GUIDELINES FOR SECURING THE INTERNET OF THINGS

Secure supply chain for IoT

NOVEMBER 2020

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. For more information, visit www.enisa.europa.eu.

AUTHORS

Christina Skouloudi, Apostolos Malatras, Rossen Naydenov

CONTACT

For contacting the authors please use iot-security@enisa.europa.eu.
For media enquiries about this paper, please use press@enisa.europa.eu.

Cédric LEVY-BENCHETON - Cetome

Patrick Lozada - TIA

Maor Vermucht - Vdoo

Andrei Costin - binare.io

Jens Mehrfeld - BSI

Alexios Lekidis - Intracom Telecom

Justin Salerno, Jeff Schutt – CISCO

Vytautas Butrimas - NATO Energy Security Center of Excellence

Alessandro Cosenza - Bticino S.p.A

LEGAL NOTICE

COPYRIGHT NOTICE

TABLE OF CONTENTS

EXECUTIVE SUMMARY

This ENISA study defines guidelines for securing the supply chain for IoT. Establishing secure supply chain across the IoT ecosystem is a fundamental building block for IoT security. Supply chain lays the foundation of IoT devices security, because the majority of these devices are comprised from a multitude of components from different suppliers (both hardware and software). At the same time, supply chains present a weak link for cybersecurity because organisations cannot always control the security measures taken by supply chain partners.

Taking a step back and looking into the entire supply chain of IoT products and services, ENISA with the input of IoT experts created security guidelines for the whole lifespan: from requirements and design, to end use delivery and maintenance, as well as disposal. The motivation is clear: security is not only about the end product, but also about the processes to be followed to develop the product.

ENISA has long argued for security by design and by default to be weaved into digital products . Setting specific security guidelines for IoT supply chain security is of paramount importance to holistically approach the issue of IoT security. IoT security needs to be considered at all stages of the supply chain, from the early conceptual design to the end user delivery and maintenance. It is therefore important to analyse the relevant supply chain security threats and accordingly to set forward security measures and guidelines that help avoiding the risks that affect trustworthiness of the IoT supply chain.

The study is developed to help IoT manufacturers, developers, integrators and all stakeholders that are involved to the supply chain of IoT to make better security decisions when building, deploying, or assessing IoT technologies. This study builds up on existing ENISA studies on IoT security, the baseline IoT security recommendations and the secure software development lifecycle for IoT, and thus should be considered as complementary to the work that has been produced from ENISA the previous years. It aims to serve as a point of reference for secure supply chain for IoT.

This ENISA study aspires to address cybersecurity challenges related to the security of the supply chain for IoT. It analyses the different stages of the IoT supply chain and explores all the important security considerations to be taken into account in each stage.

Key guidelines of the report conclude on the need to:

- Forge better relationships between actors
- Further cultivate cybersecurity expertise
- Adopt security by design principles
- Take a comprehensive and explicit approach to security
- Leverage existing standards and good practices

1. INTRODUCTION

The heterogeneous nature of the IoT ecosystem and its critical use make security an essential aspect that must be taken care of. Although most of the IoT hardware and software vendors consider and apply security measures during the design and development of their products and services, security implications[1] can be found at the stages of the supply chain where IoT solutions are produced.

Any organisation that deals with physical goods understands the concept of the supply chain. Supply chain activities transform natural resources, raw materials, software, and components into a finished IoT product or service that is delivered to the end customer. Concepts like supply chain optimisation and supply chain risk management need to be considered when developing IoT solutions[2]. Understanding supply chains is a critical factor in business success and in security and quality of end-products. ENISA has been advocating for security and privacy by design and by default. The wide range of heterogeneous actors and IoT assets involved in the IoT supply chain introduce new challenges and aspects that are reflected in this study, along with a set of good practices and guidelines to be applied in the different phases of the supply chain.

Although IoT is being used as a key enabling technology to secure the supply chain of several industries (e.g. by tracking of assets, raw materials, supplies, etc.), the supply chain security for the IoT itself must be ensured. Security in the IoT needs to be considered at all stages of the supply chain, from the early conceptual design to the end user delivery and maintenance or even repurposing.

The IoT threat landscape is highly complex and has been analysed exhaustively by ENISA studies that cover the specific elements of the IoT ecosystem (e.g. embedded devices, IoT platforms, network components). Relevant studies published by ENISA include:

- Supply Chain Integrity: An overview of the ICT supply chain risks and challenges, and vision for the way forward (2015).
- Baseline Security Recommendations for IoT (2017).
- Good Practices for Security of Internet of Things in the context of Smart Manufacturing (2018).
- Good Practices for Security of IoT - Secure Software Development Lifecycle (2019).
- Industry 4.0 - Cybersecurity Challenges and Recommendations (2019).

1.1 OBJECTIVES

This ENISA study aspires to address cybersecurity challenges related to the security of the supply chain for IoT. The main objectives of this study aim at identifying challenges, threats, security considerations and good practices for ensuring cybersecurity across the different stages of the IoT supply chain.

---

[1] Boyens, Jon M. 2020. "Key Practices in Cyber Supply Chain Risk Management: Observations from Industry." Preprint. https://doi.org/10.6028/NIST.IR.8276-draft
[2] Cascella, Roberto. 2019. "Challenges of Cybersecurity Certification and Supply Chain Management." ECSO - EUNITY Workshop, January 24.

