security Maturity Model: Description and Intended Use • ISO - ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems -- Requirements • ISO - ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls • LNS - Putting Industrial Cyber Security at the top of the CEO agenda • NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations • NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security • NIST - NISTIR 8183: Cybersecurity Framework Manufacturing Profile • NIST - Draft NISTIR 8228: Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks • Siemens - Industrial Security: Applying IoT Security Controls on the Industrial Plant Floor

DOMAIN	SECURITY MEASURE/GOOD PRACTICE	THREAT GROUPS	REFERENCE
Asset Management	PS-16: Deploy a new device into the system only according to an established, accepted and communicated change management process. Do not allow for any changes unless designated approvals are received. Approved changes should be documented and the relevant documentation updated. Emergency changes may be carried out based on a verbal approval from the Change Management Committee Head and the system owner. However, post emergency, the standard procedure for documenting the change and risk analysis is to be applied.	• Nefarious activity / Abuse • Eavesdropping / Interception / Hijacking • Physical attack • Unintentional damages (accidental)	• IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program • IEC - IEC 62443-3-3:2013 System security requirements and security levels • IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework • IIC (Industrial Internet Consortium) - IoT Security Maturity Model: Description and Intended Use • ISO - ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls • LNS - Putting Industrial Cyber Security at the top of the CEO agenda • NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations • NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security • NIST - NISTIR 8183: Cybersecurity Framework Manufacturing Profile • NIST - Draft NISTIR 8228: Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks • Siemens - Industrial Security: Applying IoT Security Controls on the Industrial Plant Floor
Asset Management	PS-17: Avoid the usage of removable devices and disable USB ports (or technically restrict use of removable media on USB ports) if there is no accepted business requirement. At least scan the removable media devices using malware detection software with up-to-date definitions if they need to be connected to the environment.	• Nefarious activity / Abuse • Eavesdropping / Interception / Hijacking • Physical attack • Unintentional damages (accidental)	• Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things • GSMA (Global System for Mobile Communications) - GSMA CLP.13 IoT Security Guidelines for Endpoint Ecosystems • Huawei - IoT Security White Paper 2017 • IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework • NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations • NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security • NIST - NIST.SP 1500-202 - Framework for Cyber-Physical Systems: Volume 2, Working Group Reports • NIST - NISTIR 8183: Cybersecurity Framework Manufacturing Profile • NIST - Draft NISTIR 8228: Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks • SANS Institute - Vulnerability Management: Tools, Challenges and Best Practices

DOMAIN	SECURITY MEASURE/GOOD PRACTICE	THREAT GROUPS	REFERENCE
			• Symantec - Smarter Security for Manufacturing in The Industry 4.0 Era: Industry 4.0 Cyber Resilience for the Manufacturing of the Future
Risk and Threat Management	PS-18: Adopt an approach to risk management dedicated to Industry 4.0 and Smart Manufacturing. The approach to risk management can be qualitative or quantitative. Consider new parameters, threats and attack scenarios and cover all interdependencies between cyber-physical scenarios, cyber-physical environmental and safety during the assessment phase.	• Nefarious activity / Abuse • Eavesdropping / Interception / Hijacking • Physical attack • Unintentional damages (accidental) • Failures / Malfunctions • Outages • Legal • Disaster	• Homeland Security - Strategic Principles for Securing the Internet of Things • IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework • IIC (Industrial Internet Consortium) - IoT Security Maturity Model: Description and Intended Use • ISO - ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls • NIST - NIST SP 800 30r1 - Guide for Conducting Risk Assessments • NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations • NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security NIST - NISTIR 8183: Cybersecurity Framework Manufacturing Profile
Risk and Threat Management	PS-19: For critical infrastructures in manufacturing environments, establish a number of risk management areas completely aligned with the corporate, safety, environmental, etc. sides. Assess and characterize threats, vulnerabilities and protection measures against those risk management areas. Based on that, in case of OT and Critical Infrastructures, build a specific impact-driven risk management approach.	• Nefarious activity / Abuse • Eavesdropping / Interception / Hijacking • Physical attack • Unintentional damages (accidental) • Failures / Malfunctions • Outages • Legal • Disaster	• Auto ISAC - Automotive Cybersecurity Best Practices - Executive Summary • IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program • IEC - IEC 62443-4-1:2013 Secure product development lifecycle requirements • IIC (Industrial Internet Consortium) - IIC Endpoint Security Best Practices • IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework • IIC (Industrial Internet Consortium) - IoT Security Maturity Model: Description and Intended Use • IoT Alliance Australia - Internet of Things Security Guidelines v1.2 • LNS - Putting Industrial Cyber Security at the top of the CEO agenda • NIST - NIST SP 800 30r1 - Guide for Conducting Risk Assessments • NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security • NIST - NISTIR 8183: Cybersecurity Framework Manufacturing Profile • Symantec - Smarter Security for Manufacturing in The Industry 4.0 Era: Industry 4.0 Cyber Resilience for the Manufacturing of the Future

DOMAIN	SECURITY MEASURE/GOOD PRACTICE	THREAT GROUPS	REFERENCE
Risk and Threat Management	PS-20: Establish risk and threat management process according to the individual needs and security requirements of your company. It should consist of security risk assessment to identify critical security assets and threat modelling to identify security risks and mitigations.	• Nefarious activity / Abuse • Eavesdropping / Interception / Hijacking • Physical attack • Unintentional damages (accidental) • Failures / Malfunctions • Outages • Legal • Disaster	• IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program • IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework • IIC (Industrial Internet Consortium) - IoT Security Maturity Model: Description and Intended Use • LNS - Putting Industrial Cyber Security at the top of the CEO agenda • NIST - NIST SP 800 30r1 - Guide for Conducting Risk Assessments • NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations • NIST - NISTIR 8183: Cybersecurity Framework Manufacturing Profile • SANS Institute - Vulnerability Management: Tools, Challenges and Best Practices
Risk and Threat Management	PS-21: Perform risk analysis which includes cybersecurity aspects at least annually. Also, integrate it with other processes, such as change management, incident handling and vulnerability management in order to ensure that risk analysis is performed: - in case of introducing a new system or a significant change to an existing system, - in the event of a critical security incident, - in case of critical vulnerabilities detection,	• Nefarious activity / Abuse • Eavesdropping / Interception / Hijacking • Physical attack • Unintentional damages (accidental) • Failures / Malfunctions • Outages • Legal • Disaster	• Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things • GSMA (Global System for Mobile Communications) - GSMA CLP.11 IoT Security Guidelines Overview Document • GSMA (Global System for Mobile Communications) - GSMA CLP.14 IoT Security Guidelines for Network Operators • Huawei - IoT Security White Paper 2017 • IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program • IIC (Industrial Internet Consortium) - IoT Security Maturity Model: Description and Intended Use • IoT Alliance Australia - Internet of Things Security Guidelines v1.2 • ISO - ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems -- Requirements • NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations • NIST - NISTIR 8183: Cybersecurity Framework Manufacturing Profile • Symantec - Smarter Security for Manufacturing in The Industry 4.0 Era: Industry 4.0 Cyber Resilience for the Manufacturing of the Future

DOMAIN	SECURITY MEASURE/GOOD PRACTICE	THREAT GROUPS	REFERENCE
	- ad-hoc at the owners' request or in case of an exceptional situation. The risk assessment should cover technical and procedural testing of effectiveness of the security policies and process.		
Risk and Threat Management	PS-22: To be informed on the potential attack types and sources and new vulnerabilities which are relevant to your company's field of operation, consider incorporating threat intelligence process within the threat management approach. Rely on various sources of threat information, such as vendor's feed, specialized entities, other companies' sites and open source. Details of threat intelligence program should be tailored to an individual company's needs and may vary from the very basic methods, such as following cyber security news, to very advanced with the utilization of special tools and aforementioned sources, especially in case of large companies. Before the implementation, plan in advance how the received data will be	• Nefarious activity / Abuse • Eavesdropping / Interception / Hijacking • Physical attack • Unintentional damages (accidental) • Failures / Malfunctions • Outages • Legal • Disaster	• Auto ISAC - Automotive Cybersecurity Best Practices - Executive Summary • Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things • GSMA (Global System for Mobile Communications) - GSMA CLP.14 IoT Security Guidelines for Network Operators • Huawei - IoT Security White Paper 2017 • IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework • IIC (Industrial Internet Consortium) - IoT Security Maturity Model: Description and Intended Use • International Telecommunications Union - Security capabilities supporting safety of the Internet of things • NIST - NIST SP 800 30r1 - Guide for Conducting Risk Assessments • NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations • NIST - NISTIR 8183: Cybersecurity Framework Manufacturing Profile • Symantec - Smarter Security for Manufacturing in The Industry 4.0 Era: Industry 4.0 Cyber Resilience for the Manufacturing of the Future

DOMAIN	SECURITY MEASURE/GOOD PRACTICE	THREAT GROUPS	REFERENCE
	handled, who the responsible persons will be and what the company's goals are in terms of this programme. Incorporate information sharing with trusted industry partners, ISACs (Information Sharing and Analysis Centres) and CERTs (Computer Emergency Readiness Teams).		
Risk and Threat Management	PS-23: From an organizational perspective, monitor selected threats and determine their impact on systems by performing a risk analysis. Control threats detected through the threat intelligence process.	• Nefarious activity / Abuse • Eavesdropping / Interception / Hijacking • Physical attack • Unintentional damages (accidental) • Failures / Malfunctions • Outages • Legal • Disaster	• Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things • GSMA (Global System for Mobile Communications) - GSMA CLP.11 IoT Security Guidelines Overview Document • IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program • IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework • IIC (Industrial Internet Consortium) - IoT Security Maturity Model: Description and Intended Use • IoT Alliance Australia - Internet of Things Security Guidelines v1.2 • SANS Institute - Vulnerability Management: Tools, Challenges and Best Practices • VDC - Industry 4.0: Secure by design
Risk and Threat Management	PS-24: Regarding the Risk Management process, adopt two different approaches at the same time: - Top-down to follow a holistic approach with a well-defined	• Nefarious activity / Abuse • Eavesdropping / Interception / Hijacking • Physical attack	• Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things • IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework • IoT Alliance Australia - Internet of Things Security Guidelines v1.2 • NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations • NIST - NISTIR 8183: Cybersecurity Framework Manufacturing Profile

DOMAIN	SECURITY MEASURE/GOOD PRACTICE	THREAT GROUPS	REFERENCE
	strategy on how to address an organisation's security issues taking into account its business needs. This will help address cybersecurity from an organisation-wide perspective through uniform policies, procedures and practices. - Bottom-up to provide a very granular and detailed view on the company's situation also from the perspective of people and assets. It will make it possible to distinguish the differences between departments, personnel roles, specific processes etc. and make the organisation-wide programme adapted to particular needs specific to smaller parts of the organisation. Combine these two approaches to establish a security plan tailored to the organisation as a whole and to its specific lower level aspects.	• Unintentional damages (accidental) • Failures / Malfunctions • Outages • Legal • Disaster	
Endpoints lifecycle	OP-01: Focus on the security of software and hardware during every stage of the endpoint lifecycle. At the ordering stage, provide the vendor with defined security	• Failures / Malfunctions • Legal	• Cloud Security Alliance - Identity and Access Management for the Internet of Things - Summary Guidance • GSMA (Global System for Mobile Communications) - GSMA CLP.13 IoT Security Guidelines for Endpoint Ecosystems • IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program • IEC - IEC 62443-3-3:2013 System security requirements and security levels • International Telecommunications Union - Security capabilities supporting safety of the Internet of things • IoT Alliance Australia - Internet of Things Security Guidelines v1.2

DOMAIN	SECURITY MEASURE/GOOD PRACTICE	THREAT GROUPS	REFERENCE
	requirements, including the security capability level of individual components. For IIoT devices perform local commissioning before using the device. During the exploitation phase, ensure security of the maintenance procedures. At the decommissioning stage of the device's lifecycle, remove critical data from the device and remove the device from production in a controlled manner.		• NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations • NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security • NIST - NIST SP 800-61r2: Computer Security Incident Handling Guide - Recommendations of the National Institute of Standards and Technology • NIST - NISTIR 8183: Cybersecurity Framework Manufacturing Profile • Symantec - Smarter Security for Manufacturing in The Industry 4.0 Era: Industry 4.0 Cyber Resilience for the Manufacturing of the Future
Endpoints lifecycle	OP-02: Take into account security considerations throughout the whole supply chain. Monitor software, hardware and its components throughout the supply chain to detect and prevent unauthorized changes, e.g. introduction of malware to the software. Create unique device identity and maintain it over the lifecycle of the device. Integrity may be verified based on roots of trust, digital signatures and embedded identifiers. Ensure that the integrity of the manufactured device can be measured and attested.	• Nefarious activity / Abuse • Eavesdropping / Interception / Hijacking • Physical attack • Unintentional damages (accidental) • Failures / Malfunctions	• Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things • GSMA (Global System for Mobile Communications) - GSMA CLP.13 IoT Security Guidelines for Endpoint Ecosystems • IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program • IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework • IIC (Industrial Internet Consortium) - IoT Security Maturity Model: Description and Intended Use • IoT Security Foundation - Security Challenges on the Way Towards Smart Manufacturing • ISO - ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls • NIST - Best practices in cyber supply chain risk management. Smart Manufacturing The Future of Manufacturing and Value Chain Competitiveness • NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations • NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security • NIST - NIST SP 800-52 r1: Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations • OWASP (Open Web Application Security Project) - IoT Security Guidance

DOMAIN	SECURITY MEASURE/GOOD PRACTICE	THREAT GROUPS	REFERENCE
Endpoints lifecycle	OP-03: Consider security aspects during whole procurement process defining security measures and requirements tailored to particular devices/solutions. The security subject matter expert shall participate during offers revision. During the IIoT procurement process prepare IIoT Technical Requirements Specification document in which you will define preferred technologies and minimum cybersecurity requirements including product support and security support lifecycle aspects.	• Failures / Malfunctions • Outages • Disaster	• Elsevier - Avoiding the internet of insecure industrial things • GSMA (Global System for Mobile Communications) - GSMA CLP.13 IoT Security Guidelines for Endpoint Ecosystems • IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program • IEC - IEC 62443-3-3:2013 System security requirements and security levels • IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework • IoT Security Foundation - Security Challenges on the Way Towards Smart Manufacturing • ISO - ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems -- Requirements • ISO - ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls • NIST - Best practices in cyber supply chain risk management. Smart Manufacturing The Future of Manufacturing and Value Chain Competitiveness • NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations
Endpoints lifecycle	OP-04: Conduct cybersecurity acceptance tests against technical specification during different validation activities or stages of the product lifecycle, e.g. FAT, SAT and penetration testing before go-live.	• Failures / Malfunctions • Outages • Disaster	• IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework • ISO - ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems -- Requirements • NIST - Cybersecurity for Smart Manufacturing • NIST - NIST SP 800-52 r1: Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations • NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations • NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security
Endpoints lifecycle	OP-05: During the handover phase of the project implementation process, properly build and transfer all cybersecurity documentation,	• Nefarious activity / Abuse • Eavesdropping / Interception / Hijacking	• Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things • Huawei - IoT Security White Paper 2017 • IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program • IEC - IEC 62443-3-3:2013 System security requirements and security levels • IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework

