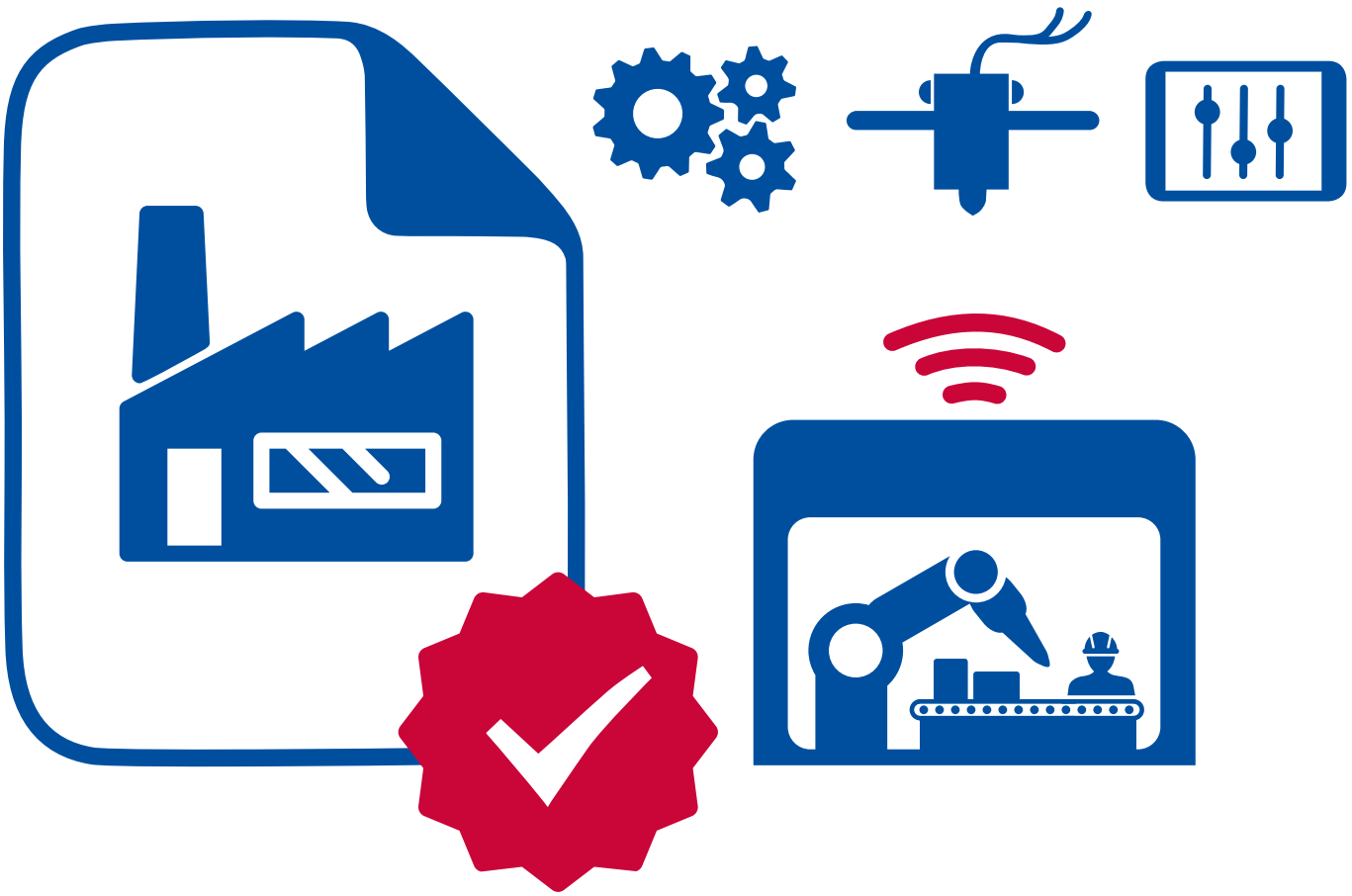
INDUSTRY 4.0 CYBERSECURITY: CHALLENGES & RECOMMENDATIONS



ENISA LISTS HIGH-LEVEL RECOMMENDATIONS TO DIFFERENT STAKEHOLDER GROUPS IN ORDER TO PROMOTE INDUSTRY 4.0 CYBERSECURITY AND FACILITATE WIDER TAKE-UP OF RELEVANT INNOVATIONS IN A SECURE MANNER.