To this end, the following objectives have been set:

- Analyse the different IoT supply chain stages and underline key cybersecurity challenges in each one.
- Identify key cybersecurity threats targeting the IoT supply chain.
- Underline main challenges for employing security across the IoT supply chain.
- Identify security measures and map them to threats and supply chain stages.
- Develop guidelines that may support IoT stakeholders securing the IoT supply chain.

1.2 SCOPE

The scope of the study includes all the stages of the IoT supply chain, defined as a holistic system of organizations, people, technology, processes, information, and other physical and virtual resources involved in the whole lifespan of any IoT product or service, from the conception to the end customer supply and the end of the product life cycle.

The following list includes the IoT supply chain stages that were considered within the scope. Detailed descriptions of each stage are provided in later sections.

- Product design
- Semiconductor fabrication
- Component manufacturing
- IoT Platform development
- Component assembly and embedded software
- Device programming
- Distribution and logistics
- Service provisioning and end-user operation
- Technical support and maintenance
- Device recovery and repurpose

1.3 TARGET AUDIENCE

This study defines good practices for security of IoT, focusing on the supply chain. Given the heterogeneous phases involved in the supply chain and the complexity of the IoT ecosystem, the target audience of this study comprises the following profiles:

- IoT software developers and manufacturers.
- Information security experts.
- IT/Security solutions architects.
- Chief Information Security Officers (CISOs).
- Critical Information Infrastructure Protection (CIIP) experts.
- Project managers.
- Procurement teams.

1.4 METHODOLOGY

This ENISA study was carried out using a five-step methodological approach.

1. **Scope definition and identification of experts:** The first step was to establish the scope of the study and to pinpoint the main topics to be considered. A concurrent activity involved identifying the relevant IoT subject matter experts to contribute to this study. The experts (members of ENISA informal expert groups on IoTSec and EICS) provided input and expertise in relation to the objectives of this report.
2. **Desktop research:** Extensive research of relevant efforts to gather information on securing the IoT supply chain. The identified documents included existing good

practices, publications, standards and other initiatives on the topics related to the objectives of the report. This served as the foundations and support for the analysis of the threats and for the development of the security measures.

3. **Questionnaire and interviews with identified experts:** ENISA reached out to the identified experts in order to collect information and get their point of view. To this end, an online questionnaire covering various security aspects, such as critical assets, key threats targeting IoT supply chain and awareness with respect to supply chain standards and guidelines, was developed. The identified experts completed the questionnaire, and interviews were conducted with experts to collect additional valuable inputs to prepare the report.

4. **Analysis and development:** The results from the desktop research, online questionnaire and the interviews were analysed to align them with the objectives of the report, developing the asset and threat taxonomies. This helped to identify the attack scenarios, as well as the IoT supply chain security measures. This led to the development of the first draft of this report.

5. **Report write-up and validation:** ENISA shared the draft of the report with its relevant stakeholder communities and reference groups for review. The draft validation will be done in parallel with the continuous improvement of the report. The final report will be shared again to be reviewed at the end of its write up.

1.5 STRUCTURE OF THE DOCUMENT

This report is structured as follows:

- **Chapter 1 - Introduction:** provides introductory information to the report and introduces the scope, objectives, and the methodology followed.
- **Chapter 2 – Overview of IoT supply chain:** presents the different phases and formal definitions of the IoT supply chain. It also discusses cybersecurity considerations in the different phases; these considerations are expanded in the following chapters.
- **Chapter 3 –Threat taxonomy:** identifies the security threats affecting IoT supply chain and details some examples of potential attack scenarios.
- **Chapter 4 – Good practices for security of IoT supply chain:** lists and descriptions of good practices and security measures to secure the IoT supply chain.
- **Chapter 5 – Guidelines and conclusions:** once the main conclusions of the report had been laid out in the format of good practices in the previous chapter, a series of written guidelines are presented to ensure a comprehensive understanding of the security in the IoT supply chain.

2. OVERVIEW OF IOT SUPPLY CHAIN

2.1 SUPPLY CHAIN REFERENCE MODEL FOR IOT

The IoT supply chain includes the actors, processes and assets that participate in the realization (e.g. development, design, maintenance, patch management) of any IoT device.

This study considers the supply chain for IoT is composed of two main aspects: the physical aspect and the logic aspect. The physical supply chain relates to all the physical objects (e.g. devices, electronic components, appliances) moved through the supply chain phases, as well as the associated manual processes (e.g. manual assembly, distribution processes). The logic aspect of the supply chain for IoT is associated with the software development and deployment, network-based communications, and virtual interactions between the IoT objects and the supply chain stakeholders.

IoT supply chain risks, and more generally IT supply chain risks, are associated with an organisation's decreased visibility into, and understanding of, how the technology they employ in their product or solution is developed, integrated, and deployed[3]. An overview of the IoT supply chain is provided , presenting all its different stages with a detailed mapping of them that can be found after the following subsections. This aims to give an approximation of the stages sequence and the interactions between actors to identify where the security concerns might arise.

Although the stage layers are presented as being separated, it should be taken into account that sometimes they are treated as a single entity due to project constraints or other business realities.

---

[3] National Cyber Security Centre. 2018. "Supply Chain Security Guidance." National Cyber Security Centre.
https://www.ncsc.gov.uk/collection/supply-chain-security

Figure 1: Supply Chain Reference Model for IoT

2.1.1 Conceptual Phase

During this phase, the products and services are conceptually designed. This includes both software and hardware units, as well as other services that may be involved. This early stage is important to define and establish the basic security foundations that will be part of the requirements during the subsequent stages in the supply chain. Security at the design phase is critical as some cost-driven decisions or mistakes at this stage may result in security flaws in the final product.