DOMAIN	SECURITY MEASURE/GOOD PRACTICE	THREAT GROUPS	REFERENCE
	processes and procedures. Within the documentation, include a list of system and service accounts, security logs, response plans, confirmation of all software and firmware versions, up-to-date network diagrams, system architecture, risk register and security limitations. Processes should comprise maintenance routines, anti-virus deployment and assurance, patching processes and accounts' management and authentication processes. Procedures should include firewalls baseline configurations, management and monitoring, change control and fall-over testing.	• Failures / Malfunctions • Legal	• IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework • IoT Alliance Australia - Internet of Things Security Guidelines v1.2 • ISO - ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls • LNS - Putting Industrial Cyber Security at the top of the CEO agenda • MIT - Security Analysis of Zigbee • NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations • NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security • NIST - NISTIR 8183: Cybersecurity Framework Manufacturing Profile • Smart Factory Innovation Forum - Managing security, safety and privacy in Smart Factories • VDMA - Industrie 4.0 Security Guidelines Recommendations for actions • World Economic Forum - Industrial Internet of Things: Unleashing the Potential of Connected Products and Services
Security Architecture	OP-06: To ensure security in a computerized ecosystem, adopt a holistic architectural-based approach and develop a risk-aligned security architecture based on business requirements.	• Nefarious activity / Abuse • Eavesdropping / Interception / Hijacking • Physical attack • Unintentional damages (accidental) • Failures / Malfunctions • Outages • Legal	• GSMA (Global System for Mobile Communications) - GSMA CLP.11 IoT Security Guidelines Overview Document • Homeland Security - Strategic Principles for Securing the Internet of Things • Huawei - IoT Security White Paper 2017 • IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program • IEC - IEC 62443-3-3:2013 System security requirements and security levels • IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework • ISA - ANSI/ISA-95 Part 1: Models and Terminology • LNS - Putting Industrial Cyber Security at the top of the CEO agenda • VDC - Industry 4.0: Secure by design

DOMAIN	SECURITY MEASURE/GOOD PRACTICE	THREAT GROUPS	REFERENCE
		• Disaster	
Security Architecture	OP-07: While defining security architecture, ensure that it comprises all relevant security aspects – from organizational to physical implementation issues. The Security Architecture should consist of (but not be limited to) the following domains: - Security Policy & Design Principles - Security Governance & Operating Model (Organization) - Security Network Blueprint (Zoning model) - Security Technical Requirements - Security Services design - Security Procedures	• Nefarious activity / Abuse • Eavesdropping / Interception / Hijacking • Physical attack • Unintentional damages (accidental) • Failures / Malfunctions • Outages • Legal • Disaster	• Homeland Security - Strategic Principles for Securing the Internet of Things • Huawei - IoT Security White Paper 2017 • IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program • IEC - IEC 62443-3-3:2013 System security requirements and security levels • IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework • IIC (Industrial Internet Consortium) - IoT Security Maturity Model: Description and Intended Use • ISA - ANSI/ISA-95 Part 1: Models and Terminology • LNS - Putting Industrial Cyber Security at the top of the CEO agenda • VDC - Industry 4.0: Secure by design
Security Architecture	OP-08: Within the Security Architecture, allocate and distribute clear roles and responsibilities for security between IT, Engineering/Automation and Operations departments. Clearly define and communicate roles	• Nefarious activity / Abuse • Unintentional damages (accidental) • Failures / Malfunctions	• IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program • IIC (Industrial Internet Consortium) - Accompanying the Industrial Internet of Things Volume G1: Reference architecture • IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework • IIC (Industrial Internet Consortium) - IoT Security Maturity Model: Description and Intended Use • ISA - ANSI/ISA-95 Part 1: Models and Terminology • ISO - ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems -- Requirements • ISO - ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls

DOMAIN	SECURITY MEASURE/GOOD PRACTICE	THREAT GROUPS	REFERENCE
	for both OT systems and security processes. Appoint a Governance Body with a clear mandate and defined decision-making process.		• SANS Institute - Building the New Network Security Architecture for the Future
Security Architecture	OP-09: Integrate compliance enforcement controls to the established Security Architecture and ensure that all products meet the requirements defined within it.	• Failures / Malfunctions • Unintentional damages (accidental) • Legal • Disaster	• Homeland Security - Strategic Principles for Securing the Internet of Things • IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program • IIC (Industrial Internet Consortium) - Accompanying the Industrial Internet of Things Volume G1: Reference architecture • IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework • IIC (Industrial Internet Consortium) - IoT Security Maturity Model: Description and Intended Use • ISA - ANSI/ISA-95 Part 1: Models and Terminology • LNS - Putting Industrial Cyber Security at the top of the CEO agenda • SANS Institute - Building the New Network Security Architecture for the Future
Incidents handling	OP-10: Define cyber incidents relevant for your organization based on the company's area and range of operation. Classify these incidents according to applicable standards, e.g. by grouping them based on utilization of a common attack vector (removable media, email, website, etc.) or according to their impact (on organization's operation, on data, etc.).	• Nefarious activity / Abuse • Eavesdropping / Interception / Hijacking • Physical attack • Unintentional damages (accidental) • Failures / Malfunctions • Outages • Legal • Disaster	• IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program • IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework • IIC (Industrial Internet Consortium) - IoT Security Maturity Model: Description and Intended Use • LNS - Putting Industrial Cyber Security at the top of the CEO agenda • NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations • NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security • Symantec - Smarter Security for Manufacturing in The Industry 4.0 Era: Industry 4.0 Cyber Resilience for the Manufacturing of the Future
Incidents handling	OP-11: Consider creation of OT Cybersecurity Operations Centre (SOC) consisting of specialists	• Nefarious activity / Abuse	• Auto ISAC - Automotive Cybersecurity Best Practices - Executive Summary • Cloud Security Alliance - Identity and Access Management for the Internet of Things - Summary Guidance • Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things

DOMAIN	SECURITY MEASURE/GOOD PRACTICE	THREAT GROUPS	REFERENCE
	with clear roles, responsibilities and IT, OT and cybersecurity competences to support cybersecurity incidents. Divide them into specific lines of support with appropriate roles and responsibilities.	• Eavesdropping / Interception / Hijacking • Physical attack • Unintentional damages (accidental) • Failures / Malfunctions • Outages • Legal • Disaster	• ENISA - Baseline Security Recommendations for IoT • IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program • IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework • ISO - ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls • NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations • NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security • NIST - NISTIR 8183: Cybersecurity Framework Manufacturing Profile • Symantec - Smarter Security for Manufacturing in The Industry 4.0 Era: Industry 4.0 Cyber Resilience for the Manufacturing of the Future
Incidents handling	OP-12: Establish a process for incidents handling that consists of identification of affected assets, identification and classification of vulnerabilities, escalation and notification. Make a revision of the process at least annually and as soon as possible in case of a major change, e.g. change in organizational hierarchy, contracts, etc. Update the process with lessons learned from analysing and resolving security incidents. Test the process at least annually and consider different possible incidents.	• Nefarious activity / Abuse • Eavesdropping / Interception / Hijacking • Physical attack • Unintentional damages (accidental) • Failures / Malfunctions • Outages • Legal • Disaster	• Auto ISAC - Automotive Cybersecurity Best Practices - Executive Summary • Cloud Security Alliance - Identity and Access Management for the Internet of Things - Summary Guidance • IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program • IIC (Industrial Internet Consortium) - IoT Security Maturity Model: Description and Intended Use • ISO - ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls • NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations • NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security • NIST - NISTIR 8183: Cybersecurity Framework Manufacturing Profile • SANS Institute - Vulnerability Management: Tools, Challenges and Best Practices
Incidents handling	OP-13: Detect and investigate promptly every unusual security related event. Require	• Nefarious activity / Abuse	• Auto ISAC - Automotive Cybersecurity Best Practices - Executive Summary • IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program • IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework • IIC (Industrial Internet Consortium) - IoT Security Maturity Model: Description and Intended Use

DOMAIN	SECURITY MEASURE/GOOD PRACTICE	THREAT GROUPS	REFERENCE
	employees, contractors and external companies with access to the IT/OT environment to notify and report about any observed or suspected security weaknesses and anomalies.	• Eavesdropping / Interception / Hijacking • Physical attack • Unintentional damages (accidental) • Failures / Malfunctions • Outages	• ISO - ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems -- Requirements • ISO - ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls • NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations • NIST - NISTIR 8183: Cybersecurity Framework Manufacturing Profile • SANS Institute - Vulnerability Management: Tools, Challenges and Best Practices
Vulnerabilities management	OP-14: Define a comprehensive vulnerability management process within the organization that covers utilization of automatic and manual tools, e.g. passive vulnerability scanners, resulting from risk analysis. In case of active scanners implementation, precede it with a testing phase require acceptance by the system owner. Have in mind that active scanners in the OT environment may cause adverse effects to the system and disrupt the production process, especially if legacy equipment is used.	• Nefarious activity / Abuse • Eavesdropping / Interception / Hijacking • Physical attack • Unintentional damages (accidental) • Failures / Malfunctions	• Huawei - IoT Security White Paper 2017 • IIC (Industrial Internet Consortium) - IoT Security Maturity Model: Description and Intended Use • LNS - Putting Industrial Cyber Security at the top of the CEO agenda • NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations • NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security • NIST - Draft NISTIR 8228: Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks • SANS Institute - The 2018 SANS Industrial IoT Security Survey: Shaping IIoT Security Concerns • Symantec - Smarter Security for Manufacturing in The Industry 4.0 Era: Industry 4.0 Cyber Resilience for the Manufacturing of the Future
Vulnerabilities management	OP-15: While eliminating security gaps, begin from the most critical vulnerabilities taking into account the criticality of assets and systems. This	• Nefarious activity / Abuse • Eavesdropping / Interception / Hijacking	• Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things • Homeland Security - Strategic Principles for Securing the Internet of Things • NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations • NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security • NIST - NISTIR 8183: Cybersecurity Framework Manufacturing Profile • OpenAI and others - The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation

DOMAIN	SECURITY MEASURE/GOOD PRACTICE	THREAT GROUPS	REFERENCE
	process may be supported by asset inventory, if the inventory contains data related to assets and systems criticality.	• Failures / Malfunctions • Outages	• SANS Institute - Vulnerability Management: Tools, Challenges and Best Practices
Vulnerabilities Management	OP-16: Establish tight collaboration between the OT and IT department. Do not allow any individual responsible for IT security to implement any cybersecurity policies, including vulnerability management, on the OT side without the full knowledge and cooperation of the plant engineers. Ensure that IT and OT departments share their knowledge about systems operations as well as about threats.	• Failures / Malfunctions	• Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things • ENISA - Baseline Security Recommendations for IoT • GSMA (Global System for Mobile Communications) - GSMA CLP.11 IoT Security Guidelines Overview Document • Homeland Security - Strategic Principles for Securing the Internet of Things • IEEE - Internet of Things (IoT) Security Best Practices • IIC (Industrial Internet Consortium) - IoT Security Maturity Model: Description and Intended Use • IoT Alliance Australia - Internet of Things Security Guidelines v1.2 • NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations • NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security • NIST - NISTIR 8183: Cybersecurity Framework Manufacturing Profile • OpenAI and others - The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation
Vulnerabilities management	OP-17: Establish a comprehensive and well-defined process for disclosure of vulnerabilities. If you are a manufacturer, in case of vulnerability identification, inform the users on how to patch the device via dedicated emails or portals. To promote vulnerability disclosure within a company, launch a bug bounty program, i.e. reward people who identify	• Nefarious activity / Abuse • Eavesdropping / Interception / Hijacking • Failures / Malfunctions	• Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things • Huawei - IoT Security White Paper 2017 • IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program • IEEE - Internet of Things (IoT) Security Best Practices • IoT Alliance Australia - Internet of Things Security Guidelines v1.2 • LNS - Putting Industrial Cyber Security at the top of the CEO agenda • NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations • NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security • NIST - NISTIR 8183: Cybersecurity Framework Manufacturing Profile • OpenAI and others - The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation • SANS Institute - Vulnerability Management: Tools, Challenges and Best Practices

DOMAIN	SECURITY MEASURE/GOOD PRACTICE	THREAT GROUPS	REFERENCE
	significant security vulnerabilities in the implemented infrastructure or in the final product.		
Vulnerabilities management	OP-18: Conduct penetration tests of new IIoT solutions in a controlled environment (e.g. in a lab, testing environment) or before / during commissioning phase (e.g. during FAT or SAT phase). In addition, conduct penetration tests regularly, e.g. once every 2 or 3 years, and after important update of the system with acceptance of a system owner.	• Unintentional damages (accidental)	• ECSO (European Cyber Security Organisation) - INDUSTRY 4.0 AND ICS SECTOR REPORT Cyber security for the industry 4.0 and ICS sector • Cloud Security Alliance - Future Proofing the connected world • IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program • IIC (Industrial Internet Consortium) - IoT Security Maturity Model: Description and Intended Use • ISO - ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls • NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations • NIST - NISTIR 8183: Cybersecurity Framework Manufacturing Profile • Shaun Bligh-Wall - Industry 4.0: Security imperatives for IoT — converging networks, increasing risks. • Siemens - Industrial Security: Applying IoT Security Controls on the Industrial Plant Floor • VDMA - Industrie 4.0 Security Guidelines Recommendations for actions
Training and Awareness	OP-19: Adopt a holistic approach to security training and awareness among employees – ensure that it includes employees on all levels of the organization, covers new threats introduced to manufacturing environment by Industry 4.0 new capabilities and is tailored to employees' roles and responsibilities as well as to different levels of knowledge of the participants. Moreover, ensure that an additional training follows every change in employee responsibilities.	• Nefarious activity / Abuse • Unintentional damages (accidental)	• IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program • ISO - ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls • NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations • NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security • NIST - NISTIR 8183: Cybersecurity Framework Manufacturing Profile • World Economic Forum - Industrial Internet of Things: Unleashing the Potential of Connected Products and Services

DOMAIN	SECURITY MEASURE/GOOD PRACTICE	THREAT GROUPS	REFERENCE
Training and Awareness	OP-20: Provide all newly hired employees with a cybersecurity training starting the job. Provide all users of IIoT solutions with basic security awareness and training materials before they receive authorization to access the system.	• Nefarious activity / Abuse • Unintentional damages (accidental)	• Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things • IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program • IoT Security Foundation - Security Challenges on the Way Towards Smart Manufacturing • ISO - ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls • NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations • NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security • NIST - NISTIR 8183: Cybersecurity Framework Manufacturing Profile • World Economic Forum - Industrial Internet of Things: Unleashing the Potential of Connected Products and Services
Training and Awareness	OP-21: Ensure that security trainings are continuous and regular. Update the training programme after new important threats disclosure and adjust them according to the lessons learned from ongoing incident handling and recovery activities.	• Nefarious activity / Abuse • Unintentional damages (accidental)	• Cloud Security Alliance - Identity and Access Management for the Internet of Things - Summary Guidance • Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things • IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program • ISO - ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls • NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security • NIST - NISTIR 8183: Cybersecurity Framework Manufacturing Profile
Training and Awareness	OP-22: Train users of IIoT on the secure usage of their devices. During training sessions, explain to the IIoT users all the technologies deployed to protect IIoT devices and the ecosystem where the solution is deployed.	• Nefarious activity / Abuse • Unintentional damages (accidental)	• Cloud Security Alliance - Identity and Access Management for the Internet of Things - Summary Guidance • Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things • IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program • ISO - ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems -- Requirements • ISO - ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls • NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations • NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security • NIST - NISTIR 8183: Cybersecurity Framework Manufacturing Profile • OpenAI and others - The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation • OpenAI and others - The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation

DOMAIN	SECURITY MEASURE/GOOD PRACTICE	THREAT GROUPS	REFERENCE
			• World Economic Forum - Industrial Internet of Things: Unleashing the Potential of Connected Products and Services
Training and Awareness	OP-23: To improve awareness, consider communicating with other companies on a sector level including the supply chain - communication with manufacturers, components providers, software providers, service providers and customers is recommended. Also, consider participation in international security infrastructures based on trust formed to enable discussion, cooperation and intelligence sharing across organizations. Examples of such infrastructures already exist and include Plattform Industrie 4.0, Industrial Internet Consortium, Cloud Security Alliance, etc.	• Failures / Malfunctions	• Auto ISAC - Automotive Cybersecurity Best Practices - Executive Summary • Cloud Security Alliance - Identity and Access Management for the Internet of Things - Summary Guidance • ECSO (European Cyber Security Organization) - INDUSTRY 4.0 AND ICS SECTOR REPORT Cyber security for the industry 4.0 and ICS sector • IIC (Industrial Internet Consortium) - IoT Security Maturity Model: Description and Intended Use • ISO - ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls • NIST - NISTIR 8200: Interagency Report on Status of International Cybersecurity Standardization for the Internet of Things (IoT) OWASP (Open Web Application Security Project) - IoT Security Guidance
Third Party Management	OP-24: Strictly control access by Third Parties to a control or production layer, e.g. by physically plugging the RJ45 jack when the vendor has access or through timer systems. In addition, utilize dedicated registry accounts, multifactor authentication and encryption. Grant access to a control or production layer to Third Parties	• Nefarious activity / Abuse • Eavesdropping / Interception / Hijacking • Physical attack • Unintentional damages (accidental) • Failures / Malfunctions	• Auto ISAC - Automotive Cybersecurity Best Practices - Executive Summary • ECSO (European Cyber Security Organization) - INDUSTRY 4.0 AND ICS SECTOR REPORT Cyber security for the industry 4.0 and ICS sector • IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework • IIC (Industrial Internet Consortium) - IoT Security Maturity Model: Description and Intended Use • IoT Alliance Australia - Internet of Things Security Guidelines v1.2 • NIST - Framework for Cyber-Physical Systems: Volume 1, Overview • NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security • NIST - Draft NISTIR 8228: Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks

DOMAIN	SECURITY MEASURE/GOOD PRACTICE	THREAT GROUPS	REFERENCE
	only on-demand, in a specified time window, for a specific purpose, and in a least privileged way. Record and supervise sessions and do not allow for idle sessions.		
Third Party Management	OP-25: Do not provide direct connection for the vendor to a system in a control or production layer. Support security of remote access with network segmentation, VLANS configuration, implemented firewalls and network traffic filtering. Allow only for access to the selected necessary functions and parts of the network (the rule of least privilege should be in place).	• Nefarious activity / Abuse • Eavesdropping / Interception / Hijacking • Unintentional damages (accidental) • Failures / Malfunctions	• Auto ISAC - Automotive Cybersecurity Best Practices - Executive Summary • Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things • ECSO (European Cyber Security Organization) - INDUSTRY 4.0 AND ICS SECTOR REPORT Cyber security for the industry 4.0 and ICS sector • ENISA - Baseline Security Recommendations for IoT • Homeland Security - Strategic Principles for Securing the Internet of Things • IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework • IoT Security Foundation - Connected Consumer Products. Best Practice Guidelines • IoT Security Foundation - Security Challenges on the Way Towards Smart Manufacturing • NIST - NISTIR 8183: Cybersecurity Framework Manufacturing Profile • NIST - Draft NISTIR 8228: Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks • OpenAI and others - The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation • SANS Institute - The 2018 SANS Industrial IoT Security Survey: Shaping IIoT Security Concerns
Third Party Management	OP-26: Prompt suppliers for information on the security of their processes and commitments to the product they deliver, e.g. by preparing a questionnaire for the suppliers regarding their security contributions to the items they deliver and select partners taking into account its results. Develop dedicated Security Requirements for Vendors and	• Unintentional damages (accidental) • Failures / Malfunctions	• Auto ISAC - Automotive Cybersecurity Best Practices - Executive Summary • Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things • ECSO (European Cyber Security Organization) - INDUSTRY 4.0 AND ICS SECTOR REPORT Cyber security for the industry 4.0 and ICS sector • IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program • IEEE - IEEE Std 802.1X-2010 - Port-Based Network Access Control • IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework • IIC (Industrial Internet Consortium) - IoT Security Maturity Model: Description and Intended Use • ISO - ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems -- Requirements • ISO - ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls

DOMAIN	SECURITY MEASURE/GOOD PRACTICE	THREAT GROUPS	REFERENCE
	service providers. Vendors and service providers' audits should be performed before choosing an IIoT solutions provider and periodically throughout a system's lifecycle.		• NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations • NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security • NIST - Draft NISTIR 8228: Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks
Third Party Management	OP-27: Clearly define all relevant aspects of the partnership with Third Parties, including security, within the appropriate agreements and contracts (e.g. SLA - service level agreement, NDA - Non-Disclosure Agreements). Sign these agreements and contracts before the start of cooperation.	• Unintentional damages (accidental) • Failures / Malfunctions • Legal	• ENISA - Baseline Security Recommendations for IoT • Huawei - IoT Security White Paper 2017 • IEC - IEC 62443-3-3:2013 System security requirements and security levels • IIC (Industrial Internet Consortium) - Accompanying the Industrial Internet of Things Volume G1: Reference architecture • IIC (Industrial Internet Consortium) - IIC Endpoint Security Best Practices • IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework • IoT Alliance Australia - Internet of Things Security Guidelines v1.2 • IoT Security Foundation - Connected Consumer Products. Best Practice Guidelines • NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations • NIST - NISTIR 8183: Cybersecurity Framework Manufacturing Profile • NIST - Draft NISTIR 8228: Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks • VDC - Industry 4.0: Secure by design
Trust and Integrity Management	TM-01: Verify the integrity of the software before starting to run it. Verify the root of trust and secure boot mechanisms. Ensure that the software comes from a reliable source (signed by the vendor) and that it is obtained in a secure manner, e.g. downloaded via an encrypted connection. Software signing and/or checksum control should be in	• Nefarious activity / Abuse • Eavesdropping / Interception / Hijacking • Physical attack	• GSMA (Global System for Mobile Communications) - GSMA CLP.12 IoT Security Guidelines for IoT Service Ecosystems • GSMA (Global System for Mobile Communications) - GSMA CLP.13 IoT Security Guidelines for Endpoint Ecosystems • Huawei - IoT Security White Paper 2017 • IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program • IEC - IEC 62443-3-3:2013 System security requirements and security levels • IIC (Industrial Internet Consortium) - Accompanying the Industrial Internet of Things Volume G1: Reference architecture • IIC (Industrial Internet Consortium) - IIC Endpoint Security Best Practices • IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework • International Telecommunications Union - Security capabilities supporting safety of the Internet of things

DOMAIN	SECURITY MEASURE/GOOD PRACTICE	THREAT GROUPS	REFERENCE
	place to ensure that the software is legitimate.		• IoT Alliance Australia - Internet of Things Security Guidelines v1.2 • IoT Security Foundation - Connected Consumer Products. Best Practice Guidelines • NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations • NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security • NIST - NISTIR 8183: Cybersecurity Framework Manufacturing Profile • VDC - Industry 4.0: Secure by design
Trust and Integrity Management	TM-02: Authorise all IIoT devices within the OT network utilising the appropriate methods, e.g. digital certificates/PKI.	• Nefarious activity / Abuse • Eavesdropping / Interception / Hijacking	• GSMA (Global System for Mobile Communications) - GSMA CLP.12 IoT Security Guidelines for IoT Service Ecosystems • GSMA (Global System for Mobile Communications) - GSMA CLP.13 IoT Security Guidelines for Endpoint Ecosystems • Huawei - IoT Security White Paper 2017 • IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program • IIC (Industrial Internet Consortium) - Accompanying the Industrial Internet of Things Volume G1: Reference architecture • IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework • NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations • NIST - NISTIR 8183: Cybersecurity Framework Manufacturing Profile • SANS Institute - The 2018 SANS Industrial IoT Security Survey: Shaping IIoT Security Concerns
Trust and Integrity Management	TM-03: Define data exchange channels between IIoT devices and ensure that the system owner accepts them. Choose only secure channels whenever possible and implement whitelists. When sending sensitive data on mobile devices, do not use insecure channels such as SMS, MMS or notifications.	• Eavesdropping / Interception / Hijacking	• GSMA (Global System for Mobile Communications) - GSMA CLP.12 IoT Security Guidelines for IoT Service Ecosystems • GSMA (Global System for Mobile Communications) - GSMA CLP.13 IoT Security Guidelines for Endpoint Ecosystems • Huawei - IoT Security White Paper 2017 • IEC - IEC 62443-3-3:2013 System security requirements and security levels • NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations • NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security • NIST - NISTIR 8183: Cybersecurity Framework Manufacturing Profile • OWASP (Open Web Application Security Project) - Mobile Top 10 2016 • Symantec - Smarter Security for Manufacturing in The Industry 4.0 Era: Industry 4.0 Cyber Resilience for the Manufacturing of the Future

DOMAIN	SECURITY MEASURE/GOOD PRACTICE	THREAT GROUPS	REFERENCE
Trust and Integrity Management	TM-04: Implement application whitelists, i.e. lists of applications that are allowed to run in the industrial control environment and mechanisms that prevent all other applications from running. Such lists shall be provided by vendor or defined in consultation with the vendor and reviewed at least annually and in case of implementation of a change to the system. On the whitelists, all unnecessary applications and applications with known vulnerabilities shall be avoided, as they contain backdoors to the system that can be used by attackers.	• Unintentional damages (accidental) • Failures / Malfunctions • Outages	• Cloud Security Alliance - Identity and Access Management for the Internet of Things - Summary Guidance • IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program • IEC - IEC 62443-3-3:2013 System security requirements and security levels • IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework • IoT Alliance Australia - Internet of Things Security Guidelines v1.2 • NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations • NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security • Symantec - An Internet of Things Reference Architecture
Trust and Integrity Management	TM-05: Ensure production data integrity through utilisation of appropriate cryptographic mechanisms and key storage tailored to processing capabilities of the implemented solutions.	• Nefarious activity / Abuse • Eavesdropping / Interception / Hijacking	• GSMA (Global System for Mobile Communications) - GSMA CLP.12 IoT Security Guidelines for IoT Service Ecosystems • GSMA (Global System for Mobile Communications) - GSMA CLP.13 IoT Security Guidelines for Endpoint Ecosystems • Huawei - IoT Security White Paper 2017 • IEC - IEC 62443-3-3:2013 System security requirements and security levels • NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations • NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security • NIST - NISTIR 8183: Cybersecurity Framework Manufacturing Profile • Siemens - Industrial Security: Applying IoT Security Controls on the Industrial Plant Floor
Trust and Integrity Management	TM-06: Monitor the production data at rest and in transit to	• Nefarious activity / Abuse	• Cloud Security Alliance - Future Proofing the connected world • Cloud Security Alliance - Identity and Access Management for the Internet of Things - Summary Guidance

DOMAIN	SECURITY MEASURE/GOOD PRACTICE	THREAT GROUPS	REFERENCE
	identify potential unauthorised data modification.	• Eavesdropping / Interception / Hijacking	• GSMA (Global System for Mobile Communications) - GSMA CLP.12 IoT Security Guidelines for IoT Service Ecosystems • IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework • SANS Institute - Building the New Network Security Architecture for the Future
Cloud security	TM-07: Base your decisions regarding the choice of the type of cloud on a business and privacy impact assessment, i.e. a type of quantitative risk assessments, taking also into consideration laws and regulations applicable to cloud service provider's country and points of presence. Risk based approach to assess the criticality is of great importance.	• Nefarious activity / Abuse • Eavesdropping / Interception / Hijacking • Unintentional damages (accidental) • Failures / Malfunctions • Legal	• Cloud Security Alliance - Future Proofing the connected world • Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things • GSMA (Global System for Mobile Communications) - GSMA CLP.12 IoT Security Guidelines for IoT Service Ecosystems • IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework • SANS Institute - Building the New Network Security Architecture for the Future
Cloud security	TM-08: Include security and availability aspects in agreements with cloud security providers. Responsibilities for cloud security aspects shall be clearly defined and allocated to particular parties or persons. Availability of service shall be measurable and defined through specified parameters.	• Eavesdropping / Interception / Hijacking • Outages • Legal	• Federal Office for Information Security (BSI) - BSI-Standards 100-4 - Business Continuity Management • Federal Office for Information Security (BSI) - BSI-Standards 100-4 - Business Continuity Management • GSMA (Global System for Mobile Communications) - GSMA CLP.12 IoT Security Guidelines for IoT Service Ecosystems • IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework • Online Trust Alliance - IoT trust framework 2.5
Cloud security	TM-09: In cloud-based application and centralised systems, avoid single points of failure.	• Failures / Malfunctions • Outages	• ECSO (European Cyber Security Organization) - INDUSTRY 4.0 AND ICS SECTOR REPORT Cyber security for the industry 4.0 and ICS sector • IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework • NIST - NIST SP 800-146 Cloud Computing Synopsis and Recommendations • Online Trust Alliance - IoT trust framework 2.5

DOMAIN	SECURITY MEASURE/GOOD PRACTICE	THREAT GROUPS	REFERENCE
			SANS Institute - Building the New Network Security Architecture for the Future
Cloud security	TM-10: Locate critical systems and applications within the private or at least hybrid deployment models. If you consider utilisation of a public cloud, precede this decision with risk analysis.	• Nefarious activity / Abuse • Eavesdropping / Interception / Hijacking • Failures / Malfunctions	• Cloud Security Alliance - Future Proofing the connected world • Cloud Security Alliance - Identity and Access Management for the Internet of Things - Summary Guidance • Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things • GSMA (Global System for Mobile Communications) - GSMA CLP.12 IoT Security Guidelines for IoT Service Ecosystems • IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework • Online Trust Alliance - IoT trust framework 2.5
Cloud Security	TM-11: To mitigate the risk related to cloud attacks, adopt a zero-knowledge security approach. It means that providers of services should store and manage data without access to encryption keys. Protect all the data within the cloud and data in transfer. Ideally, all data should be encrypted. Application and interfaces should be secured as well.	• Nefarious activity / Abuse • Eavesdropping / Interception / Hijacking	• Federal Office for Information Security (BSI) - BSI-Standards 100-4 - Business Continuity Management • IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program • IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework • IoT Alliance Australia - Internet of Things Security Guidelines v1.2 • ISO - ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems -- Requirements • NIST - NIST Advanced Manufacturing Series 300-1 Reference Architecture for Smart Manufacturing Part 1: Functional Models • NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations • NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security • NIST - NISTIR 8183: Cybersecurity Framework Manufacturing Profile
Business continuity and recovery	TM-12: Focus on ensuring the resilience of Industry 4.0 systems by creating a business continuity plan (BCP) and disaster recovery plan (DRP). Ensure continuity of the systems operation even in the event of security incidents. Perform periodic testing of the plans and adapt them according	• Nefarious activity / Abuse • Eavesdropping / Interception / Hijacking • Physical attack • Unintentional damages (accidental)	• Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things • Federal Office for Information Security (BSI) - BSI-Standards 100-4 - Business Continuity Management • Homeland Security - Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies • IEC - IEC 62443-3-3:2013 System security requirements and security levels • IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework • IIC (Industrial Internet Consortium) - IoT Security Maturity Model: Description and Intended Use • NIST - NIST Advanced Manufacturing Series 300-1 Reference Architecture for Smart Manufacturing Part 1: Functional Models

DOMAIN	SECURITY MEASURE/GOOD PRACTICE	THREAT GROUPS	REFERENCE
	to lessons learnt from tests and actual security incidents.	• Failures / Malfunctions • Outages • Legal • Disaster	• NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations • NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security • NIST - NISTIR 8183: Cybersecurity Framework Manufacturing Profile • Symantec - Smarter Security for Manufacturing in The Industry 4.0 Era: Industry 4.0 Cyber Resilience for the Manufacturing of the Future
Business continuity and recovery	TM-13: Define critical business and technological processes and determine to what extent they influence business continuity.	• Nefarious activity / Abuse • Eavesdropping / Interception / Hijacking • Physical attack • Unintentional damages (accidental) • Failures / Malfunctions • Outages • Legal • Disaster	• ETSI (European Telecommunications Standards Institute) - ETSI GR QSC 004 V1.1.1 (2017-03) Quantum Safe Cryptography; Quantum-Safe threat assessment • Federal Office for Information Security (BSI) - BSI-Standards 100-4 - Business Continuity Management • Huawei - IoT Security White Paper 2017 • IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program • IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework • ISO - ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems -- Requirements • ISO - ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls • NIST - NIST Advanced Manufacturing Series 300-1 Reference Architecture for Smart Manufacturing Part 1: Functional Models • NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations • NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security • NIST - NISTIR 8183: Cybersecurity Framework Manufacturing Profile
Business continuity and recovery	TM-14: Develop written procedures on how to return to the normal – well-defined – state of operation. Before establishing these procedures, perform threat and risk assessment and tailor the procedures to the assessment's results. Within the procedures, define roles and responsibilities for particular required actions. Distribute copies of the incident response	• Nefarious activity / Abuse • Eavesdropping / Interception / Hijacking • Physical attack • Unintentional damages (accidental) • Failures / Malfunctions • Outages	• Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things • IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program • IEC - IEC 62443-3-3:2013 System security requirements and security levels • IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework • NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations • NIST - NISTIR 8183: Cybersecurity Framework Manufacturing Profile • Symantec - Smarter Security for Manufacturing in The Industry 4.0 Era: Industry 4.0 Cyber Resilience for the Manufacturing of the Future