THE EU AGENCY FOR CYBERSECURITY

1. INTRODUCTION

The ENISA study on "Good Practices for Security of IoT in the context of Smart Manufacturing"[1] focuses on 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 are 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.

Building on this work, this document provides the results of a gap analysis conducted in order to identify main challenges to the adoption of the security measures and security of Industry 4.0 and Industrial IoT. Moreover, ENISA lists high-level recommendations to different stakeholder groups in order to promote Industry 4.0 cybersecurity and facilitate wider take-up of relevant innovations in a secure manner.

This document provides the results of a gap analysis conducted in order to identify main challenges to the adoption of the security measures and security of Industry 4.0 and Industrial IoT.

The adoption of the high-level recommendations proposed by ENISA aims at contributing to the enhancement of Industry 4.0 cybersecurity across the European Union and at laying the foundations of the relevant forthcoming work, as well as at serving as a basis for future developments.

In this short paper, ENISA follows a holistic and comprehensive approach to the issues related to cybersecurity in Industry 4.0, whereby challenges and recommendations are associated with one of the following categories: People, Processes, and Technologies. This ensures consistency with the relevant ENISA study1. Additionally, recommendations are also categorised in terms the target audience groups to which they are addressed (the icons for the 5 stakeholder groups identified below may be used as a guidance, i.e. the presence of an icon next to a recommendation indicates that a particular set of recommendations is aimed at the corresponding stakeholder group).

STAKEHOLDERS GROUPS

Industry 4.0 security experts (OT and IT security)

Industry 4.0 operators (solution providers & manufacturers)

Regulators

Standardisation community

Academia and R&D bodies

1 See ENISA study on "Good Practices for Security of IoT in the context of Smart Manufacturing": https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot, November 2018

2. PEOPLE

CHALLENGE: NEED TO FOSTER AND ALIGN IT/OT SECURITY EXPERTISE AND AWARENESS

Lack of sufficient information security expertise and awareness is a major barrier that hinders the adoption of Industry 4.0 security measures. People involved in deployments of new solutions usually have only knowledge of either IT or OT security, while Industry 4.0 and Smart Manufacturing require expertise over several areas, e.g. network security, embedded systems, OT and IT security to name a few. It is becoming increasingly difficult to find qualified specialists who are well aware of security issues.

The emergence of Industry 4.0 introduces new technologies into traditional OT environments and thus people familiar with OT that work in such environments need to adapt. These people have knowledge on how to operate such environments for years and are nowadays faced with adapting the way they work and embrace new Industry 4.0 capabilities. Being unfamiliar with such technologies, employees lack new competences that are essential for secure utilization of Industry 4.0 solutions within the Smart Manufacturing systems. Such new competences would include, among others:

- operational security knowledge and skills required to monitor, prevent, and detect anomalies due to security violations;
- security aspects of new protocols used by Industry 4.0 solutions;
- skills to utilize security functionalities of the components and services (which may seem overly complicated to users if not adequately explained);
- methods of secure integration with legacy systems;
- information systems security over complex supply chains.

The emergence of Industry 4.0 introduces new technologies into traditional OT environments and thus people familiar with OT that work in such environments need to adapt.

Moreover, large manufacturing companies often are lagging in training employees who work with OT equipment and instead employ security solutions for Industry 4.0 systems without first ensuring take-up by employees. In addition, nowadays there are a limited number of state-of-the-art cybersecurity trainings dedicated to IT/OT convergence and Industry 4.0 systems and in any case, such trainings in most cases do not cover all essential aspects of these areas, are often very expensive and not always tailored to specific industry needs.