This phase contains the design of security models. Physical and digital assets are inextricably linked in the IoT domain—a security model for the IoT supply chain should merge both physical safety and digital security.

Requirements are also specified at the conceptual stage. One of the main challenges is the harmonization of the different disciplines (e.g. hardware engineering, security engineering, business) to achieve proper security in the IoT product while properly considering all the requirements. One other challenge is the understanding the target environment. For 'general purpose' devices there is likely to be a wide range of target environments, all exhibiting different risks and therefore expressing different risk appetite.

Finally, it should be noted that the investment of resources in the conceptual and development phases tends to contribute to minimize the cost of making an error in later stages.

2.1.2 Development Phase

Broadly speaking the Development Phase consists of a wide range of tasks that span from semiconductor fabrication to firmware programming and whose main objective is producing a physical device ready to ship to customers. Development of software services and platforms required for the operation and deployment of IoT devices are also included in this phase. This is one of the most critical phases as most of the risks and threats arise from poor decisions, omissions or mistakes at this point.

As is the case with the conceptual phase, the lack of visibility of the development-related differences (e.g. timelines, needs) between the different teams (e.g. software, security) can have a significant and negative impact on security.

On a deeper level, a typical IoT device will go through many steps during the Development Phase. Those steps can roughly be categorized under Hardware and Software, with the former consisting mainly in semiconductor fabrication (according to design guidelines), PCB manufacturing, component integration and functional testing; while the latter involves components like on-chip microcode, operating systems, middleware, third-party libraries, cloud services integration and several development tools.

The number of actors involved in this stage can be potentially very high. For example, semiconductor manufacturers, PCB integrators, security engineers, device assembly and packaging and developers (micro-code, firmware, operating systems, middleware, libraries).

2.1.3 Production Phase

This phase involves mass production, distribution, and logistics. A significant percentage of IoT devices use multiple units from different vendors and thus require a wide, and often complex, supply chain. This usually leads to a multi-faceted logistic challenge, where keeping track of all the stages and sources is not an easy task.

This phase is linked with the support and retirement phases, as the challenges that are involved in the initial distribution resurface when products have to be retrieved due to malfunction or to be disposed of.

The IoT supply chain production phase may be defined as the effort needed to efficiently and securely deliver while keeping track of all the units in IoT devices. Typically, this involves several different actors: shipping, warehousing, inventory management, delivery fleet operation, packaging, handling and customer support, among others.

2.1.4 Utilisation Phase

Although it depends greatly on the type of device and services provided, the Utilisation Phase contains all those tasks required to get the device up and running at the customer final location.

For a typical device this usually involves tasks ranging from delivery to the customer or retailers, physical installation at the operating location, device initial set-up, establishing secure user credentials both at device level and remote services, pairing with mobile devices, data collection/sharing agreements up to cloud/3rd-party services.

As is the case in the other phases, the complexities of the supply chain require a significant number of potential actors to be involved in this phase. For example, logistics companies to

transport IoT products, retailers, technicians to participate in the deployment process or cloud service providers that offer the services that serve as building blocks of IoT platforms. These actors are usually also involved in the following support and retirement phases.

2.1.5 Support Phase

When thinking about the support phase in the life cycle of a product, we always tend to think in repairing damages or fixing issues. From the perspective of the supply chain in IoT devices this often means repairing or replacing damaged units. The IoT devices are very susceptible to damage and malfunctions, as such the IoT suppliers usually have a good size team working as support of their product, that work closely with the developers and users if needed.

But there is another very important part of the support phase that revolves around the constant supervision of the unit's security. This part is mainly divided between maintaining updates[4] for the devices (firmware, software and libraries) and remote support.

For this phase of the supply chain, the report is focusing on the continuous prevention aspect.The majority of the IoT devices are widespread and usually have various components with different origins. This makes it even harder to ensure the security of the devices, and even presents threats to the functionality of the product. This is why a lot of security measures and good practices have been centred around this phase, using different technologies and standards to ensure a correct support of the IoT devices through its life cycle.

2.1.6 Retirement Phase

The final phase of a product consists in a series of steps to ensure that the disposal of the IoT device is done securely. One of the key aspects of this phase is the secure removal of the information in the device[5].

If needed, another step in the disposal of a device is its physical destruction. This presents challenges not only in the cyber-security department but also logistics and environmental concerns, as electronics wastes involve a great deal of contamination problems. One of these problems is the scarcity of some of the materials used in creating them, so an important part of the retirement process is the recycling of the devices.

So, the retirement process can be summarized as the recycling of the devices in economically feasible and environmentally friendly ways while adhering to security and privacy standards.

Another important breach in security is added when the device is not completely taken out of circulation but instead is repurposed or refurbished. When reused, there is again a strong need for information erasing, but also extra measures <u>must</u> be taken to ensure that the product can fit into its new use.

2.2 DESCRIPTION OF IOT SUPPLY CHAIN STAGES

This section contains brief descriptions of each of the stages in the IoT supply chain. All of them are relevant from a security standpoint and should be considered in the security process.