DOMAIN	SECURITY MEASURE/GOOD PRACTICE	THREAT GROUPS	REFERENCE
	plan to active incident response personnel.	• Legal • Disaster	
Business continuity and recovery	TM-15: Consider contingency planning preceded by a risk analysis. Define contingency plans and test them executing controlled exercises. Regularly review the plan (at least annually and in case of a major change) and adjust it appropriately. While preparing a contingency plan, consider both major disasters and smaller scale events caused by cyber incidents, which may disrupt normal operation of the company. Define responsible persons for every stage of the plan and establish a reporting process. Keep in mind that the plan needs to be simple and ensure employees' awareness through adequate training.	• Nefarious activity / Abuse • Eavesdropping / Interception / Hijacking • Physical attack • Unintentional damages (accidental) • Failures / Malfunctions • Outages • Legal • Disaster	• Federal Office for Information Security (BSI) - BSI-Standards 100-4 - Business Continuity Management • ISO - ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls • NIST - NIST Advanced Manufacturing Series 300-1 Reference Architecture for Smart Manufacturing Part 1: Functional Models • NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations • NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security • The Cavalry - Hippocratic Oath for Connected Medical Devices
Business continuity and recovery	TM-16: In business continuity and recovery plans, include Third Parties aspects. Appropriate Third Party management and control over its involvement is essential for ensuring company's continuity of operations.	• Unintentional damages (accidental) • Failures / Malfunctions	• Center for Internet Security (CIS) - Critical Security Controls • Federal Office for Information Security (BSI) - BSI-Standards 100-4 - Business Continuity Management • IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program • NIST - NIST Advanced Manufacturing Series 300-1 Reference Architecture for Smart Manufacturing Part 1: Functional Models • NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations • NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security • NIST - NISTIR 8183: Cybersecurity Framework Manufacturing Profile

DOMAIN	SECURITY MEASURE/GOOD PRACTICE	THREAT GROUPS	REFERENCE
Business continuity and recovery	TM-17: Define important parameters for business continuity of your company, such as the recovery time objective (RTO), recovery point objective (RPO), maximum tolerable outage (MTO) and minimum business continuity objective (MBCO).	• Nefarious activity / Abuse • Eavesdropping / Interception / Hijacking • Physical attack • Unintentional damages (accidental) • Failures / Malfunctions • Outages • Legal • Disaster	• IEC - IEC 62443-3-3:2013 System security requirements and security levels • IIC (Industrial Internet Consortium) - IIC Endpoint Security Best Practices • IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework • Infineon - Hardware-based solutions secure machine identities in smart factories • IoT Security Foundation - Connected Consumer Products. Best Practice Guidelines • oneM2M - Standards for M2M and the Internet of Things - TR 0008 Security V2.0.0 - Security. Technical Report
Machine-to-Machine security	TM-18: Store long-term service-layer keys (other than public keys) in a server-HSM residing in infrastructure equipment. The HSM containing the M2M long-term service keys should be bound to the M2M Device or M2M Gateway, using physical and/or logical means. HSM/server-HSM should not reveal the value of the stored secret keys (other than public keys), even to a management system or to an authorised representative of the M2M System Operator, such as a System Administrator.	• Eavesdropping / Interception / Hijacking	• Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things • GSMA (Global System for Mobile Communications) - GSMA CLP.12 IoT Security Guidelines for IoT Service Ecosystems • Huawei - IoT Security White Paper 2017 • IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework • IoT Alliance Australia - Internet of Things Security Guidelines v1.2 • IoT Security Foundation - Connected Consumer Products. Best Practice Guidelines • NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations • NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security • NIST - NIST SP 800-52 r1: Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations • oneM2M - Standards for M2M and the Internet of Things - TR 0008 Security V2.0.0 - Security. Technical Report • Symantec - An Internet of Things Reference Architecture

DOMAIN	SECURITY MEASURE/GOOD PRACTICE	THREAT GROUPS	REFERENCE
Machine-to-Machine security	TM-19: Establish a security association with proven and secure cryptographic algorithms between the communicating entities to provide mutual authentication, integrity and confidentiality.	• Eavesdropping / Interception / Hijacking	• IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program • IEC - IEC 62443-3-3:2013 System security requirements and security levels • IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework • IIC (Industrial Internet Consortium) - IoT Security Maturity Model: Description and Intended Use • IoT Alliance Australia - Internet of Things Security Guidelines v1.2 • ISO - ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls • NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations • NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security • NIST - NIST SP 800-52 r1: Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations • oneM2M - Standards for M2M and the Internet of Things - TR 0008 Security V2.0.0 - Security. Technical Report
Machine-to-Machine security	TM-20: Use communication protocols that include the functionality to detect if all or part of a message is an unauthorised repeat of an earlier message.	• Nefarious activity / Abuse • Eavesdropping / Interception / Hijacking	• ENISA - Baseline Security Recommendations for IoT • GSMA (Global System for Mobile Communications) - GSMA CLP.12 IoT Security Guidelines for IoT Service Ecosystems • GSMA (Global System for Mobile Communications) - GSMA CLP.13 IoT Security Guidelines for Endpoint Ecosystems • Huawei - IoT Security White Paper 2017 • IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program • IEC - IEC 62443-3-3:2013 System security requirements and security levels • IoT Alliance Australia - Internet of Things Security Guidelines v1.2 • NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security • Siemens - Industrial Security: Applying IoT Security Controls on the Industrial Plant Floor
Machine-to-Machine security	TM-21: Use positive/whitelist input validation to protect against cross site scripting and command injection, i.e. decode any encoded input and then validate the length, characters,	• Nefarious activity / Abuse • Eavesdropping / Interception / Hijacking • Failures / Malfunctions	• Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things • ENISA - Baseline Security Recommendations for IoT • GSMA (Global System for Mobile Communications) - GSMA CLP.12 IoT Security Guidelines for IoT Service Ecosystems • Huawei - IoT Security White Paper 2017 • IEC - IEC 62443-3-3:2013 System security requirements and security levels • IIC (Industrial Internet Consortium) - IIC Endpoint Security Best Practices • IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework

DOMAIN	SECURITY MEASURE/GOOD PRACTICE	THREAT GROUPS	REFERENCE
	and format on that data before accepting the input.		• IoT Alliance Australia - Internet of Things Security Guidelines v1.2 • NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations • NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security • NIST - NISTIR 8183: Cybersecurity Framework Manufacturing Profile • OWASP (Open Web Application Security Project) - IoT Security Guidance
Data protection	TM-22: Protect data at rest (both in volatile and non-volatile memory), in transit and in use. For data at rest, it can be achieved through role-based access control and requirement of authentication. For critical data, implementation of encryption algorithms is advisable. Take special care not to store any sensitive data on SD cards without proper security measures such as access control lists. In terms of data in transit, it is advisable to ensure that traffic between system components is encrypted, e.g. utilising an SSL/VPN Tunnel or TSL. To protect data in use, implement access control and authentication mechanisms.	• Nefarious activity / Abuse • Eavesdropping / Interception / Hijacking	• Cloud Security Alliance - Identity and Access Management for the Internet of Things - Summary Guidance • Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things • GSMA (Global System for Mobile Communications) - GSMA CLP.12 IoT Security Guidelines for IoT Service Ecosystems • GSMA (Global System for Mobile Communications) - GSMA CLP.13 IoT Security Guidelines for Endpoint Ecosystems • IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program • IIC (Industrial Internet Consortium) - IoT Security Maturity Model: Description and Intended Use • IOActive, Embedi - SCADA And Mobile Security In The Internet Of Things Era • IoT Alliance Australia - Internet of Things Security Guidelines v1.2 • IoT Security Foundation - Connected Consumer Products. Best Practice Guidelines • ISO - ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems -- Requirements • ISO - ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls • NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security • NIST - Draft NISTIR 8228: Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks
Data protection	TM-23: Categorise data related to the OT system based on risk analysis. Take into account	• Nefarious activity / Abuse	• Cloud Security Alliance - Identity and Access Management for the Internet of Things - Summary Guidance • Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things • IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework • IIC (Industrial Internet Consortium) - IoT Security Maturity Model: Description and Intended Use

DOMAIN	SECURITY MEASURE/GOOD PRACTICE	THREAT GROUPS	REFERENCE
	production, device and user information. Defined categories may include for example production schedule data, customer data, R&D data, asset management data, defect and quality data, production line data, etc. For each category, assess the criticality of data and define required security measures that will ensure proper level of security. Recipes for instance are considered critical for manufacturing companies and shall be therefore protected with the most advanced measures, e.g. encryption.		• IoT Alliance Australia - Internet of Things Security Guidelines v1.2 • ISO - ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations
Data protection	TM-24: Grant access to certain categories of data to Third Parties with least privilege and need-to-know principles in mind and document this access, i.e. ensure that Third Parties have access only to the necessary data and have minimal privileges, e.g. read only access to data that they should not be alter.	• Nefarious activity / Abuse • Eavesdropping / Interception / Hijacking • Unintentional damages (accidental)	• Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things • GSMA (Global System for Mobile Communications) - GSMA CLP.12 IoT Security Guidelines for IoT Service Ecosystems • Huawei - IoT Security White Paper 2017 • IEC - IEC 62443-3-3:2013 System security requirements and security levels • IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework • IIC (Industrial Internet Consortium) - IoT Security Maturity Model: Description and Intended Use • IoT Alliance Australia - Internet of Things Security Guidelines v1.2 • IoT Security Foundation - Connected Consumer Products. Best Practice Guidelines • ISO - ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls • NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations • NIST - NISTIR 8183: Cybersecurity Framework Manufacturing Profile • NIST - Draft NISTIR 8228: Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks

DOMAIN	SECURITY MEASURE/GOOD PRACTICE	THREAT GROUPS	REFERENCE
			• Symantec - Smarter Security for Manufacturing in The Industry 4.0 Era: Industry 4.0 Cyber Resilience for the Manufacturing of the Future
Data protection	TM-25: For data of high confidentiality, implement encryption and key management so that the information can be read only by authorised users. In addition, use data loss prevention solutions.	• Nefarious activity / Abuse • Eavesdropping / Interception / Hijacking • Unintentional damages (accidental)	• Cloud Security Alliance - Identity and Access Management for the Internet of Things - Summary Guidance • Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things • Huawei - IoT Security White Paper 2017 • IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program • IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework • IoT Alliance Australia - Internet of Things Security Guidelines v1.2 • IoT Security Foundation - Connected Consumer Products. Best Practice Guidelines • OWASP (Open Web Application Security Project) - IoT Security Guidance
Data protection	TM-26: Anonymise any direct or indirect personal data processed within the company system (e.g. names of system operators and information on their performance), having considered all relevant legal requirements, or properly secure it, e.g. through role-based access control and encryption.	• Nefarious activity / Abuse • Eavesdropping / Interception / Hijacking	• Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things • GSMA (Global System for Mobile Communications) - GSMA CLP.11 IoT Security Guidelines Overview Document • Homeland Security - Strategic Principles for Securing the Internet of Things • IIC (Industrial Internet Consortium) - IIC Endpoint Security Best Practices • IIC (Industrial Internet Consortium) - IoT Security Maturity Model: Description and Intended Use • IoT Alliance Australia - Internet of Things Security Guidelines v1.2 • IoT Security Foundation - Connected Consumer Products. Best Practice Guidelines • ISO - ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls • NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security • NIST - NISTIR 8183: Cybersecurity Framework Manufacturing Profile • OWASP (Open Web Application Security Project) - IoT Security Guidance • Siemens - Industrial Security: Applying IoT Security Controls on the Industrial Plant Floor • The Cavalry - Hippocratic Oath for Connected Medical Devices
Software/Firmware updates	TM-27: Verify endpoints' software/firmware authenticity and integrity and ensure tight control over the update. Signing code updates (to be able to	• Nefarious activity / Abuse	• Cloud Security Alliance - Identity and Access Management for the Internet of Things - Summary Guidance • GSMA (Global System for Mobile Communications) - GSMA CLP.13 IoT Security Guidelines for Endpoint Ecosystems • Homeland Security - Strategic Principles for Securing the Internet of Things • IIC (Industrial Internet Consortium) - IIC Endpoint Security Best Practices

DOMAIN	SECURITY MEASURE/GOOD PRACTICE	THREAT GROUPS	REFERENCE
	authenticate the code before it is loaded) and maintaining the authenticity is advisable.	• Eavesdropping / Interception / Hijacking • Physical attack • Failures / Malfunctions	• IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework • ISO - ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls • NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security • Siemens - Industrial Security: Applying IoT Security Controls on the Industrial Plant Floor The Cavalry - Hippocratic Oath for Connected Medical Devices
Software/Firmware updates	TM-28: Execute automatic update procedures only if they are based on the risk analysis and if the devices for which the automatic update can be allowed are identified. Verify the source of the update.	• Nefarious activity / Abuse • Physical attack	• Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things • Homeland Security - Strategic Principles for Securing the Internet of Things • IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework • IoT Security Foundation - Connected Consumer Products. Best Practice Guidelines • ISO - ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls • NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations • NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security The Cavalry - Hippocratic Oath for Connected Medical Devices
Software/Firmware updates	TM-29: Perform deployment of patches for the IIoT devices only after proving that no negative consequences exist. Test the patches in a test environment before implementing them in production. If this is not possible, begin with deploying patches only on a segment of a system, ensuring that other zones will continue to operate normally in case a patch exerts any negative impact on a chosen segment.	• Failures / Malfunctions	• Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things • IIC (Industrial Internet Consortium) - IoT Security Maturity Model: Description and Intended Use • IoT Security Foundation - Connected Consumer Products. Best Practice Guidelines • ISO - ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls • NIST - Framework for Improving Critical Infrastructure Cybersecurity V1.1 NIST - NIST SP 800-52 r1: Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations
Software/Firmware updates	TM-30: Allow Third Parties to perform patching only if they guarantee and are able to prove	• Unintentional damages (accidental)	• IoT Security Foundation - Connected Consumer Products. Best Practice Guidelines • IoT Security Foundation - Establishing Principles for IoT Security • NIST - Framework for Improving Critical Infrastructure Cybersecurity V1.1

DOMAIN	SECURITY MEASURE/GOOD PRACTICE	THREAT GROUPS	REFERENCE
	that the patch has been tested and will not have any negative consequences on the device or if the Third Party assumes the liability for the update according to an applicable agreement. In addition, require Third Parties to report any executed actions related to the patching process and inform about them in advance. Update procedures shall be documented, known and controlled by the organisation.	• Failures / Malfunctions	• The Cavalry - Hippocratic Oath for Connected Medical Devices
Software/Firmware updates	TM-31: For control systems which cannot be updated (e.g. legacy systems), apply compensating measures, such as network segmentation, micro segmentation, system relocation or additional real-time monitoring tools. Perform risk analysis to determine if it is possible and sufficient to improve security of existing system or if the replacement of the system is necessary.	• Nefarious activity / Abuse • Eavesdropping / Interception / Hijacking • Physical attack • Unintentional damages (accidental) • Failures / Malfunctions • Outages • Legal • Disaster	• GSMA (Global System for Mobile Communications) - GSMA CLP.13 IoT Security Guidelines for Endpoint Ecosystems • IIC (Industrial Internet Consortium) - IIC Endpoint Security Best Practices • IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework • IoT Security Foundation - Connected Consumer Products. Best Practice Guidelines • NIST - Framework for Improving Critical Infrastructure Cybersecurity V1.1 • NIST - NIST SP 800-52 r1: Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations
Access Control	TM-32: Segregate remote access, i.e. develop a set of rules for control of the remote communication. Limit remote	• Nefarious activity / Abuse	• GSMA (Global System for Mobile Communications) - GSMA CLP.12 IoT Security Guidelines for IoT Service Ecosystems • GSMA (Global System for Mobile Communications) - GSMA CLP.13 IoT Security Guidelines for Endpoint Ecosystems