RECOMMENDATION: PROMOTE CROSS-FUNCTIONAL KNOWLEDGE ON IT AND OT SECURITY

Raising awareness on basic industrial control security as well as on the secure way for transitioning to Industry 4.0 and Smart manufacturing is of paramount importance. To address the lack of IoT and Industry 4.0 security talent, it is essential is to cultivate such knowledge both within and across organisational boundaries. Persons in charge of security within Industry 4.0 organizations should invest in state-of-the-art dedicated cybersecurity trainings that cover all necessary aspects specific to IT/OT convergence and Smart manufacturing. Lastly, trainings and courses at schools and universities (considering localisation to reach a wider audience) will further promote a better understanding of Industry 4.0 security among younger generations and thus in the long-term will contribute to raising awareness.

To promote cross-functional knowledge on IT and OT security, ENISA recommends:

- Encourage cross-functional security and safety knowledge exchange between IT and OT experts respectively.
- Launch security education and training in industries transitioning to Industry 4.0, including knowledge of state-of-the-art, best practices, methodologies and tools for secure convergence of IT and OT systems.
- Establish tailor made training courses focused on Industry 4.0 security to increase effectiveness of the training and assist OT and IT security experts to address relevant cybersecurity issues more efficiently.
- Develop competency profiles to provide IoT and Industry 4.0 specific awareness and education training for all staff.
- Introduce programs at schools and universities to address the lack of security and safety knowledge across the industry and to empower the next generation of IT and OT security experts.
- Organise cyber-culture and cyber-hygiene induction courses for OT personnel and conversely safety-culture and safety-hygiene courses for IT personnel, also involving all staff. Introduce to OT people the notion of security and to IT people the notion of safety, with special mentions to cases where the two notions may align or not.

CHALLENGE: INCOMPLETE ORGANISATIONAL POLICIES AND RELUCTANCE TO FUND SECURITY

Industry 4.0 operators, which are at various stages of Industry 4.0 adoption, often do not have appropriate governance structures in place for secure implementation of new technologies and secure maintenance of the existing ones. Defined security programs are rarely in place and in general comprehensive programs that consider security and safety in tandem are lacking. It is also often noted that security related roles and responsibilities of employees are not clearly defined and there is minimal planning to consider safety engineers within the cybersecurity ecosystem. This results in companies' lack of resilience and vulnerability to potential security breaches.

Industry 4.0 operators, which are at various stages of Industry 4.0 adoption, often do not have appropriate governance structures in place for secure implementation of new technologies and secure maintenance of the existing ones.

This is because to date cybersecurity was traditionally not perceived as a Board-level topic, since its impact on increasing revenue or optimizing cost remains generally unclear. This results in the fact that the majority of technological transformations mostly focus on increased functionality and business value rather than cybersecurity, i.e. hindering the potential negative impact of associated risks. A typical example of this is the ongoing migration of manufacturing companies towards Cloud. In general, companies decide to opt for Cloud solutions to benefit from cost efficiency and ubiquitous access to information. During this migration, security should be considered as a high priority issue –and accordingly it should play an equally important role in decision-making as cost efficiency– especially when manufacturing companies choose public clouds and thus increase the risk of exposing their data and operations, while at the same time improving their resilience.

Furthermore, it is worth highlighting that ensuring security of a system or solution, both in the context of Industry 4.0 vendors and operators, requires funding and commitment from top-level management. However, as there is no clearly discernible link to generate profits from investing in cybersecurity, it is often the case that due consideration to cybersecurity is given when a security breach directly leads to financial losses. Striking the proper balance between the costs and the need for security remains an open challenge.

RECOMMENDATION: FOSTER ECONOMIC AND ADMINISTRATIVE INCENTIVES FOR INDUSTRY 4.0 SECURITY

It is clear that lack of security has the potential to significantly affect business continuity. Industry 4.0 is no exception given the criticality of related operations and the associated impact on safety as well. In this respect, best practices for business continuity can serve as a driver for investing in cybersecurity solutions and accordingly for supporting the unobstructed operation of Industry 4.0 processes.

Investments in cybersecurity should not be driven only by fear of losing money. It is equally if not more important, for industries and organisations to not look at cybersecurity only as a cost, but to also start seeing it as an important business opportunity. Cybersecurity can be an important competitive advantage for businesses, since it leads to having secure, reliable and trustworthy products and services. Accordingly, cybersecurity is an enabler of business opportunities, not a hindering factor and certainly not another item on a checklist.