2.2.1 Product Design

The first stage includes the generation of the required design resources for both hardware and software components before proceeding to fabrication and development stages. This process

---

[4] Kissel, Richard, Andrew Regenscheid, Matthew Scholl, and Kevin Stine. 2014. "Guidelines for Media Sanitization." NIST SP 800-88r1. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-88r1
[5] Kyung Lee, Teddy. 2020. "VIA PUF Technology as a Root of Trust in IoT Supply Chain." Global Semiconductor Alliance (blog). 2020.

shall take into account security features to support a secure supply chain (e.g. secure root of trust, process isolation for trusted software). The design of IoT products tends to be complex due to the highly coupled nature of the relationship between hardware and software—these products usually have restrictive constraints (e.g. cost, size) and are based on hardware platforms specifically tailored to the scenario.

Design tasks in the software domain include, for example, gathering functional and non-functional requirements, producing initial versions of threat models, designing architectures, defining the technology stack and developing small-scale proof-of-concepts to assess viability. On the other hand, hardware requires producing schematics for PCBs (Printed Circuit Boards) and mechanical elements using ECAD (Electronic Computer-Aided Design) and MCAD (Mechanical Computer-Aided Design) tools. Schematics can then be validated using simulation processes (e.g. thermal).

The product design phase is significantly challenging due to the fact that is forces designers to think long-term and consider multiple future issues and possibilities (e.g. how to deal with remote management of credentials when a root of trust is implemented). On the other hand, it is comparatively easy to verify.

2.2.2 Semiconductor Fabrication

Developments in the semiconductor fabrication field have played a major role in the recent growth of the IoT domain, increasing the capabilities and computational resources of devices with low power consumption and small form factor requirements.

The fabrication stage includes the chemical processes involved in transforming raw semiconductor materials into silicon wafers; the production of the masks containing patterns that will be transferred to the silicon wafers after being irradiated with UV light; and what is commonly known as the IC (Integrated Circuit) frontend process. Two distinct and consecutive steps can be identified in this process: FEOL (Front End-Of-Line) refers to the first part where individual electrical components (e.g. transistors, capacitors) are formed on the silicon, while BEOL (Back End-Of-Line) is the second part where interconnections are formed between components.

With the shortage of materials being an increasingly pressing issue, the competition for the access to resources has intensified. Additionally, it should be noted that the separation lines between fabrication and manufacturing phases are often blurred. Actors such as foundries can sometimes offer services beyond their expected scope, benefiting from a stronger integration between steps in the semiconductor chain to optimize costs. The Semiconductor Fabrication and Component Manufacturing stages could therefore be considered as a single unit depending on the specific case. Furthermore, another reasonable model of the IoT supply chain could even group the fabrication and manufacturing stages under the initial design phase due to their low-level nature.

Not all IoT projects require the design and fabrication of ad-hoc ICs; many products can be based on off-the-shelf chips to avoid dealing with the high barriers and costs of entry of low-level semiconductor fabrication (which is only cost-efficient on projects with a high volume of devices).

Unlike the product design stage, the fabrication and manufacturing stages tend to be more difficult to verify—this has the side effect of increasing challenges from a security perspective.

2.2.3 Component Manufacturing

This stage is comprised of the tasks that are necessary to arrive at a production-ready IC after the electrical components and interconnections are formed on the wafers during the Semiconductor Fabrication stage. These steps include separation of each individual die from the silicon wafer, and packaging of the die into the final physical IC container for protection and usage. Extensive testing is also involved[6] to validate and ensure that ICs meet the performance requirements.

PCB manufacturing is another common task that is included in this stage. Unlike ad-hoc ICs, many IoT projects require the design of custom PCBs that serve as an interconnection platform for components such as microcontrollers, FPGAs or physical connectors. The PCB only provides the substrate and interconnection tracks, the actual components are assembled on the next stage.

2.2.4 Component & Embedded Software Assembly

In this stage electronic components are mounted and soldered on the PCBs. This process may be manual or automated, depending on the capabilities of the assembly pipeline and the type of the components—through-hole components tend to be manually soldered, while SMDs (Surface-Mount Devices) can be automatically placed by specialized machinery.

Software modules or pieces of information that are integral to the units and are not directly related to the actual IoT application logic (developed in later stages) are loaded and initialized in this phase. Two distinct types of initialization may be identified: one type includes modules that are the same for the entire range of devices (e.g. bootloader, firmware); the other includes modules that change on a per device basis (e.g. device ID). It should be noted that this is logically separated from the setup that takes part during the service provision stage.

Finally, devices are integrated into their physical enclosures and packaged for distribution to end users or intermediary VARs (Value-Added Resellers).

Security challenges in this stage arise from the combinations of the same software running with different configurations in different hardware platforms. The impact of different hardware platforms in software safety and reliability needs to be evaluated, although this is a hard process.

2.2.5 Device Programming

This stage can be defined as all the tasks geared towards writing, testing and deploying functional software on all the components of an IoT device. Depending on the complexity of the device and the number of different components these tasks might require developing software at several layers: low-level firmware (e.g. bootloader)[7], drivers, networking/communication stacks, Operating System, Middleware (e.g. web server), user GUI.

This stage can potentially span along most of the lifecycle of the product as part of the development team is usually involved in the support phase: fixing detected flaws, implementing new features or simply working alongside the maintenance team in keeping online/cloud services fully operational.

---

[6] Fagan, Michael, Katerina N Megas, Karen Scarfone, and Matthew Smith. 2020. "Foundational Cybersecurity Activities for IoT Device Manufacturers." NIST IR 8259. Gaithersburg, MD: National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8259
[7] Trusted Computing Group. 2020. "TCG Guidance for Secure Update of Software and Firmware on Embedded Systems." Version 1.0 Revision 72.