DOMAIN	SECURITY MEASURE/GOOD PRACTICE	THREAT GROUPS	REFERENCE
	access only to the required systems and monitor it. Ensure full traceability and accountability of the users.	• Eavesdropping / Interception / Hijacking • Unintentional damages (accidental) • Failures / Malfunctions	• IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program • IEC - IEC 62443-3-3:2013 System security requirements and security levels • IIC (Industrial Internet Consortium) - IIC Endpoint Security Best Practices • International Telecommunications Union - Security capabilities supporting safety of the Internet of things • IoT Alliance Australia - Internet of Things Security Guidelines v1.2 • ISO - ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems -- Requirements • ISO - ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls • NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations • NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security • NIST - NISTIR 8183: Cybersecurity Framework Manufacturing Profile • NIST - Draft NISTIR 8228: Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks • OWASP (Open Web Application Security Project) - IoT Security Guidance • VDMA - Smart Manufacturing General security and privacy principles to ensure a Trusted IoT environment
Access Control	TM-33: Ensure minimal level of authentication security for the IIoT devices and systems. In a segmented network/system, ensure that authorisation only allows for access to a certain segment and no other parts of the system.	• Nefarious activity / Abuse • Eavesdropping / Interception / Hijacking • Unintentional damages (accidental)	• Cloud Security Alliance - Identity and Access Management for the Internet of Things - Summary Guidance • Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things • GSMA (Global System for Mobile Communications) - GSMA CLP.12 IoT Security Guidelines for IoT Service Ecosystems • GSMA (Global System for Mobile Communications) - GSMA CLP.13 IoT Security Guidelines for Endpoint Ecosystems • Huawei - IoT Security White Paper 2017 • IEC - IEC 62443-3-3:2013 System security requirements and security levels • IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework • IIC (Industrial Internet Consortium) - IoT Security Maturity Model: Description and Intended Use • IoT Alliance Australia - Internet of Things Security Guidelines v1.2 • IoT Security Foundation - Connected Consumer Products. Best Practice Guidelines • ISO - ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls • OWASP (Open Web Application Security Project) - IoT Security Guidance

DOMAIN	SECURITY MEASURE/GOOD PRACTICE	THREAT GROUPS	REFERENCE
			• VDC - Industry 4.0: Secure by design
Access Control	TM-34: As an IIoT solutions vendor, implement multi-factor authentication capability (e.g. Apple Touch ID, security tokens). As a user of such solutions, utilise multi-factor system authentication.	• Nefarious activity / Abuse • Eavesdropping / Interception / Hijacking • Physical attack	• Cloud Security Alliance - Identity and Access Management for the Internet of Things - Summary Guidance • ENISA - Baseline Security Recommendations for IoT • GSMA (Global System for Mobile Communications) - GSMA CLP.12 IoT Security Guidelines for IoT Service Ecosystems • GSMA (Global System for Mobile Communications) - GSMA CLP.13 IoT Security Guidelines for Endpoint Ecosystems • IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program • IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework • IoT Security Foundation - Connected Consumer Products. Best Practice Guidelines • NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations • OpenAI and others - The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation • OWASP (Open Web Application Security Project) - IoT Security Guidance
Access Control	TM-35: Change default passwords and usernames during commissioning/first use. Use strong passwords aligned to internal password complexity policy and require setting of a new password after a defined period. Device manufacturers and cloud services providers should give these options to users. Have in mind that passwords for industrial control systems should not be too complex to ensure immediate access when needed. When complex passwords are used, organisations should ensure that the frequency of password change is not too high.	• Nefarious activity / Abuse • Eavesdropping / Interception / Hijacking • Physical attack	• Cloud Security Alliance - Identity and Access Management for the Internet of Things - Summary Guidance • Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things • ENISA - Baseline Security Recommendations for IoT • GSMA (Global System for Mobile Communications) - GSMA CLP.12 IoT Security Guidelines for IoT Service Ecosystems • GSMA (Global System for Mobile Communications) - GSMA CLP.13 IoT Security Guidelines for Endpoint Ecosystems • IEC - IEC 62443-3-3:2013 System security requirements and security levels • IoT Alliance Australia - Internet of Things Security Guidelines v1.2 • IoT Security Foundation - Connected Consumer Products. Best Practice Guidelines • ISO - ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls • NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations • NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security • OWASP (Open Web Application Security Project) - IoT Security Guidance • SANS Institute - The 2018 SANS Industrial IoT Security Survey: Shaping IIoT Security Concerns

DOMAIN	SECURITY MEASURE/GOOD PRACTICE	THREAT GROUPS	REFERENCE
	Ensure that secure passwords recovery mechanisms are in place.		
Access Control	TM-36: Apply the least privilege principle when setting user privileges. Ensure that in an environment with multiple users, roles are properly segregated and approved by the right person.	• Nefarious activity / Abuse • Eavesdropping / Interception / Hijacking • Physical attack • Unintentional damages (accidental)	• ENISA - Baseline Security Recommendations for IoT • GSMA (Global System for Mobile Communications) - GSMA CLP.12 IoT Security Guidelines for IoT Service Ecosystems • GSMA (Global System for Mobile Communications) - GSMA CLP.13 IoT Security Guidelines for Endpoint Ecosystems • Huawei - IoT Security White Paper 2017 • IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program • IEC - IEC 62443-3-3:2013 System security requirements and security levels • IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework • ISO - ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls • NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations • NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security • NIST - Draft NISTIR 8228: Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks • OWASP (Open Web Application Security Project) - IoT Security Guidance • Siemens - Industrial Security: Applying IoT Security Controls on the Industrial Plant Floor
Access Control	TM-37: Avoid using shared accounts for access to IIoT devices and systems. Create individual accounts for every user whenever possible, as this will enable tracking of the performed actions to a specific person. If shared accounts are used, change passwords periodically (e.g. every 90 days) and in case of personnel changes within a shared account group	• Physical attack • Unintentional damages (accidental)	• GSMA (Global System for Mobile Communications) - GSMA CLP.12 IoT Security Guidelines for IoT Service Ecosystems • GSMA (Global System for Mobile Communications) - GSMA CLP.13 IoT Security Guidelines for Endpoint Ecosystems • IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program • IEC - IEC 62443-3-3:2013 System security requirements and security levels • ISO - ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems -- Requirements • ISO - ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls • VDMA - Industrie 4.0 Security Guidelines Recommendations for actions

DOMAIN	SECURITY MEASURE/GOOD PRACTICE	THREAT GROUPS	REFERENCE
	(e.g. when an employee leaves). Also, consider deployment of additional compensating controls (e.g. segregation of duties, real-time monitoring tools such as industrial IDS).		
Access Control	TM-38: Implement in the device and/or use an account lockout functionality that activates after the number of failed login attempts exceeds the value of a set parameter. This also applies to cloud and mobile interfaces. Develop a policy to specify details such as the number of allowed attempts and time of the lockout.	• Nefarious activity / Abuse	• Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things • GSMA (Global System for Mobile Communications) - GSMA CLP.12 IoT Security Guidelines for IoT Service Ecosystems • GSMA (Global System for Mobile Communications) - GSMA CLP.13 IoT Security Guidelines for Endpoint Ecosystems • IEC - IEC 62443-3-3:2013 System security requirements and security levels • IoT Alliance Australia - Internet of Things Security Guidelines v1.2 • NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations • OWASP (Open Web Application Security Project) - IoT Security Guidance
Access Control	TM-39: In case of extensive and diversified networks with a large number of devices, adopt the Privilege Access Management (PAM) solution to manage elevated privileges (i.e. administrator privileges) in an orderly manner.	• Nefarious activity / Abuse • Eavesdropping / Interception / Hijacking • Physical attack • Unintentional damages (accidental)	• Cloud Security Alliance - Identity and Access Management for the Internet of Things - Summary Guidance • Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things • IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program • ISO - ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls • NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations
Access Control	TM-40: Within access control, include physical access to buildings, areas, rooms and cabinets locations (e.g. by means of walls, fences,	• Physical attack	• Cloud Security Alliance - Identity and Access Management for the Internet of Things - Summary Guidance • Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things • IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program • IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework • IIC (Industrial Internet Consortium) - IoT Security Maturity Model: Description and Intended Use

DOMAIN	SECURITY MEASURE/GOOD PRACTICE	THREAT GROUPS	REFERENCE
	electronic/mechanical locks and casings). Periodically revise access rights (especially to critical areas), limit physical access only to the required minimum and segregate it based on roles in the company. Ensure that the departure of an employee or change of a role within the company is followed by a prompt change/termination of physical access (e.g. physical access system can be connected to the HR system). Consider implementing tracking and alarm systems for supporting physical security.		• IoT Security Foundation - Connected Consumer Products. Best Practice Guidelines • ISO - ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems -- Requirements • ISO - ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls • NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations • NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security • NIST - NISTIR 8183: Cybersecurity Framework Manufacturing Profile • NIST - NISTIR 8200: Interagency Report on Status of International Cybersecurity Standardization for the Internet of Things (IoT) • NIST - Draft NISTIR 8228: Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks
Networks, protocols and encryption	TM-41: Ensure security of communications channels related to IIoT solutions. Encrypt communications in case of important data (e.g. configuration, personal data, data for control purposes), where it is possible to do so without affecting safety, availability and performance.	• Eavesdropping / Interception / Hijacking	• BITAG (Broadband Internet Technical Advisory Group) - Internet of Things (IoT) Security and Privacy Recommendations • Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things • GSMA (Global System for Mobile Communications) - GSMA CLP.12 IoT Security Guidelines for IoT Service Ecosystems • GSMA (Global System for Mobile Communications) - GSMA CLP.13 IoT Security Guidelines for Endpoint Ecosystems • GSMA (Global System for Mobile Communications) - GSMA CLP.14 IoT Security Guidelines for Network Operators • IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework • International Telecommunications Union - Security capabilities supporting safety of the Internet of things • IoT Alliance Australia - Internet of Things Security Guidelines v1.2 • IoT Security Foundation - Connected Consumer Products. Best Practice Guidelines • NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security • NIST - Draft NISTIR 8228: Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks

DOMAIN	SECURITY MEASURE/GOOD PRACTICE	THREAT GROUPS	REFERENCE
			• OpenAI and others - The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation • OWASP (Open Web Application Security Project) - IoT Security Guidance
Networks, protocols and encryption	TM-42: Segment industrial plants networks based on a pre-defined zoning model (e.g. into Office Layer, Manufacturing Layer and Control Layer according to the Purdue Model). Ensure that direct traffic between Office and Control layers is prohibited - these networks should always communicate with each other through a De-Militarised Zone (DMZ) with a 0-Trust rule. Traffic between each of the zones should always be controlled by a firewall. Locate shared infrastructure services which serve Manufacturing and Control networks (e.g. DC, DNS, NTP, Backup server, AV server, Jump Server) obtaining or providing data to the Office in a De-Militarised Zone (DMZ). Ensure dedicated network infrastructure (physical separation) for critical systems in the Control Layer.	• Nefarious activity / Abuse • Eavesdropping / Interception / Hijacking	• ENISA - Baseline Security Recommendations for IoT • Huawei - IoT Security White Paper 2017 • IEC - IEC 62443-1-1:2009 Terminology, concepts and models • IEC - IEC 62443-3-3:2013 System security requirements and security levels • IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework • IoT Alliance Australia - Internet of Things Security Guidelines v1.2 • ISO - ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems -- Requirements • LNS - Putting Industrial Cyber Security at the top of the CEO agenda • NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security • NIST - Draft NISTIR 8228: Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks • SANS Institute - Building the New Network Security Architecture for the Future • SANS Institute - The 2018 SANS Industrial IoT Security Survey: Shaping IIoT Security Concerns • Siemens - Industrial Security: Applying IoT Security Controls on the Industrial Plant Floor

DOMAIN	SECURITY MEASURE/GOOD PRACTICE	THREAT GROUPS	REFERENCE
Networks, protocols and encryption	TM-43: Follow micro segmentation approach that is based on building within the same network (e.g. IT or OT) small islands of components that communicate only inside these islands. Control traffic between different segments using a firewall. While segmenting the network, use the principles of least privilege and need-to-know. This means that only the necessary system-to-system communication using necessary protocols on necessary ports should be allowed and the rest should be disabled. In case of an infection, isolated micro-segments prevent it from spreading further onto the network. Micro segmentation within networks can be achieved through: - using VLANs for each micro segment, - physical network separation or - network traffic filtering at various layers, such as network layer filtering, state-based	• Nefarious activity / Abuse • Eavesdropping / Interception / Hijacking	• IEC - IEC 62443-1-1:2009 Terminology, concepts and models • IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program • IEC - IEC 62443-3-3:2013 System security requirements and security levels • IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework • IoT Alliance Australia - Internet of Things Security Guidelines v1.2 • LNS - Putting Industrial Cyber Security at the top of the CEO agenda • NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security • SANS Institute - Building the New Network Security Architecture for the Future

DOMAIN	SECURITY MEASURE/GOOD PRACTICE	THREAT GROUPS	REFERENCE
	filtering, port and protocol level filtering, application filtering.		
Networks, protocols and encryption	TM-44: Isolate safety networks from business and control networks. If this is not possible due to business requirements, ensure that solutions for network traffic filtering are in place.	• Nefarious activity / Abuse • Eavesdropping / Interception / Hijacking	• Homeland Security - Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies • IEC - IEC 62443-1-1:2009 Terminology, concepts and models • IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program • IEC - IEC 62443-3-3:2013 System security requirements and security levels • IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework • International Telecommunications Union - Security capabilities supporting safety of the Internet of things • NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security • NIST - Draft NISTIR 8228: Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks
	TM-45: For IIoT solutions implement proven-in-use protocols (rather than recently introduced ones) with known security capabilities, based on standards and technical recommendations. Choose solutions that use protocols that have been proved secure or tackle previous security issues (e.g. TLS 1.3) and avoid protocols with known vulnerabilities (e.g. Telnet, SNMP v1 or v2).		
Networks, protocols and encryption	TM-46: Ensure security capabilities and interoperability between protocols when implementing different protocols for various devices within the	• Nefarious activity / Abuse • Eavesdropping / Interception / Hijacking	• BITAG (Broadband Internet Technical Advisory Group) - Internet of Things (IoT) Security and Privacy Recommendations • Cloud Security Alliance - Identity and Access Management for the Internet of Things - Summary Guidance • Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things • ENISA - Baseline Security Recommendations for IoT