Investments in cybersecurity should not be driven only by fear of losing money. It is equally if not more important, for industries and organisations to not look at cybersecurity only as a cost, but to also start seeing it as an important business opportunity.

Nonetheless, economic and administrative stimuli are also required to incentivize investments in Industry 4.0 security, given that maturity and mentality of organisations and businesses needs to grow further when it comes to identifying the role and importance of security.

To foster economic and administrative incentives for Industry 4.0 security, ENISA recommends:

- Establish administrative structures for top-level management to discuss and exchange views with cybersecurity experts and CISOs.
- Launch funding schemes for SMEs and other bodies to support their transition to a secure Industry 4.0 ecosystem, including financial support for cooperative actions.
- Incentivize innovation and R&D activities for securing IT and OT environments, components and systems.
- Ensure a homogeneous and stable legal environment for Industry 4.0 cybersecurity to allow companies to plan long-term, sustainable business strategies including the aspect of security.
- Consider the development of certification schemes for Industry 4.0 security (taking into account the inherent particularities when defining the target of evaluation), since they promote harmonisation of the market, increase consumer trust and open up new business opportunities.
- Promote Public Private Partnerships (PPPs) focused on Industry 4.0 cybersecurity to benefit from multi-stakeholder dialogues and much needed synergies.

3. PROCESSES

CHALLENGE: LIABILITY OVER INDUSTRY 4.0 PRODUCTS' LIFECYCLE IS POORLY DEFINED

Liability for Industry 4.0 cybersecurity is an open issue (a gap also identified for most of emerging technologies) as accountability for Industry 4.0 cybersecurity incidents remains unclear. There is a large number of stakeholders involved in the supply chain and in the use lifecycle of Industry 4.0, therefore apportioning liability in the aftermath of a security incident becomes challenging as currently, only general provisions of liability are applicable.

The major difficulty in finding a clear solution for liability stems for the inherent complexity of the ecosystem. The majority of Industrial IoT devices are usually built from a large number of components manufactured by multiple vendors, in disperse locations (possibly subject to different administrative and legal constraints) and including vendors of the software embedded in the devices. The complexity of the supply chain further exacerbates relevant concerns. Apportioning liability thus remains an open challenge.

The major difficulty in finding a clear solution for liability stems for the inherent complexity of the ecosystem.

In the context of cybersecurity, an Industry 4.0 device manufacturer is broadly expected to implement functionalities in its product that would enable a proper level of security. In a similar fashion, the role of Industry 4.0 operators would see them using these available security features and perform all security upgrades provided by the manufacturer. In reality, the situation is more complicated. The long lifespan of Industry 4.0 solutions (especially in comparison to IT systems) and the financial commitments related to their long-term maintenance (e.g. software patching), both aggravate the requirements on manufactures, users and operators of such solutions. Shared ownership of connected, Industry 4.0 solutions, unclear or unspecified role assignments and lack of provisions in procurement contracts and service level agreements further complicate the issue of liability.

RECOMMENDATION: CLARIFY LIABILITY AMONG INDUSTRY 4.0 ACTORS

The Industry 4.0 paradigm introduces emerging technologies and services in manufacturing and the industrial ecosystem in general. Given the cyber-physical nature of this paradigm, security and safety are tightly intertwined. Therefore, it is of particular importance to address liability concerns not only to protect end-users and consumers of such products and services, but also to stimulate corresponding investments through a comprehensive and stable legal framework. The European Commission has recently published a Staff Working Document that sets the scene for liability issues in emerging technologies such as IoT and Artificial Intelligence[2]. This will serve as a reference point for forthcoming work.

The question of where liability may fall lies between the different and diverse stakeholders of the Industry 4.0 supply chain, such as developers, manufacturers, providers, vendors, aftermarket support operators, third party providers and the end users, to name a few.

2 See EC Staff Working Document on "Liability for emerging digital technologies": http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=51633, April 2018

To clarify liability among Industry 4.0 actors, ENISA recommends:

- Address liability issues in the context of European and national legislation and case law, especially where gaps in existing legislation are identified.
- Adjust procurement language to clarify liability among stakeholders in supply chains, e.g. specify Industry 4.0 cybersecurity requirements as part of SLAs (Service Level Agreements) and contracts during procurement.
- Assess the potential of cyber-insurance policies to transfer residual cyber risk and reduce the impact of cybersecurity incidents, for which an entity might be held liable.
- Raise awareness of end users and consumers on their rights concerning liability legislation.
- Specify in a clear manner the legal obligations of Industry 4.0 operators when it comes to liability.