2.2.6 IoT Platform Development

An IoT platform is comprised of all the services that are required for the operation and support of a fleet of IoT devices. These services tend to be centralized in nature, providing intelligence and capabilities that cannot be implemented in a local fashion in the IoT devices (e.g. due to constrained resources). The following list contains some examples of IoT platform services:

- Identification and authorization services.
- Streaming platforms for the ingestion of data flows originated on the IoT devices. Processing pipelines are usually included to clean, analyse and persist the data.
- Services for the provisioning of the environment and configuration of IoT devices.
- APIs for the exposition of historical data or events.
- Gateways or bridges for the adaptation and translation of protocols.

Tasks involved in this stage are commonly a combination of the development of ad-hoc projects tailored for the specific context of use, and the integration of third-party APIs and services—whether exposed on the cloud following the SaaS model (Software as a Service) or installed in private servers. It is important to note that the endorsement of third-party software is a significant security challenge for all stages related to software development.

2.2.7 Distribution & Logistics

From the end-user point of view the classical definition of distribution and logistics is about how to make the goods reach the customer quickly and reliably. However, most IoT devices use many components and services from different vendors and so require a wide, and often complex, supply chain. This usually leads to a multi-faceted logistic challenge, where keeping track of all the stages is not an easy task.

With this in mind we can define IoT supply chain distribution and logistics as the effort needed to efficiently and securely deliver while keeping track of all the components in IoT devices[8]. Typically, this involves several different tasks and actors: shipping, warehousing, inventory management, delivery fleet operation, packaging and handling among others.

2.2.8 Service Provision & End-User Operation

This term is usually applied to the initial steps to be taken in order to bring an IoT device to a fully operational state at the customer site (once the physical installation is completed). This usually requires device initialization, user/application account set-up, networking set-up, cloud services enrolment and any further custom/ad-hoc device configuration. It is one of the critical stages at which proper security practices must be enforced, especially by the end-user.

There are many approaches to the service provisioning procedure: End-user driven (either via manuals or software-based wizards), technician driven (a skilled staff set-up all required services asking the customer key configuration items) or automatic (device shipped totally/partially pre-configured or remote configuration retrieval upon device boot).

Three additional sub-stages could be identified: Provision of Public Key Infrastructure, Evaluation and Certification for Security and Safety, and Third-party and Independent Security and Safety Assessments. These could be considered as separate stages but are included here for simplicity.

---

[8] Xu, Xiaolin, Fahim Rahman, Bicky Shakya, Apostol Vassilev, Domenic Forte, and Mark Tehranipoor. 2019. "Electronics Supply Chain Integrity Enabled by Blockchain." ACM Transactions on Design Automation of Electronic Systems 24 (3): 1–25. https://doi.org/10.1145/3315571

2.2.9 Technical Support & Maintenance

Support and maintenance can be defined as the series of actions and processes that are taken during the device life cycle to keep the IoT product from degrading and ensuring it fulfils its purpose according to the requirements (i.e. functional, security) in the face of the passage of time or unexpected developments (e.g. software bugs, zero day vulnerabilities).

Support and maintenance processes can be classified in two categories, remote and local. The former leverages network infrastructure and techniques like secure firmware or credential updates to achieve its goal and could be considered more cost-effective. However, the sensitivity of the information involved can sometimes pose a big challenge that may require of the physical approach. An example challenge could be remotely revoking and updating device credentials using a communication channel enabled by those same credentials.

In the case of a technical support instance due to a proactive request from the user's part, the assigned technician fixes the issue by either guiding the user in the required steps (e.g. delivering a software update) or remotely connecting to the device. The opportunities for remote assistance—and the related beneficial cost implications—are defined by the capabilities established in the product design stage.

Occasionally some issues cannot be fixed and require a full or partial product replacement. In this case the device recovery and service provisioning stages are clearly interlinked with the support stage.

From the staff point of view the support effort can be structured in tiers, usually starting with first line operators trained to deal with the most common problems down to highly skilled technicians with expertise in a particular area.

Providing proper support for IoT devices can help in addressing the issues that may arise even in the presence of a good design. Furthermore, a good design has a big impact in keeping the volume of said issues to an acceptable level.

2.2.10 Device Recovery & Repurpose

This stage can be defined as the procedure followed after a device has reached the end of the operational life at a particular location. Depending on its condition (or customer needs) the device will be scrapped and recycled or repurposed to start a new operational cycle at a different location. In case of device repurpose it must be provisioned again.

The recovery procedure can involve several operations at two different levels. Examples in the software domain include data retrieval for archiving purposes, user data erasure[9], full wipe and operating system installation. Some operations are also usually required on the IoT platform backend such as revoking credentials or access permissions. On the other hand, hardware operations include destruction of storage media, recycling of components or raw materials and biological sanitization.