DOMAIN	SECURITY MEASURE/GOOD PRACTICE	THREAT GROUPS	REFERENCE
	same system. One of the example methods to achieve this is by using dedicated gateways that provide translation of protocols. A gateway can translate an insecure protocol into a modern, secure protocol before sending it further, thus reducing the attack surface.	• Failures / Malfunctions • Outages	• GSMA (Global System for Mobile Communications) - GSMA CLP.14 IoT Security Guidelines for Network Operators • Huawei - IoT Security White Paper 2017 • IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program • IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework • IoT Alliance Australia - Internet of Things Security Guidelines v1.2 • IoT Security Foundation - Connected Consumer Products. Best Practice Guidelines • NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations • NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security • NIST - Draft NISTIR 8228: Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks • OWASP (Open Web Application Security Project) - IoT Security Guidance
Networks, protocols and encryption	TM-47: If possible, limit the number of protocols implemented within a given environment to ensure manageability of the system. Also, disable all unused default network services.	• Failures / Malfunctions • Outages	• Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things • ENISA - Baseline Security Recommendations for IoT • GSMA (Global System for Mobile Communications) - GSMA CLP.14 IoT Security Guidelines for Network Operators • IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program • IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework • SANS Institute - The 2018 SANS Industrial IoT Security Survey: Shaping IIoT Security Concerns
Networks, protocols and encryption	TM-48: Ensure a secure environment for key exchange and key management while avoiding sharing cryptographic keys across multiple devices.	• Eavesdropping / Interception / Hijacking • Physical attack • Outages	• BITAG (Broadband Internet Technical Advisory Group) - Internet of Things (IoT) Security and Privacy Recommendations • Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things • IEC - IEC 62443-3-3:2013 System security requirements and security levels • NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations • SANS Institute - The 2018 SANS Industrial IoT Security Survey: Shaping IIoT Security Concerns • Siemens - Industrial Security: Applying IoT Security Controls on the Industrial Plant Floor
Networks, protocols and encryption	TM-49: Ensure the proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of data and information (including	• Eavesdropping / Interception / Hijacking	• BITAG (Broadband Internet Technical Advisory Group) - Internet of Things (IoT) Security and Privacy Recommendations • Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things • GSMA (Global System for Mobile Communications) - GSMA CLP.12 IoT Security Guidelines for IoT Service Ecosystems

DOMAIN	SECURITY MEASURE/GOOD PRACTICE	THREAT GROUPS	REFERENCE
	control messages), in transit and in rest. Ensure the proper selection of standard and strong encryption algorithms and strong keys and disable insecure protocols. Verify the robustness of the implementation.		• GSMA (Global System for Mobile Communications) - GSMA CLP.13 IoT Security Guidelines for Endpoint Ecosystems • GSMA (Global System for Mobile Communications) - GSMA CLP.14 IoT Security Guidelines for Network Operators • Huawei - IoT Security White Paper 2017 • IoT Security Foundation - Connected Consumer Products. Best Practice Guidelines • ISO - ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls • NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security • OWASP (Open Web Application Security Project) - IoT Security Guidance
Networks, protocols and encryption	TM-50: Implement passive monitoring solution in the IT and OT environments to create industrial network traffic baseline and monitor anomalies and adherence to the baseline. Deploy the monitoring solution on the Access Layer to capture relevant internal traffic.	• Nefarious activity / Abuse • Eavesdropping / Interception / Hijacking	• AT&T Cybersecurity Insights - Exploring IoT Security Volume 2 • BITAG (Broadband Internet Technical Advisory Group) - Internet of Things (IoT) Security and Privacy Recommendations • Cloud Security Alliance - Future Proofing the connected world • EC Alliance for Internet of Things Innovation (AIOTI) - AIOTI Digitisation of Industry Policy Recommendations • EuroSMART (the voice of the Smart Security Industry) - Internet Of Trust Security And Privacy In The Connected World • Federal Office for Information Security (BSI) - Protection Profile for the Gateway of a Smart Metering System (Smart Meter Gateway PP), Certification-ID: BSI-CC-PP-0073 • GSMA (Global System for Mobile Communications) - GSMA CLP.11 IoT Security Guidelines Overview Document • IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework • Infineon - Hardware Security for Smart Grid End Point Devices • International Telecommunications Union - Unleashing the potential of the Internet of Things • Internet Engineering Task Force (IETF) - Best Current Practices for Securing Internet of Things (IoT) Devices • Internet Engineering Task Force (IETF) - IETF RFC 7452 Architectural Considerations in Smart Object Networking • Internet Research Task force (IRTF) - State-of-the-Art and Challenges for the Internet of Things Security • IOT-A (Internet of Things Architecture) • ISACA - Performing a Security Risk Assessment

DOMAIN	SECURITY MEASURE/GOOD PRACTICE	THREAT GROUPS	REFERENCE
			• ISO - ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems -- Requirements #A10. Cryptography • ISO - ISO/IEC 27031:2011 Information technology -- Security techniques -- Guidelines for information and communication technology readiness for business continuity 7.4.3 • NIST - Draft NISTIR 8228: Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks • NIST - Framework for Improving Critical Infrastructure Cybersecurity V1.1 • NIST - NIST SP 800 30r1 - Guide for Conducting Risk Assessments • NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations - SC-13 Cryptographic Protection • oneM2M - Standards for M2M and the Internet of Things • OWASP (Open Web Application Security Project) - Guide to Cryptography • Software Assurance Forum for Excellence in Code (SAFECode) - NPO - Call it the Internet of Connected Things: The IoT Security Conundrum • Symantec - Internet Security Threat Report (ISTR) Volume 22 • Trusted Computing Group (TCG) - Guidance for Securing IoT Using TCG Technology Reference Document
Monitoring and auditing	TM-51: Collect security logs (i.e. change logs, fault logs, performance logs) to enable analysis of events. To the extent possible, event logs should include user IDs, system activities, dates, times and details of key events (e.g. log-on and log-off times), use of privileges, etc. Ensure that the logs are filtered, correlated and analysed in real-time using a dedicated tool, e.g. a SIEM class solutions, for example within a Security Operation Centre (SOC). If it is	• Nefarious activity / Abuse • Eavesdropping / Interception / Hijacking • Physical attack • Unintentional damages (accidental) • Failures / Malfunctions	• Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things • Federal Office for Information Security (BSI) - BSI-Standards 100-1 - Information Security Management Systems (ISMS) • Huawei - IoT Security White Paper 2017 • IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program • IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework • LNS - Putting Industrial Cyber Security at the top of the CEO agenda • NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations • NIST - NISTIR 8183: Cybersecurity Framework Manufacturing Profile • NIST - Draft NISTIR 8228: Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks • SANS Institute - The 2018 SANS Industrial IoT Security Survey: Shaping IIoT Security Concerns • Siemens - Industrial Security: Applying IoT Security Controls on the Industrial Plant Floor • Symantec - An Internet of Things Reference Architecture • Symantec - Smarter Security for Manufacturing in The Industry 4.0 Era: Industry 4.0 Cyber Resilience for the Manufacturing of the Future

DOMAIN	SECURITY MEASURE/GOOD PRACTICE	THREAT GROUPS	REFERENCE
	not technically feasible, review logs manually on a regular basis. Take further actions based on risk analysis. Also, ensure that logs are accessible through a commonly accepted interface and stored for a defined period.		
Monitoring and auditing	TM-52: Perform periodic reviews of access control privileges and asset configurations at least annually and in case of a major change in the system.	• Nefarious activity / Abuse • Eavesdropping / Interception / Hijacking • Physical attack • Unintentional damages (accidental) • Failures / Malfunctions	• Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things • ENISA - Baseline Security Recommendations for IoT • IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program • IEC - IEC 62443-3-3:2013 System security requirements and security levels • IIC (Industrial Internet Consortium) - IIC Endpoint Security Best Practices • IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework • IoT Security Foundation - Connected Consumer Products. Best Practice Guidelines • NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security • NIST - Draft NISTIR 8228: Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks • OWASP (Open Web Application Security Project) - IoT Security Guidance • SANS Institute - An Abbreviated History of Automation & Industrial Controls Systems and Cybersecurity • Siemens - Industrial Security: Applying IoT Security Controls on the Industrial Plant Floor • VDC - Industry 4.0: Secure by design
Monitoring and auditing	TM-53: Monitor the availability of the IIoT devices in real time, where technically feasible.	• Nefarious activity / Abuse • Eavesdropping / Interception / Hijacking • Physical attack • Unintentional damages (accidental)	• ENISA - Baseline Security Recommendations for IoT • Huawei - IoT Security White Paper 2017 • IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework • ISO - ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems -- Requirements • ISO - ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls • NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations • NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security • NIST - NISTIR 8183: Cybersecurity Framework Manufacturing Profile

DOMAIN	SECURITY MEASURE/GOOD PRACTICE	THREAT GROUPS	REFERENCE
		• Failures / Malfunctions	• NIST - NISTIR 8200: Interagency Report on Status of International Cybersecurity Standardization for the Internet of Things (IoT) • NIST - Draft NISTIR 8228: Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks • OWASP (Open Web Application Security Project) - IoT Security Guidance
Monitoring and auditing	TM-54: Establish baseline security configurations tailored to different types of assets. Within these baselines include, among others, information about system components (e.g. required software that is installed with version numbers and patch information on operating systems, whitelists of applications, required ports, protocols, functions and set parameters), network topology, logical placement within the system architecture, etc. In addition, establish procedures for reviewing and creating new baselines, as organisational information systems change over time.	• Nefarious activity / Abuse • Physical attack • Unintentional damages (accidental) • Failures / Malfunctions • Outages • Disaster	• ETSI (European Telecommunications Standards Institute) - ETSI GR QSC 004 V1.1.1 (2017-03) Quantum Safe Cryptography; Quantum-Safe threat assessment • IEC - IEC 62443-3-3:2013 System security requirements and security levels • IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework • IoT Alliance Australia - Internet of Things Security Guidelines v1.2 • NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security • NIST - NISTIR 8200: Interagency Report on Status of International Cybersecurity Standardization for the Internet of Things (IoT) • Smart Card Alliance - Embedded HW Security for IoT Applications
Configuration Management	TM-55: Implement a mechanism and supporting tools that allow for configuration management. This mechanism should enable tracking of changes and	• Nefarious activity / Abuse • Eavesdropping / Interception / Hijacking • Physical attack	• Huawei - IoT Security White Paper 2017 • IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program • IEC - IEC 62443-3-3:2013 System security requirements and security levels • IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework • NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations • NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security • NIST - NISTIR 8183: Cybersecurity Framework Manufacturing Profile

DOMAIN	SECURITY MEASURE/GOOD PRACTICE	THREAT GROUPS	REFERENCE
	recreation of the state of the system from before the change.	• Unintentional damages (accidental) • Failures / Malfunctions • Outages • Legal • Disaster	• NIST - Draft NISTIR 8228: Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks
Configuration Management	TM-56: Implement and document changes in configuration according to a change management policy developed by the organisation based on risk analysis. This policy should include responsibility (i.e. system owner, approvers, etc.) and security aspects. The business owners of assets should accept it.	• Nefarious activity / Abuse • Eavesdropping / Interception / Hijacking • Physical attack • Unintentional damages (accidental) • Failures / Malfunctions	• IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program • IEC - IEC 62443-3-3:2013 System security requirements and security levels • IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework • ISA - ANSI/ISA-95 Part 1: Models and Terminology • ISO - ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems -- Requirements • NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations • NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security • NIST - NISTIR 8183: Cybersecurity Framework Manufacturing Profile • Siemens - Industrial Security: Applying IoT Security Controls on the Industrial Plant Floor
Configuration Management	TM-57: Develop a dedicated procedure for impact analysis. Before implementation of change in the system, perform an analysis to determine the criticality of the considered change. Test changes to the configuration that may exert an impact on operations and precede them with risk analysis.	• Unintentional damages (accidental)	• IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program • IEC - IEC 62443-3-3:2013 System security requirements and security levels • IIC (Industrial Internet Consortium) - Accompanying the Industrial Internet of Things Volume G1: Reference architecture • IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework • ISO - ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems -- Requirements • ISO - ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls • NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations • NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security • NIST - NISTIR 8183: Cybersecurity Framework Manufacturing Profile • NIST - Draft NISTIR 8228: Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks

DOMAIN	SECURITY MEASURE/GOOD PRACTICE	THREAT GROUPS	REFERENCE
			• SANS Institute - The 2018 SANS Industrial IoT Security Survey: Shaping IIoT Security Concerns
Configuration Management	TM-58: Harden IIoT solutions and include this in the change management policy. Ensure that all unused network ports, protocols and unnecessary functionalities of the devices are disabled and that test/debug features are locked. Hardening should include, where applicable, operation system, software, firmware and application. In addition, perform periodic checks of critical samples at least annually and in case of a major change to the system.	• Unintentional damages (accidental)	• IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program • IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework • ISA - ANSI/ISA-95 Part 1: Models and Terminology • ISO - ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems -- Requirements • NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations • NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security
Configuration Management	TM-59: Create and apply a comprehensive backup plan, including provisions for periodic testing, tailored to different types of assets. Perform backups before updates and other important changes to the system. For some assets, backups should be made regularly with the frequency depending on the asset type. When making a backup, verify whether it will work properly (perform a test of the backup).	• Eavesdropping / Interception / Hijacking • Physical attack • Failures / Malfunctions	• Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things • ENISA - Baseline Security Recommendations for IoT • IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework • IIC (Industrial Internet Consortium) - IoT Security Maturity Model: Description and Intended Use • IoT Alliance Australia - Internet of Things Security Guidelines v1.2 • IoT Security Foundation - Connected Consumer Products. Best Practice Guidelines • NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security • NIST - Draft NISTIR 8228: Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks • OpenAI and others - The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation • OWASP (Open Web Application Security Project) - IoT Security Guidance • Siemens - Industrial Security: Applying IoT Security Controls on the Industrial Plant Floor • Symantec - Smarter Security for Manufacturing in The Industry 4.0 Era: Industry 4.0 Cyber Resilience for the Manufacturing of the Future

DOMAIN	SECURITY MEASURE/GOOD PRACTICE	THREAT GROUPS	REFERENCE
	To do so, you may check hash or use a dedicated application.		
Configuration Management	TM-01: Verify the integrity of the software before starting to run it. Verify the root of trust and secure boot mechanisms. Ensure that the software comes from a reliable source (signed by the vendor) and that it is obtained in a secure manner, e.g. downloaded via an encrypted connection. Software signing and/or checksum control should be in place to ensure that the software is legitimate.	• Failures / Malfunctions • Outages • Disaster	• IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program • IEC - IEC 62443-3-3:2013 System security requirements and security levels • ISO - ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems -- Requirements • ISO - ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls • NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations • NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security • NIST - NISTIR 8183: Cybersecurity Framework Manufacturing Profile

Annex C: Security standards and references reviewed

AUTHOR	TITLE	REFERENCE
1. EU Initiatives		
EC Alliance for Internet of Things Innovation (AIOTI)	AIOTI Digitisation of Industry Policy Recommendations	https://aioti-space.org/wp-content/uploads/2017/03/AIOTI-Digitisation-of-Ind-policy-doc-Nov-2016.pdf
ECSO (European Cyber Security Organization)	INDUSTRY 4.0 AND ICS SECTOR REPORT Cyber security for the industry 4.0 and ICS sector	http://www.ecs-org.eu/documents/uploads/industry-40-and-ics-sector-report-032018.pdf
ENISA	Baseline Security Recommendations for IoT	https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot
European Parliament and Council of the European Union	The General Data Protection Regulation (GDPR) (EU) 2016/679	https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG
IOT-A (Internet of Things Architecture)	IOT-A (Internet of Things Architecture)	http://cordis.europa.eu/project/rcn/95713_en.html http://www.meet-iot.eu/iot-a-deliverables.html
2. US Government Initiatives		
Homeland Security	Strategic Principles for Securing the Internet of Things	https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf
Homeland Security	Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies	https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf
NIST	NISTIR 8183: Cybersecurity Framework Manufacturing Profile	https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8183.pdf

AUTHOR	TITLE	REFERENCE
NIST	Draft NISTIR 8228: Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks	https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8228-draft.pdf
NIST	NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf
NIST	NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf
NIST	NIST.SP 1500-202 - Framework for Cyber-Physical Systems: Volume 2, Working Group Reports	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1500-202.pdf
NIST	NIST SP 800 30r1 - Guide for Conducting Risk Assessments	https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf
NIST	Best practices in cyber supply chain risk management. Smart Manufacturing The Future of Manufacturing and Value Chain Competitiveness	https://www.nist.gov/sites/default/files/documents/itl/csd/NIST_USRP-SmartManu-Cyber-SCRM-Case-Study.pdf
NIST	NIST SP 800-52 r1: Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r1.pdf
NIST	Cybersecurity for Smart Manufacturing	https://www.nist.gov/sites/default/files/documents/2016/12/05/cybersecurity_for_smart_manufacturing.pdf
NIST	Framework for Cyber-Physical Systems: Volume 1, Overview	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1500-201.pdf
NIST	Framework for Improving Critical Infrastructure Cybersecurity V1.1	https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