CHALLENGE: FRAGMENTATION OF INDUSTRY 4.0 SECURITY TECHNICAL STANDARDS

The current landscape of standards and policy initiatives related to IoT and Industry 4.0 cybersecurity is quite large, covering security aspects at both a horizontal and vertical (application specific deployments, e.g. automotive, health, and consumer) manner. In the context of IoT, many high-level reference documents have been published, as well as baselines, good practices, checklists and general guidance[3]. Concerning connected industrial systems and manufacturing systems in particular, there are also useful sources that may serve as guidelines for relevant stakeholders[4].

However, when it comes to Industry 4.0 and Smart Manufacturing the situation is slightly different. Given the nascent nature of these areas, comprehensive initiatives to address security in a holistic manner are lagging behind. Nonetheless, it is important to refer to some notable examples that already exist (such as IEC 62443[5] or the efforts under IUNO/Industrie 4.0[6] to name a few). Accordingly, interested parties currently utilize documentation that is only partially applicable to the broad spectrum of Industry 4.0 and Smart Manufacturing.

The fragmentation of Industry 4.0 security standards and initiatives is of particular importance for the manufacturing sector. Large manufacturing companies commonly have sites spread across the world. Accordingly, the lack of uniform standardization efforts at a global level results in a situation when sites that belong to one organization cannot collaborate and share security expertise and solutions with each other, as they are subject to different schemes. Moreover, secure collaboration across companies is also hindered. At the same time, it is promising that cross-mapping initiatives have started to evolve, e.g. ENISA Baseline Security Recommendations for IoT[7], UK Government Code of Practice for Consumer IoT Security[8], NIST Internal Report 8228[9]. Whereas, such initiatives contribute to increasing homogeneity in the area of IoT security, further work to expand them in the Industry 4.0 ecosystem is desirable[10].

The fragmentation of Industry 4.0 security standards and initiatives is of particular importance for the manufacturing sector. Large manufacturing companies commonly have sites spread across the world.

3 ENISA online tool for IoT and Smart Infrastructures Security maintains a continuously updated list of relevant efforts mapped against the ENISA IoT Security Baseline: https://www.enisa.europa.eu/iot-tool

4 See Annex C of ENISA study on "Good Practices for Security of IoT in the context of Smart Manufacturing": https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot

5 See IEC 62443 family of standards at: https://www.iec.ch/index.htm

6 See IUNO project homepage at: https://iuno-projekt.de/

7 See ENISA "Baseline IoT Security Recommendations" study at: https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot, October 2017

8 See Code of Practice for Consumer IoT Security at: https://www.gov.uk/government/collections/secure-by-design

9 See NIST Internal Report 8228 (Draft) Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks at: https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8228-draft.pdf

10 See Annex B of ENISA study on "Good Practices for Security of IoT in the context of Smart Manufacturing" for a relevant effort: https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot

Moreover, there is a need for systematic recipes for implementing the recommendations proposed in Industry 4.0 security standards and guidelines. Current lack of pragmatic ways to achieve this objective is leading to significant diversities of systems and services security in the manufacturing sector.

RECOMMENDATION: HARMONIZE EFFORTS ON INDUSTRY 4.0 SECURITY STANDARDS

To address the fragmentation of current technical standards for Industry 4.0 cybersecurity, it is necessary to harmonize relevant efforts wherever there are significant gaps and overlaps. One option towards this direction involves the introduction of baseline standards dedicated to Industry 4.0 security. Along these lines, it is encouraging that such efforts have recently emerged in the context of IoT[11].

Alternatively, it is beneficial to explore initiatives and guidelines that map security standards from many different sources to provide a complete point of reference and thus ensure all necessary security controls are considered. At any rate, standardization activities should be based on the input of the different actors of the Industry 4.0 ecosystem to ensure fair and comprehensive representation of relevant requirements and eventually wider adoption.