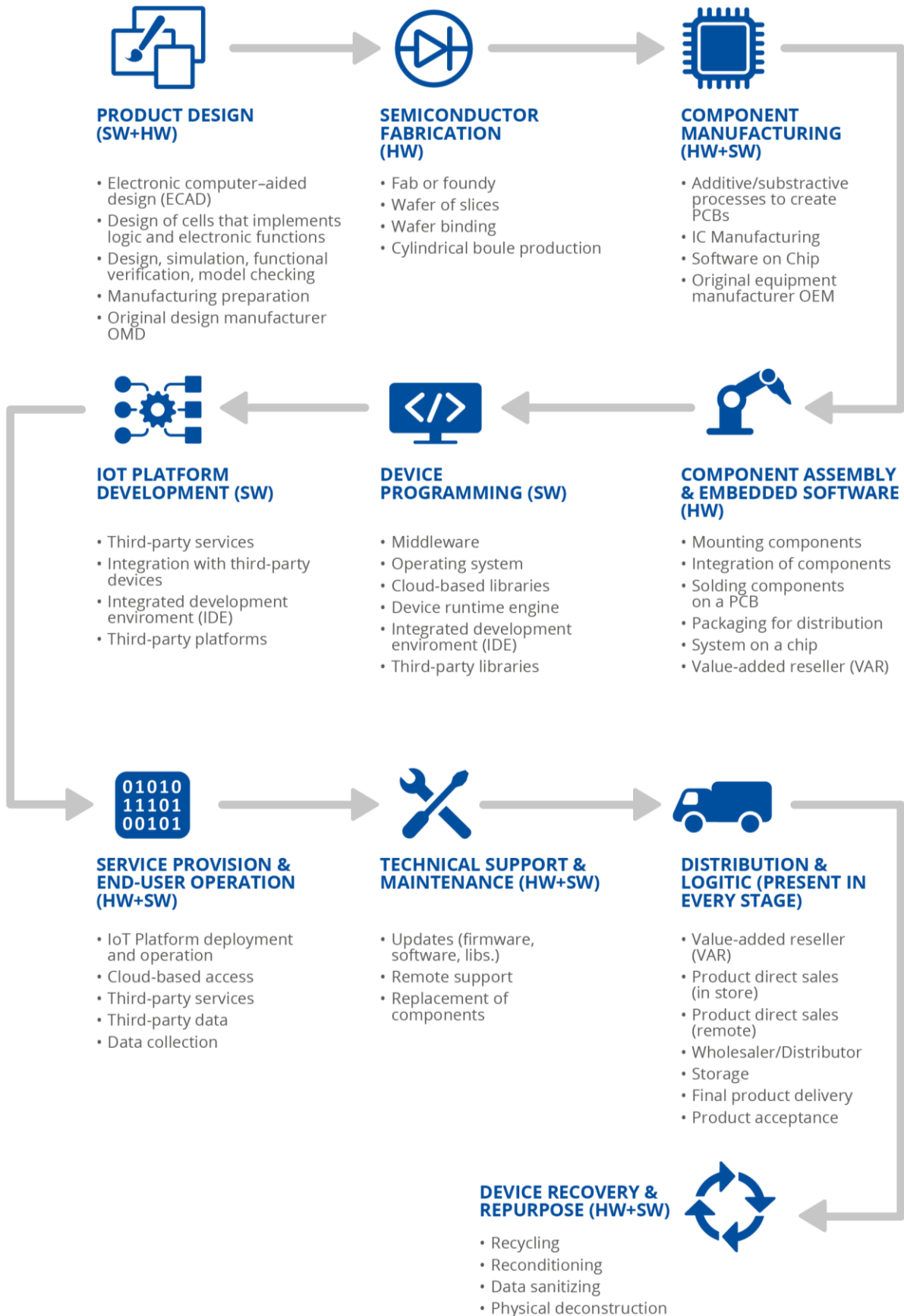### 2.3 MAPPING OF THE IOT SUPPLY CHAIN

Whereas the previous section presented an overview of the general phases of supply chain, the mapping below provides a visualization of the more detailed activities specific to the stages of the supply chain for IoT. It also helps to develop a linear understanding of the correlation between subsequent phases.

---

[9] Kissel, Richard, Andrew Regenscheid, Matthew Scholl, and Kevin Stine. 2014. "Guidelines for Media Sanitization." NIST SP 800-88r1. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-88r1

Figure 2: Mapping of the IoT supply Chain

PRODUCT DESIGN (SW+HW)

- Electronic computer–aided design (ECAD)
- Design of cells that implements logic and electronic functions
- Design, simulation, functional verification, model checking
- Manufacturing preparation
- Original design manufacturer OMD

SEMICONDUCTOR FABRICATION (HW)

- Fab or foundy
- Wafer of slices
- Wafer binding
- Cylindrical boule production

COMPONENT MANUFACTURING (HW+SW)

- Additive/substractive processes to create PCBs
- IC Manufacturing
- Software on Chip
- Original equipment manufacturer OEM

IOT PLATFORM DEVELOPMENT (SW)

- Third-party services
- Integration with third-party devices
- Integrated development enviroment (IDE)
- Third-party platforms

DEVICE PROGRAMMING (SW)

- Middleware
- Operating system
- Cloud-based libraries
- Device runtime engine
- Integrated development enviroment (IDE)
- Third-party libraries

COMPONENT ASSEMBLY & EMBEDDED SOFTWARE (HW)

- Mounting components
- Integration of components
- Solding components on a PCB
- Packaging for distribution
- System on a chip
- Value-added reseller (VAR)

SERVICE PROVISION & END-USER OPERATION (HW+SW)

- IoT Platform deployment and operation
- Cloud-based access
- Third-party services
- Third-party data
- Data collection

TECHNICAL SUPPORT & MAINTENANCE (HW+SW)

- Updates (firmware, software, libs.)
- Remote support
- Replacement of components

DISTRIBUTION & LOGITIC (PRESENT IN EVERY STAGE)

- Value-added reseller (VAR)
- Product direct sales (in store)
- Product direct sales (remote)
- Wholesaler/Distributor
- Storage
- Final product delivery
- Product acceptance

DEVICE RECOVERY & REPURPOSE (HW+SW)

- Recycling
- Reconditioning
- Data sanitizing
- Physical deconstruction

3. THREATS TO IOT SUPPLY CHAIN

This chapter presents a series of threats that are considered the most relevant in the context of the IoT supply chain. Relevance has been determined by conducting a preliminary desktop research phase, followed by a validation phase where threats were discussed with experts using two distinct formats—personal interviews and questionnaires.