AUTHOR	TITLE	REFERENCE
NIST	NIST Advanced Manufacturing Series 300-1 Reference Architecture for Smart Manufacturing Part 1: Functional Models	https://nvlpubs.nist.gov/nistpubs/ams/NIST.AMS.300-1.pdf
NIST	NIST SP 800-146 Cloud Computing Synopsis and Recommendations	https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-146.pdf
NIST	NIST SP 800-61r2: Computer Security Incident Handling Guide - Recommendations of the National Institute of Standards and Technology	https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf
NIST	NISTIR 8200: Interagency Report on Status of International Cybersecurity Standardization for the Internet of Things (IoT)	https://csrc.nist.gov/publications/detail/nistir/8200/draft
3. International Organizations/Alliances		
Auto ISAC (Automotive Information Sharing and Analysis Center)	Automotive Cybersecurity Best Practices - Executive Summary	http://www.sovereign-plc.co.uk/sites/default/files/Auto%20ISAC%20Cyber%20Security%20Best%20Practices%20Executive%20Summary.pdf
BITAG (Broadband Internet Technical Advisory Group)	Internet of Things (IoT) Security and Privacy Recommendations	https://www.bitag.org/documents/BITAG_Report_-_Internet_of_Things_(IoT)_Security_and_Privacy_Recommendations.pdf
Center for Internet Security (CIS)	Critical Security Controls	https://www.cisecurity.org/wp-content/uploads/2017/03/Poster_Winter2016_CSCs.pdf
Cloud Security Alliance	Security Guidance for Early Adopters of the Internet of Things	https://downloads.cloudsecurityalliance.org/whitepapers/Security_Guidance_for_Early_Adopters_of_the_Internet_of_Things.pdf
Cloud Security Alliance	Identity and Access Management for the Internet of Things - Summary Guidance	https://downloads.cloudsecurityalliance.org/assets/research/internet-of-things/identity-and-access-management-for-the-iot.pdf
Cloud Security Alliance	Future Proofing the connected world	https://downloads.cloudsecurityalliance.org/assets/research/internet-of-things/future-proofing-the-connected-world.pdf

AUTHOR	TITLE	REFERENCE
ETSI (European Telecommunications Standards Institute)	ETSI GR QSC 004 V1.1.1 (2017-03) Quantum Safe Cryptography; Quantum-Safe threat assessment	http://www.etsi.org/deliver/etsi_gr/QSC/001_099/004/01.01.01_60/gr_QSC004v010101p.pdf
ETSI (European Telecommunications Standards Institute)	ETSI TR 103 375 SmartM2M; IoT Standards landscape and future evolutions	http://www.etsi.org/deliver/etsi_tr/103300_103399/103375/01.01.01_60/tr_103375v010101p.pdf
ETSI (European Telecommunications Standards Institute)	ETSI TR 118 518 V2.0.0 (2016-09) oneM2M; Industrial Domain Enablement	https://www.etsi.org/deliver/etsi_tr/118500_118599/118518/02.00.00_60/tr_118518v020000p.pdf
EuroSMART (the voice of the Smart Security Industry)	Internet Of Trust Security And Privacy In The Connected World	http://www.eurosmart.com/news-publications/99-policy-papers/245-eurosmart-internet-of-trust-security-and-privacy-in-the-connected-world.html
Federal Office for Information Security (BSI)	BSI-Standards 100-4 - Business Continuity Management	https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/BSIStandards/standard_100-4_e_pdf.pdf?__blob=publicationFile&v=1
Federal Office for Information Security (BSI)	BSI-Standards 100-1 - Information Security Management Systems (ISMS)	https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/BSIStandards/standard_100-1_e_pdf.pdf?__blob=publicationFile&v=1
Federal Office for Information Security (BSI)	Protection Profile for the Gateway of a Smart Metering System (Smart Meter Gateway PP), Certification-ID: BSI-CC-PP-0073	https://www.commoncriteriaportal.org/files/ppfiles/pp0073b_pdf.pdf
GSMA	GSMA CLP.11 IoT Security Guidelines Overview Document	https://www.gsma.com/iot/wp-content/uploads/2016/02/CLP.11-v1.1.pdf
GSMA	GSMA CLP.12 IoT Security Guidelines for IoT Service Ecosystems	https://www.gsma.com/iot/wp-content/uploads/2016/02/CLP.12-v1.0.pdf
GSMA	GSMA CLP.13 IoT Security Guidelines for Endpoint Ecosystems	https://www.gsma.com/iot/wp-content/uploads/2016/02/CLP.13-v1.0.pdf
GSMA	GSMA CLP.14 IoT Security Guidelines for Network Operators	https://www.gsma.com/iot/wp-content/uploads/2017/10/CLP.14-v2.0.pdf

AUTHOR	TITLE	REFERENCE
IEC	IEC 62443-1-1:2009 Terminology, concepts and models	https://webstore.iec.ch/publication/7029
IEC	IEC 62443-2-1:2010 Establishing an industrial automation and control system security program	https://webstore.iec.ch/publication/7030
IEC	IEC 62443-3-3:2013 System security requirements and security levels	https://webstore.iec.ch/publication/7033
IEC	IEC 62443-4-1:2013 Secure product development lifecycle requirements	https://webstore.iec.ch/publication/33615
IEEE	Internet of Things (IoT) Security Best Practices	https://internetinitiative.ieee.org/images/files/resources/white_papers/internet_of_things_feb2017.pdf
IEEE	IEEE Std 802.1X-2010 - Port-Based Network Access Control	http://moodle.eece.cu.edu.eg/pluginfile.php/1799/mod_folder/content/1/802.1X-2010.pdf?forcedownload=1
IIC (Industrial Internet Consortium)	IIC Endpoint Security Best Practices	https://www.iiconsortium.org/pdf/Endpoint_Security_Best_Practices_Final_Mar_2018.pdf
IIC (Industrial Internet Consortium)	Accompanying the Industrial Internet of Things Volume G1: Reference architecture	https://www.iiconsortium.org/IIC_PUB_G1_V1.80_2017-01-31.pdf
IIC (Industrial Internet Consortium)	Industrial Internet of Things Volume G4: Security Framework	https://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB.pdf
IIC (Industrial Internet Consortium)	IoT Security Maturity Model: Description and Intended Use	https://www.iiconsortium.org/pdf/SMM_Description_and_Intended_Use_2018-04-09.pdf
International Telecommunications Union	Security capabilities supporting safety of the Internet of things	https://www.itu.int/rec/T-REC-Y.4806/en

AUTHOR	TITLE	REFERENCE
International Telecommunications Union	Unleashing the potential of the Internet of Things	https://www.itu.int/en/publications/Documents/tsb/2016-InternetOfThings/index.html
Internet Engineering Task Force (IETF)	Best Current Practices for Securing Internet of Things (IoT) Devices	https://www.ietf.org/proceedings/56/
Internet Engineering Task Force (IETF)	IETF RFC 7452 Architectural Considerations in Smart Object Networking	https://tools.ietf.org/html/rfc7452
Internet Research Task force (IRTF)	State-of-the-Art and Challenges for the Internet of Things Security	https://tools.ietf.org/pdf/draft-irtf-t2trg-iot-seccons-04.pdf
IoT Alliance Australia	Internet of Things Security Guidelines v1.2	http://www.iot.org.au/wp/wp-content/uploads/2016/12/IoTAA-Security-Guideline-V1.2.pdf
IoT Security Foundation	Connected Consumer Products. Best Practice Guidelines	https://iotsecurityfoundation.org/wp-content/uploads/2016/12/Connected-Consumer-Products.pdf
IoT Security Foundation	Security Challenges on the Way Towards Smart Manufacturing	https://www.iotsecurityfoundation.org/security-challenges-on-the-way-towards-smart-manufacturing/
IoT Security Foundation	Establishing Principles for IoT Security	https://iotsecurityfoundation.org/wp-content/uploads/2015/09/IoTSF-Establishing-Principles-for-IoT-Security-Download.pdf
ISA	ANSI/ISA-95 Part 1: Models and Terminology	https://www.isa.org/store/ansi/isa-950001-2010-iec-62264-1-mod-enterprise-control-system-integration-part-1-models-and-terminology/116636
oneM2M - Standards for M2M and the Internet of Things	TR 0008 Security V2.0.0 - Security. Technical Report	http://www.onem2m.org/images/files/deliverables/Release2/TR-0008-Security-V2_0_0.pdf
Online Trust Alliance	IoT trust framework 2.5	https://otalliance.org/system/files/files/initiative/documents/iot_trust_framework6-22.pdf

AUTHOR	TITLE	REFERENCE
OWASP (Open Web Application Security Project)	Guide to Cryptography	https://www.owasp.org/index.php/Guide_to_Cryptography
OWASP (Open Web Application Security Project)	IoT Security Guidance	https://www.owasp.org/index.php/IoT_Security_Guidance
OWASP (Open Web Application Security Project)	Mobile Top 10 2016	https://www.owasp.org/index.php/Mobile_Top_10_2016-Top_10
SANS Institute	An Abbreviated History of Automation & Industrial Controls Systems and Cybersecurity	https://ics.sans.org/media/An-Abbreviated-History-of-Automation-and-ICS-Cybersecurity.pdf
SANS Institute	Building the New Network Security Architecture for the Future	https://www.sans.org/reading-room/whitepapers/cloud/building-network-security-architecture-future-38255
SANS Institute	The 2018 SANS Industrial IoT Security Survey: Shaping IIoT Security Concerns	https://www.sans.org/reading-room/whitepapers/analyst/2018-industrial-iot-security-survey-shaping-iiot-security-concerns-38505
SANS Institute	Vulnerability Management: Tools, Challenges and Best Practices	https://www.sans.org/reading-room/whitepapers/threats/vulnerability-management-tools-challenges-practices-1267
Smart Card Alliance	Embedded HW Security for IoT Applications	https://www.securetechalliance.org/downloads/Embedded-HW-Security-for-IoT-WP-FINAL-December-2016.pdf
Software Assurance Forum for Excellence in Code (SAFECode) - NPO	Call it the Internet of Connected Things: The IoT Security Conundrum	http://www.safecode.org/call-it-the-internet-of-connected-things-the-iot-security-conundrum/
Trusted Computing Group (TCG)	Guidance for Securing IoT Using TCG Technology Reference Document	https://trustedcomputinggroup.org/guidance-securing-iot-using-tcg-technology-reference-document/
World Economic Forum	Industrial Internet of Things: Unleashing the Potential of Connected Products and Services	http://www3.weforum.org/docs/WEFUSA_IndustrialInternet_Report2015.pdf

4. Other references

AUTHOR	TITLE	REFERENCE
AT&T Cybersecurity Insights	Exploring IoT Security Volume 2	https://www.business.att.com/cybersecurity/docs/exploringiotsecurity.pdf
Elsevier	Avoiding the internet of insecure industrial things	https://www.sciencedirect.com/science/article/pii/S0267364917303217
Huawei	IoT Security White Paper 2017	https://www.huawei.com/minisite/iot/img/hw_iot_secutity_white_paper_2017_en_v2.pdf
Infineon	Hardware-based solutions secure machine identities in smart factories	https://www.infineon.com/dgdl/Infineon-IoT+Security+in+Smart+Factories-ART-v01_00-EN.pdf?fileId=5546d46254e133b40154e22c8a7d0251
Infineon	Hardware Security for Smart Grid End Point Devices	https://www.nrel.gov/esif/assets/pdfs/hardware_security_smart_grid.pdf
ISACA	Performing a Security Risk Assessment	https://www.isaca.org/journal/archives/2010/volume-1/pages/performing-a-security-risk-assessment1.aspx
ISO	ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems -- Requirements	https://www.iso.org/standard/54534.html
ISO	ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls	https://www.iso.org/standard/54533.html
ISO	ISO/IEC 27031:2011 Information technology -- Security techniques -- Guidelines for information and communication technology readiness for business continuity	https://www.iso.org/standard/44374.html
LNS	Putting Industrial Cyber Security at the top of the CEO agenda	https://www.honeywellprocess.com/en-US/online_campaigns/lns-cyber-report/Pages/Honeywell-LNS-Study_PuttingIndustrialCyberSecurityattheTopCEOAgenda.pdf
MIT	Security Analysis of Zigbee	https://courses.csail.mit.edu/6.857/2017/project/17.pdf

AUTHOR	TITLE	REFERENCE
OpenAI and others	The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation	https://www.eff.org/files/2018/02/20/malicious_ai_report_final.pdf
Shaun Bligh-Wall	Industry 4.0: Security imperatives for IoT — converging networks, increasing risks.	https://www.henrystewartpublications.com/sites/default/files/Bligh-Wall.pdf
Siemens	Industrial Security: Applying IoT Security Controls on the Industrial Plant Floor	https://www.industry.usa.siemens.com/automation/us/en/formsdocs/Documents/2016%20MIA-%2023%20Industrial%20Security%20Applying%20IoT%20Security%20Controls%20on%20the%20Industrial%20Plant%20Floor.pdf
Smart Factory Innovation Forum	Managing security, safety and privacy in Smart Factories	https://www.pinsentmasons.com/dokument/it-security-in-smart-factories-white-paper-april-2015.pdf
Symantec	An Internet of Things Reference Architecture	https://www.symantec.com/content/en/us/enterprise/white_papers/iot-security-reference-architecture-wp-en.pdf
Symantec	Internet Security Threat Report (ISTR) Volume 22	https://www.symantec.com/security-center/threat-report https://resource.elq.symantec.com/LP=3980?cid=70138000001BjppAAC&mc=202671&ot=wp&tt=sw&inid=symc_threat-report_regular_to_leadgen_form_LP-3980_ISTR22-report-main
Symantec	Smarter Security for Manufacturing in The Industry 4.0 Era: Industry 4.0 Cyber Resilience for the Manufacturing of the Future	https://www.symantec.com/content/dam/symantec/docs/solution-briefs/industry-4.0-en.pdf
The Cavalry	Hippocratic Oath for Connected Medical Devices	https://www.iamthecavalry.org/wp-content/uploads/2016/01/I-Am-The-Cavalry-Hippocratic-Oath-for-Connected-Medical-Devices.pdf
VDC	Industry 4.0: Secure by design	https://cdn2.hubspot.net/hubfs/582328/whitepapers/VDC%20-%20Industry%204.0%20Secure%20by%20Design%20-%20for%20GrammaTech.pdf?t=1519834251604

AUTHOR	TITLE	REFERENCE
VDMA	Industrie 4.0 Security Guidelines Recommendations for actions	http://www.vdmashop.de/refs/Leitf_I40_Security_En_LR_neu.pdf
VDMA	Smart Manufacturing General security and privacy principles to ensure a Trusted IoT environment	http://ec.europa.eu/information_society/newsroom/image/document/2017-11/smart_manufacturing_to_ensure_a_trusted_iot_environment_by_vdma_0B8285E7-9C90-7E5C-04DA25B61A5C3FA5_43660.pdf
IOActive, Embedi	SCADA And Mobile Security In The Internet Of Things Era	https://ioactive.com/pdfs/SCADA-and-Mobile-Security-in-the-IoT-Era-Embedi-FINALab%20(1).pdf