To harmonize efforts on Industry 4.0 security standards, ENISA recommends:

- Launch standardization activities addressing the entire spectrum of Industry 4.0 security.
- Conduct analyses on current standards for Industry 4.0 security to examine potential gaps, i.e. whether existing standards adequately address Industry 4.0 security requirements[12].
- Promote multi-stakeholder dialogues between Industry 4.0 actors to ensure consensus in the development of relevant technical standards.
- Develop and maintain mapping schemes between standardization activities (such as the ones by ENISA[2], NIST[8], UK DCMS[7]) to explore cross-standard commonalities and synergies.

CHALLENGE: SUPPLY CHAIN MANAGEMENT COMPLEXITY

Supply chain management in the manufacturing sector is a well-known challenge acknowledged by the majority of involved actors and stakeholders.

Supply chain management in the manufacturing sector is a well-known challenge acknowledged by the majority of involved actors and stakeholders. Although the supply chain characteristics depend on the company (for example, a large corporation may be able to control a significant part of the supply chain as it manufacturers its own components), typically companies rely on others to take over part of this work. Recently, the situation has become even more complicated as Smart Manufacturing introduced new capabilities (End-to-End visibility, predictive analysis, automation and data-driven decision-making) that have an additional impact on the supply chain. Accordingly, supply chains have become more dynamic, flexible, interdependent and demanding in terms of performance. However, increased inter-dependence of supply chains results in broader impact caused by existing security risks and introduction of new ones.

Scalability is one of the most significant concerns, as a large number of people, organizations and processes are involved. In such cases, companies need to make numerous decisions (e.g. select vendors, agree on methods of collaboration, establish organizational processes),

11 See ETSI TS 103 645 "Cyber Security for Consumer Internet of Things": https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/01.01.01_60/ts_103645v010101p.pdf, February 2019

12 See relevant ENISA study on "IoT Security Standards Gap Analysis": https://www.enisa.europa.eu/publications/iot-security-standards-gap-analysis, January 2019

on which the security of the final product will depend. Having an effective control over the supply chain is essential, as not being able to track every component to its source further erodes confidence in a product's security. The notion of trustworthiness is also noteworthy, since companies need to delineate the amount of trust they place on their partners as well as to manage any residual risks.

The plethora of supply chain actors, who may be subject to different national legislative frameworks, also means that security incidents may occur at various tiers and stages. Such incidents may be related to the exchange of goods, services or information and consequently may result in a propagation of errors and risks across the whole supply chain[13]. Detecting the source of a problem becomes extremely challenging and possible cascade effects could be very hard to predict. At any rate, it is evident that a security breach at any point of the supply chain would have a negative impact on the final product's security.

The complexity of the supply chain exacerbates the utilization of security standards and solutions that are applicable across the different actors involved. Therefore, it is often that diverse requirements apply to different actors and processes making this an even more cumbersome issue.

RECOMMENDATION: SECURE SUPPLY CHAIN MANAGEMENT PROCESSES

Supply chain management in the manufacturing sector is a well-known challenge acknowledged by the majority of involved actors and stakeholders.

Cybersecurity is a shared responsibility. When we talk about IoT and Industry 4.0, with complex supply chains and several actors involved, this becomes an even more pressing reality. In securing Industry 4.0, collaboration is everything. There are many players, many interdependencies, and many facets. Trust is the root of a secure supply chain, since the amount of trust that an organisation places on another that will eventually feed into the risk assessment process and the introduction of appropriate security controls.

Addressing the complexity and the risks involved in large supply chains is a matter of identifying how much trust one can afford to place, and what residual risks it can accept in order to define appropriate levels of security.

Another important consideration involves holistic management of security across the supply chain. Securing the interaction between two entities is not adequate, when such an interaction is only part of a longer supply chain. End-to-end security is a prerequisite for Industry 4.0 to succeed.

To fully understand and secure supply chain management processes, ENISA recommends:

- Conduct risk assessment at periodic intervals to identify potential Industry 4.0 supply chain risks.
- Define amount of trust placed on each supplier and review this definition at periodic intervals, also considering cyber threat intelligence to monitor ongoing and emerging threat landscape.
- Rely on suppliers whose products comply with recognised security standards and certification schemes.
- Apply trust models instead of concrete technical security controls (e.g. certificates).
- Ensure security of digital supply chain by following secure software development lifecycle for Industry 4.0 products and services.