These threats have been classified under a set of high-level categories. Please note that horizontal threats that apply to all domains (e.g. vandalism) should still be considered in addition to the specific threats of the supply chain.

All threats include a **short description** and the **list of IoT supply chain stages** that are most likely to be affected by the threat. This doesn´t mean that other stages are not related to a threat, instead affected stages are the phases in which the threats are more dangerous and/or can be tackled most effectively.

3.1 PHYSICAL ATTACK (DELIBERATE/INTENTIONAL)

Sabotage	
The assembly pipeline may provide malicious actors with the opportunity to interfere and inject defects that may end up causing problems (up to the total shutdown and malfunction of the product) in later stages. The threat of attacking manufacturing processes (independently discussed in another category) is relevant and closely related in the context of sabotage.	• Component assembly & embedded software.

Grey markets	
Defective, discarded or lost products may end up in grey markets that exist outside of the proper distribution channels. This can lead to unforeseen consequences and add numerous difficulties to the implementation of strict security and quality standards by injecting untested and unreliable products into the market.	• Technical support & maintenance. • Device disposal & decommissioning.

Exploitation of inadequate physical enclosures	
Some devices require to be physically tamper-proof depending on the scenario. The choice of materials and construction method must be adequate for the intended use of the product. For instance, it doesn't matter how good the software of a smart lock is if the device can be easily torn apart with bare hands . Besides worrying about the physical enclosure, the designer should also consider how ports are included in the case. For instance, a maintenance port only used in manufacturing can be used by an attacker in the field. This port should be disabled or removed prior to field installation.	• Service provision & end-user operation. • Technical support & maintenance.

3.2 INTELLECTUAL PROPERTY LOSS

IP theft	
Malicious actors may be able to illegally acquire, exploit, store or redistribute intellectual property and sensitive pieces of information (e.g. design documents, source code, credentials or other secrets). These provide dangerous insight into the vulnerabilities of the specific IoT products and may serve as valuable assets for attackers. This threat is closely related to the security-by-obscurity strategy (i.e. achieving security by ensuring documentation and sources remain secret) whose effectiveness and relevance is regularly criticized by experts.	• Product design. • Component manufacturing.

Reverse engineering	
The consequences of reverse engineering are arguably similar to those of IP theft; the main difference resides in the method used to obtain the sensitive assets and pieces of information (e.g. source code from the binaries, deep understanding of hardware blocks). These are derived from trial-and-error and meticulous study of the behaviour of a final product during the utilization phase by attackers that lack access to the original designs. This process may also lead to the discovery and release into the public domain of vulnerabilities (whether in first or third-party components) or firmware backdoors. It is important to note that reverse engineering in itself is not a threat, and should only be considered as such when used with malicious intent.	• Component assembly & embedded software. • Device programming. • Technical support & maintenance. • Device disposal & decommissioning.

Overproduction and cloning	
Overproducing is the practice of fabricating a product whose design documents and specifications have been provided willingly by the rightful owner, with the particularity that this is done outside of the established bounds of a legal contract. These products appear to be original but are insecure and pose a threat to the supply chain. A malicious factory can also clone the physical characteristics, firmware/software and security configuration of the device. Deployed devices might also be compromised and their software reverse-engineered, allowing for cloning. Cloned devices may be sold cheaply in the market and can contain functional modifications including backdoors. Alternatively, a genuine device may be substituted with a variant or clone during transportation or commissioning .	• Component manufacturing. • Component assembly & embedded software.

3.3 NEFARIOUS ACTIVITY/ABUSE

Magnetic field attacks	
Devices that are deployed in the field may be exposed to magnetic field attacks. These attacks are based on interfering with the units on an electromagnetic level, corrupting system memory in the process. Possible consequences include a Denial of Service (DoS) attack or the extraction of sensitive information (e.g. private keys during generation).	• Component assembly & embedded software. • Service Provision & End-user Operation

Malware insertion	
Attackers are presented with the opportunity to insert malicious software whose main objective is to provide illicit access or any other functionality that goes against the intended usage of the system. Insecure update mechanisms and poisoned update services are prime examples of such opportunities for malware injection. IoT gateways are especially relevant in this context; these are functional devices that are commonly found in IoT architectures, but can also function as a threats source. IoT gateways usually have a supporting role in the scope of security requirements, they are, however, an avenue to compromise IoT devices for a malicious actor, providing access into trusted networks and a method to acquire data from supported constrained devices.	• Component manufacturing. • Component assembly & embedded software. • Device programming. • IoT platform development • Service provision & end-user operation

Exploitation of debug interfaces	
Debugging IoT devices without compromising confidentiality, integrity and availability is a relevant challenge—there are no standards to incorporate debugging interfaces such as JTAG. Hardware or software interfaces specifically meant for internal use in the organization may be improperly disabled and end up as part of the final designs that reach the production and assembly stages. The existence of these interfaces is commonly attributed to oversight in the early phases, as they are meant to serve as tools for debugging and detection of errors, although there may be cases where those interfaces are included with malicious intent. The key is enabling this functionality securely and only to authorized personnel which seems to be the industry challenge. They provide attackers with a dangerous level of access to the final product .	• Service provision & end-user operation.