Annex D: Description of indicative Industry 4.0 security incidents

SECURITY INCIDENT	DATE	DESCRIPTION
Triton malware attack on Safety Instrumented System (SIS)	November 2017	The purpose of an SIS is to take immediate action when a critical process goes some other way than planned e.g. if the pressure in a tank rises above a predetermined level, SIS will activate valves to lower the pressure to prevent an explosion. Disturbing this failsafe mechanism can have severe physical consequences, especially in an industrial plant. One of these systems was attacked in 2017 by Triton – an industry-targeted malware designed to inflict severe damage. This was the first cyber-attack on a Safety Instrumented System (SIS) ever recorded. After obtaining remote access to a workstation, attackers infected SIS with malware. Using Zero-Day vulnerability, Triton managed to install itself on SIS, providing attackers with full control. However, once in, the attackers "tripped" and triggered the safety shut down of a process governed by SIS. This alarmed employees, leading to detection of the malware and stopping the attack before it caused any serious damage that would most probably have destroyed infrastructure and halted production. [48] [49]
NotPetya - ransomware created to cause damage	June 2017	Just 6 weeks after WannaCry, a new global cyberattack emerged. Originally targeted at Ukraine – its central bank, government and utilities (such as electrical grids), it managed to disrupt people's everyday life across the country. Spreading further, NotPetya (also known as ExPetr, often referred to as Petya) infected more than 200,000 computers worldwide and affected mostly industrial companies such as Rosneft, Merck and Maersk. Using an SMB protocol exploit to achieve initial infection it then tried to steal credentials and take control of other machines on the network, including those immune (e.g. patched) to this exploit. This made NotPetya especially dangerous, as even a single vulnerable device could lead to the compromise of the whole network. Soon after the infection, NotPetya proceeded to encrypt files on the computer using an irreversible. This means that once encrypted, all affected files are lost, which makes the virus work like a wiper, deleting important data from the system. Combined with the attackers' inability to collect ransom, this raised serious speculations whether NotPetya was really ransomware or a cyber-weapon disguised as one. [50] [51] [52] [53] [54]

[48] See CyberArk (2018) "Anatomy of the Triton malware attack": https://www.cyberark.com/threat-research-blog/anatomy-triton-malware-attack/
[49] See Sentryo (2018) "Analysis of Triton industrial malware": https://www.sentryo.net/analysis-triton-malware/
[50] See Kaspersky Lab (2017) "More than 50% of organizations attacked by ExPetr (Petya) cryptolocker are industrial companies": https://ics-cert.kaspersky.com/alerts/2017/06/29/more-than-50-percent-of-organizations-attacked-by-expetr-petya-cryptolocker-are-industrial-companies/
[51] See The New York Times (2017) "Cyberattack Hits Ukraine Then Spreads Internationally": https://www.nytimes.com/2017/06/27/technology/ransomware-hackers.html
[52] See CNet (2018) "US: Russia's NotPetya the most destructive cyberattack ever": https://www.cnet.com/news/uk-said-russia-is-behind-destructive-2017-cyberattack-in-ukraine/
[53] See TechRepublic (2017) "NotPetya ransomware outbreak cost Merck more than $300M per quarter": https://www.techrepublic.com/article/notpetya-ransomware-outbreak-cost-merck-more-than-300m-per-quarter/
[54] See The Register (2018) "IT 'heroes' saved Maersk from NotPetya with ten-day reinstallation bliz": https://www.theregister.co.uk/2018/01/25/after_notpetya_maersk_replaced_everything/

SECURITY INCIDENT	DATE	DESCRIPTION
WannaCry ransomware worldwide cyberattack	May 2017	This enormous, worldwide cyberattack infected more than 230,000 computers across 150 countries and affected manufacturers, banks and governments. Organisations such as Renault and Honda were forced to halt production, FedEx clients experienced delays on deliveries, and the UK's National Health Service was forced to cancel thousands of appointments. Those are only a few of the confirmed victims of this ransomware, with many more organisations not admitting to having been infected. WannaCry, as this virus is called, using two sophisticated exploits in Microsoft Windows systems managed to spread through the SMB protocol, installing itself on a vulnerable machine without any user action (such as opening a malicious e-mail attachment). Once in, it scanned the network for other targets, infecting all of them, repeating the process and spreading the infection further into the system. Fortunately, the attack was slowed down by discovery of a kill-switch – a major flaw in the virus that allowed researchers to "turn off" its spreading functionality, leaving asset owners with a few hours to secure their devices and prepare for another wave of infections. Securing those devices could have been as easy as installing the security updates released by Microsoft a few months earlier.
Industroyer – second cyberattack on Ukrainian power grid	December 17, 2016	The second cyberattack on the Ukrainian power grid came almost exactly a year after the first one. It shared many similarities with its predecessor but varied in the method used. This time, attackers used a new malware specifically designed to attack electrical grids – Industroyer. It targets widely used communication protocols, providing the attacker with a backdoor to an industrial control system. Once again, attackers opened circuit breakers stopping power supply and once again they delayed recovery by additional means, such as wiping crucial files to make the system unresponsive. As a result, one fifth of Kiev, the capital of Ukraine, was left without electricity for an hour. It is suspected that this attack was a large-scale test, as attackers did not harness the malware's full potential. As Industroyer can be slightly modified to target other types of critical infrastructure, such as water or gas, it is a major threat to industrial control systems that has been proven to work. [55] [56]
BrickerBot – permanent denial of service botnet	November 2016 – December 2017	An alert was issued by ICS-CERT warning of a new bot attack similar to Mirai. Named BrickerBot by its creator, it uses brute force in the telnet to gain access to a device and then puts it in a permanent denial of service state forcing its owner to reinstall the device or replace it altogether. According to its creator, BrickerBot "bricked" over 10 million devices in about a year. [57] [58]

[55] See WeLiveSecurity (2017) "Industroyer: Biggest threat to industrial control systems since Stuxnet": https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/

[56] See MIT Technology Review (2016) "Ukraine's Power Grid Gets Hacked Again, a Worrying Sign for Infrastructure Attacks": https://www.technologyreview.com/s/603262/ukraines-power-grid-gets-hacked-again-a-worrying-sign-for-infrastructure-attacks/

[57] See ICS-CERT (2017) "Alert (ICS-ALERT-17-102-01A) BrickerBot Permanent Denial-of-Service Attack": https://ics-cert.us-cert.gov/alerts/ICS-ALERT-17-102-01A

[58] See BleepingComputer (2017) "BrickerBot Author Retires Claiming to Have Bricked over 10 Million IoT Devices": https://www.bleepingcomputer.com/news/security/brickerbot-author-retires-claiming-to-have-bricked-over-10-million-iot-devices/

SECURITY INCIDENT	DATE	DESCRIPTION
Mirai – IoT botnets attack	October 21, 2016	The botnet made of IoT devices infected by Mirai has been associated with one of the largest Distributed Denial of Service (DDoS) attacks ever performed. The most notable attack was on a DNS service provider called Dyn. By attacking Dyn with up to 100,000 infected devices across the world, the attackers managed to disrupt or even disconnect several popular services, such as Twitter, Netflix or Spotify, at the same time. The way the malware infected so many devices was simply by utilising the most popular and vendor provided passwords to gain access to them. Having "recruited" them, the attackers left the devices almost untouched, seemingly unaffected by malware. With an army at their disposal, the attackers were able to order it to flood selected destinations, such as Dyn, exceeding their bandwidth limits and bringing them down. What is probably the most troubling about Mirai is that its source code is publicly available, providing anyone with a way to build a botnet. Every month a new improved variety of Mirai is discovered. Even though the original Mirai did not specifically target IIoT devices, a version of it that does can surface any day now.[59] [60]
Cyberattack on a power grid in Ukraine	December 23, 2015	The cyberattack on the power grid in Ukraine was well planned, carefully prepared and flawlessly executed. The attackers' goal was not only to disturb power supply, but also to delay restoration for as long as possible. It started similarly to many other attacks, namely with phishing emails containing malicious Microsoft Office files with embedded malware. This malware, known as BlackEnergy, allowed the attackers to steal privileged credentials and perform network reconnaissance, finding out all the information about the infected system. Then, after as much as 6 months, attackers remotely seized control over a SCADA system, opening multiple electricity breakers and leaving about 230 thousand people without electricity. At the same time, they took a number of steps to prolong the effect. One, every infected computer's hard drive was wiped. Two, uninterruptible power supply (UPS) was compromised resulting in service outages. Three, they "blew the bridges" by uploading malicious firmware to gateway devices, making remote recovery impossible. These side-attacks successfully delayed recovery, leaving people without electricity for up to 6 hours. This attack and the helplessness of the defence served as a wake-up call to a lot of manufacturers.[61]
Cyberattack on Kemuri Water Company's water treatment plant	2015	Kemuri Water Company (KWC) is an alias for an anonymous water company which experienced a security breach in its water treatment plant in 2015. Due to major security flaws such as the usage of outdated operating systems or storing all data on a single "ancient" server (IBM AS/400 from 1988), attackers exploiting vulnerability in an online payments system gained access to all of KWC's customers' data and their ICS. Then, by manipulating PLCs, attackers changed the amount of chemicals used, influencing the tap water's properties. Luckily, this change was harmless as it is supposed that the attackers' main goal was to obtain sensitive

[59] See Sentryo (2016) "The 'mirai' iot botnet, a publically available turn-key threat": https://www.sentryo.net/the-mirai-iot-botnet-a-publically-available-turn-key-threat-2/
[60] See Xage Security (2016) "Mirai and IIoT Security": https://xage.com/press/mirai-and-iiot-security/
[61] See SANS ICS (2016) "Analysis of the Cyber Attack on the Ukrainian Power Grid Defense Use Case": https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf

SECURITY INCIDENT	DATE	DESCRIPTION
		customer data and not disturb the water treatment process. Had their goals been different, it would have posed a serious threat to the public.[62]
German steel mill attack	2014	This attack, as many others, started with a phishing email opened by a reckless employee. Once in the corporate network, attackers, using an unknown technique, moved into the plant network and seized control of multiple ICS components (including PLCs, HMIs and alarm systems). Then, manipulating individual systems and causing their failure, attackers disrupted the safe shutdown of a blast furnace, which resulted in serious physical damage to the system.[63]
Havex / Dragonfly – a Remote Access Trojan targeted on SCADA, PLC and DCS systems	2014	In 2014 it was reported that a number of European and US power facilities were infected with a new malware created by a group known as Dragonfly. The malware targeting ICSs consisted of two Remote Access Trojans (RATs) which allowed the attacker to upload, download and execute files from the infected computer. Its main mission was to collect data and information about the infected system but with persistent backdoor access it could easily transform into something more malicious. What is even more interesting is how this malware infected its victims. Besides phishing emails and watering hole attacks, it also hacked some ICS vendors software downloads and planted RATs in them thereby even infecting somewhat cautious targets.[64]
Shamoon virus - Cyberattack on Saudi Arabian Oil Company (Saudi Aramco)	August 15, 2012	This attack started with a Saudi Aramco employee from the IT team opening a malicious phishing email providing a point of entry for the attacker. Once inside, attackers dropped a virus later known as Shamoon. It immediately started spreading across Saudi Aramco's entire IT network, infecting at least 35,000 computers. Then, at a carefully selected date – Saudi Arabia's national holiday – the virus began to wipe all the data on the infected computers replacing it with the image of a burning American Flag. After that, it proceeded to overwrite the computers' Master Boot Record making it unusable. Even though the attack affected only the IT network, leaving separate ICS completely functional, it had a huge impact on other business processes, such as loading gasoline trucks.[65]
Duqu – Stuxnet evolved	2011	Duqu is "nearly identical to Stuxnet, but with a completely different purpose" according to Symantec. It targets Microsoft Windows, just like Stuxnet, and uses Microsoft Word to execute code in kernel mode. Once the machine is infected, Duqu's purpose is not to destroy it, but rather gather information useful in future attacks. Other than recording keystrokes and system information, according to McAfee, Duqu steals digital certificates that may be used to make future viruses appear more legitimate. Although there was no code related to industrial control

[62] See Sentryo (2017) "The Sentryo Files: Industries Vs. Cyberattacks Episode 5: A Water Treatment Plant Under Attack": https://www.sentryo.net/sentryo-files-attack-water-treatment-plant/
[63] See SANS ICS (2014) "German Steel Mill Cyber Attack": https://ics.sans.org/media/ICS-CPPE-case-Study-2-German-Steelworks_Facility.pdf
[64] See Belden (2014) "How Dragonfly Hackers and RAT Malware Threaten ICS Security": https://www.belden.com/blog/industrial-security/how-dragonfly-hackers-and-rat-malware-threaten-ics-security
[65] See CNNMoney (2015) "The inside story of the biggest hack in history": https://money.cnn.com/2015/08/05/technology/aramco-hack/index.html

SECURITY INCIDENT	DATE	DESCRIPTION
		systems found in analyses, the information gathered by Duqu might enable future attacks on Industrial Internet of Things.[66]
Cyberattack on a SCADA system of an American Water and Utility company causing destruction of one of the pumps	November 8, 2011	This attack started with utility's SCADA software vendor being hacked and a list of usernames and passwords to customer systems being stolen. Vendors allowing them access to customers' systems for support purposes sometimes maintain these lists. Once the attacker had these credentials, he could access the pump's controlling system and issue commands leading to its destruction.[67]
Cyberattacks on Smart Meters	2010	In 2010, it was reported that power thieves exploiting vulnerability in smart meters caused PREPA (Puerto Rico Electric Power Authority) to incur costs of 400 million dollars a year. Only a few things were required to carry out this attack, namely optical probes, freely available software and physical access to the meter. Because of its simplicity, many smart meters recordings were modified resulting in such an enormous loss.[68]
Stuxnet worm attack on Natanz nuclear enrichment lab in Iran	2010	In 2010 workers at the Natanz nuclear facility realised that a strange number of uranium enriching centrifuges were breaking. After inspection, it was found that the Stuxnet worm that targets programmable logic controllers (PLCs) infected their computer systems. It is believed that it was introduced into the system by a USB drive, from where it targeted Microsoft Windows and Siemens Step7 software exploiting their vulnerabilities to gain access to PLCs, modifying the codes and giving unexpected commands to the PLC while returning unsuspicious feedback. In this incident, the attackers made centrifuges spin fast enough to tear themselves apart while giving no warning to operators. Although no official report was released, it is estimated that Stuxnet ruined almost one fifth of Iran's nuclear centrifuges.[69]
Disruption of multiple DaimlerChrysler's car manufacturing plants by a Zotob worm	August 16, 2005	Auto manufacturer DaimlerChrysler underwent a cyberattack in 2005 caused by a Zotob worm – a virus that spreads online and exploits the vulnerabilities of Windows' Plug and Play service. Despite the separation of OT and IT networks with a firewall, due to the lack of patching of Windows 2000 servers, the worm spread across the plants and stopped the operation of 13 DaimlerChrysler's sites for over an hour. This resulted in huge financial losses totalling 14 million dollars[70].

[66] See Symantec (2011) "W32.Duqu The precursor to the next Stuxnet": https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_duqu_the_precursor_to_the_next_stuxnet.pdf

[67] See Computerworld (2011) "Apparent cyberattack destroys pump at Ill. water utility": https://www.computerworld.com/article/2497351/cybercrime-hacking/apparent-cyberattack-destroys-pump-at-ill--water-utility.html

[68] See KrebsOnSecurity (2012) "FBI: Smart Meter Hacks Likely to Spread": https://krebsonsecurity.com/2012/04/fbi-smart-meter-hacks-likely-to-spread/

[69] See Michael Holloway (2015) "Stuxnet Worm Attack on Iranian Nuclear Facilities": http://large.stanford.edu/courses/2015/ph241/holloway1/

[70] See Sentryo (2017) "The Sentryo Files: Industries Vs. Cyberattacks Episode 9: Cyberattack On A Car Manufacturing Plant": https://www.sentryo.net/the-sentryo-files-daimlerchrysler-cyberattack/

ENISA

European Union Agency for Network
and Information Security
1 Vasilissis Sofias
Marousi 151 24, Attiki, Greece

Heraklion Office

Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Catalogue Number: TP-04-18-940-EN-N

1 Vasilissis Sofias Str, Maroussi 151 24, Attiki,
Greece Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu

ISBN: 978-92-9204-261-5
DOI: 978-92-9204-261-5