13 See ENISA Infonote on Supply Chain Attacks: https://www.enisa.europa.eu/publications/info-notes/supply-chain-attacks, August 2017

4. TECHNOLOGY

CHALLENGE: INTEROPERABILITY OF INDUSTRY 4.0 DEVICES, PLATFORMS AND FRAMEWORKS

With the introduction and integration of Industry 4.0 devices, platforms and frameworks to existing systems comes the issue of interoperability. In industrial environments, securing interconnectivity between diverse devices is often challenging, especially when considering devices that are long out of support. It is thus essential to promote secure solutions for ensuring smooth integration of Industry 4.0 devices with legacy systems and among each other, e.g. gateways to ensure transparent communication in the case of different networking or other protocols.

Additionally, lack of interoperability relates to dedicated, proprietary protocols that are in use by Industry 4.0 devices. In case of utilization of devices and platforms from different vendors, ensuring interoperability may not always be possible. Ensuring interoperability between devices / platforms is not only about seamless operation, but also about security. It is therefore essential to address the problem of proprietary protocols that are not always secure and adopt common frameworks in order to improve functionality and security of Industry 4.0 solutions.

Lastly, the notion of interoperability does not only refer to communication protocols and different application frameworks. In the complex supply chains of Industry 4.0, the notion of security interoperability emerges, meaning that it is very challenging to ensure a common, baseline of security across platforms, devices, protocols and frameworks. The weakest link of the chain can have detrimental effects on the entire chain, therefore ensuring a unifying common cybersecurity layer across all these elements is a very challenging issue.

With the introduction and integration of Industry 4.0 devices, platforms and frameworks to existing systems comes the issue of interoperability.

RECOMMENDATION: ESTABLISH INDUSTRY 4.0 BASELINES FOR SECURITY INTEROPERABILITY

The challenge of security interoperability is pertinent to the Industry 4.0 ecosystem especially considering integration with legacy systems. Most of the interoperability and security challenges derive from the interconnection of devices (both critical and non-critical manufacturing components) from different manufacturers and different communication protocols. Ensuring and fostering interoperability of Industry 4.0 devices, platforms and frameworks, as well as security practices is therefore essential.

To establish Industry 4.0 baselines for security interoperability, ENISA recommends:

- Encourage the use of interoperability frameworks[14] that promote a common security language and use of protocols for Industry 4.0 components.
- Identify specific security levels between cooperation partners and companies across the supply chain to cover all three cybersecurity facets, namely people, processes and technologies.
- Promote open and accessible interoperability laboratories and testbeds for security.

14 Notable examples in this direction involve the NIST Cyber Security Framework and IEC 62541 (OPC UA).

CHALLENGE: TECHNICAL CONSTRAINTS HAMPERING SECURITY IN INDUSTRY 4.0 AND SMART MANUFACTURING

Difficulties in ensuring security in Industry 4.0 result also from lack of technical capabilities of connected industrial devices and systems, especially considering integration with legacy infrastructures. Constraints in embedded systems brings about a major challenge, especially when referring to low end ICSs and PLCs, as they face many issues with a direct impact on their security. Indicatively one can consider the following limitations:

- Limited processing capabilities and the need to ensure long time of operation while maintaining a suitable size and competitive price of the device considerably affects implementation of comprehensive security features in the design phase.
- No consideration for fundamental protection mechanisms when designing Industry 4.0 devices adversely influences their security. Patching and software updates over-the-air are in most cases not feasible solutions when it comes to low-end devices, as they do not support such functionality.
- Lack of more advanced security measures such as encryption or authentication for example, lower the protection level of devices that are closest to the industrial process. A quite common approach of only securing the network is insufficient, e.g. if an attacker breaks into the network, the devices are vulnerable to attacks.

Difficulties in ensuring security in Industry 4.0 result also from lack of technical capabilities of connected industrial devices and systems, especially considering integration with legacy infrastructures.

Finally, while considering gaps related to limited technical capabilities, it is worth mentioning the fact that dedicated cybersecurity tools for Industry 4.0 systems are generally too few or too expensive. Tools for network monitoring, automatic asset discovery, and configuration and change management at the OT environment have increased the security level of such systems and have raised their availability. Such tools however are not yet fully prepared for handling new Industry 4.0 devices, thus creating a gap in terms of security. Addressing such challenging issues by developing security solutions adapted for the Industry 4.0 world is needed.

RECOMMENDATION: APPLY TECHNICAL MEASURES TO ENSURE INDUSTRY 4.0 SECURITY

Given the complexity and scalability of the ecosystem, there is no one size fits all solution for IoT and Industry 4.0 security. It is a matter of combining solutions and ensuring that these solutions cater for flexibility and extensibility without sacrificing security, also taking into account the factor of usability. The notion of flexibility in this context also refers to the economics of cybersecurity, namely that adopted solutions should come as a result of a systemic cost-benefit analysis, where evidently the benefit is that of secure and reliable products and services.

Identifying baseline security recommendations for Industry 4.0 components, services and processes based on risk analysis is a first step to approach a solution to the challenging technical constraints of this domain. ENISA has published relevant guidelines from ENISA both horizontally for the IoT ecosystem6, but also in the vertical sector of Industry 4.01.

In terms of applying technical measures to ensure Industry 4.0 security, ENISA recommends:

- Define a security architecture for Industry 4.0 taking into account a methodological risk assessment.
- Apply principles of security-by-design and privacy-by-design and by-default for all Industry 4.0 components, devices, services, protocols, communications and processes.
- Assess the maturity of implemented cybersecurity solutions periodically, also considering cyber threat intelligence to monitor ongoing and emerging threat landscape.
- Monitor the cybersecurity posture of industries concerning Industry 4.0 deployments, also catering for legacy systems and infrastructures.
- Enable continuous updatability & upgradability of Industry 4.0 components and services throughout their lifecycle, with failsafe and effective operation as guiding principle.
- Keep track of developments in cybersecurity standards and best practices for Industry 4.0 cybersecurity and ensure proper implementation of relevant security measures subject to risk assessment also considering removing unnecessary functionality.

RECOMMENDATIONS INDEX

 **INDUSTRY 4.0 SECURITY EXPERTS (OT AND IT SECURITY)**	Promote cross-functional knowledge on IT and OT security Secure supply chain management processes Establish Industry 4.0 baselines for security interoperability Apply technical measures to ensure Industry 4.0 security
 **INDUSTRY 4.0 OPERATORS (SOLUTION PROVIDERS & MANUFACTURERS)**	Promote cross-functional knowledge on IT and OT security Clarify liability among Industry 4.0 actors Foster economic and administrative incentives for Industry 4.0 security Secure supply chain management processes Establish Industry 4.0 baselines for security interoperability Apply technical measures to ensure Industry 4.0 security
 **REGULATORS**	Clarify liability among Industry 4.0 actors Foster economic and administrative incentives for Industry 4.0 security Harmonize efforts on Industry 4.0 security standards Establish Industry 4.0 baselines for security interoperability
 **STANDARDISATION COMMUNITY**	Harmonize efforts on Industry 4.0 security standards Establish Industry 4.0 baselines for security interoperability
 **ACADEMIA AND R&D BODIES**	Promote cross-functional knowledge on IT and OT security Establish Industry 4.0 baselines for security interoperability

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 EU citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists 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 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 media enquires about this paper, please use press@enisa.europa.eu.

LEGAL NOTICE

Notice must be taken that this publication represents the views and interpretations of ENISA, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to the Regulation (EU) No 526/2013. This publication does not necessarily represent state-of the-art and ENISA may update it from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

ACKNOWLEDGEMENTS

ENISA would like to thank all the experts that have been acknowledged in the ENISA study "Good practices for security of IoT in the context of Smart Manufacturing" (November 2018) for their input and feedback in this publication.

AUTHORS

Dr. Apostolos Malatras
Christina Skouloudi
Aggelos Koukounas

Catalogue number: TP-03-19-407-EN-N
ISBN: 978-92-9204-293-6
DOI: 10.2824/143986

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