Tampering and counterfeits	
Counterfeit products are sold by unauthorized suppliers who are not part of manufacturer's official sales channel. These products, which have been designed and manufactured by unknown parties, are labeled as the manufacturer's products. This threat contemplates the inclusion of counterfeit chips in boards—chips that contain some kind of malicious modification (e.g. hardware trojans) or that have not been properly validated. Boards that present this issue are referred to as tampered boards. These unauthorized chips range from similar parts with lower tolerances and capabilities, defective parts that needed to be disposed of, parts reused from other boards that do not meet the quality standards, overproduced parts, or parts produced through an unauthorized use of intellectual property . The window of opportunity for tampering may appear during multiple stages, including distribution, especially when operating with logistics companies that lack transparency about their security measures.	• Semiconductor fabrication. • Component manufacturing. • Component assembly & embedded software. • Distribution & logistics. • Device recovery & repurpose.

3.4 LEGAL

Implications due to standard and regulation non-compliance	
Architecting processes around privacy/encryption is a challenge that is affected by existing privacy laws and regulations and by the fact that some actors in the supply chain ecosystem have their own different understanding about the security aspects. SLAs are signed between different actors in the supply chain to ensure a common contractual enforced view of the security aspects. All devices should comply with security guidelines mandated by respective industries (e.g. energy, medical, automotive). Moreover, GDPR and any other local regulation should be applied to cover the risks associated with standards/regulation non-compliance.	• Product design. • Service provision & end-user operation. • Technical support & maintenance.

3.5 UNINTENTIONAL DAMAGE OR LOSS OF INFORMATION

Compromise of Network	
Systems that are necessary for the control of supply chain processes and exist in a network could become compromised without the proper QoS or firewall policies. These assets could be weaponized to orchestrate, for example, large scale Denial of Service (DoS) attacks, or to degrade the operation of the supply chain. Those that have access to the Internet are the most vulnerable, although isolated internal networks are also at risk from insider attacks.	• Product design. • Device programming. • Service provision & end-user operation.

Use of factory authentication settings	
Devices which require authentication should never leave the factory with a fixed global default credentials or a credentials derived from easily obtainable information (i.e. MAC address). Each device should have a unique random credentials assigned to it during manufacturing. Especially during any updates, which represent an important critical point in security.	• Product design. • Component assembly & embedded software. • Device programming. • Service provision & end-user operation • Technical support & maintenance.

Undetected software or hardware disruptions of the devices	
Systems related in any fashion to the operation of the supply chain should ideally be extensively monitored for an early detection of hardware of software issues. A more proactive approach on detection usually results in a reduced number of disruptions to the supply chain, especially when compared with reactive measures.	• All stages.

User Errors	
Users should be properly informed and trained to raise awareness about the functionality and the security risks; whether in the case of internal members of an organization operating critical supply chain systems and tools, or end users whose compromised devices could be used to gain access to other nodes that could disrupt the supply chain. Unintentional human errors could be the most direct approach to infiltrating into an	• Service provision & end-user operation. • Technical support & maintenance. • Device recovery & repurpose.

otherwise adequately protected system. The interception of communications to other stakeholders related to the supply chain (e.g. procurements) and other attacks that derive from social engineering techniques are important threats to be considered in the context of user errors.

Technological evolution during device life cycle

The technological landscape is constantly evolving. This evolution can result in unexpected vulnerabilities that were not present during the design and implementation stages; this is especially impactful in the case of devices with long life cycles (e.g. cars). Examples of such vulnerabilities include devices lacking the performance to run state of the art encryption after a flaw is discovered in previous schemes, or abandonment of software support by the vendors.

- Service provision & end-user operation.
- Technical support & maintenance.

Use of unpatched devices and systems

It is a common occurrence to discover vulnerabilities during the device life cycle that were not considered in the first stages of the supply chain. This is in fact expected, as no system can ever be considered perfectly secure. Failure to integrate a software upgrade mechanism during the design phase can pose a serious threat, as it robs the manufacturer of the ability to react to these security issues. Moreover, this mechanism must implement all technical measures to avoid code tampering and ensure the deployed firmware is genuine.

- Product design.
- Device programming.
- Technical support & maintenance.

Disruptions in cloud services

Systems that depend on cloud services and are critical to the operation of the supply chain should be able to perform their core functionality even when disconnected for extended periods of time. Organizations should consider the possibility of the service vendor going out of business, ensuring their data is available in some form of backup. Security measures to handle malicious takeover of the original domain names for the cloud services should also be ideally implemented.

- Device programming.
- IoT platform development.
- Service provision & end-user operation.

Failure of recovery procedures

Due to an attack, the system (and the device) is not able to be recovered impacting functionality and security. During the lifecycle of an IoT device, several assets (firmware, configuration, credentials) might need to be updated. Chain of trust must be considered since depending the asset to be updated (impacted), different mechanisms must be used. The recovery plan must define which mechanism and which process must be followed to fix any potential situation that might compromise the service and the security of the device. Depending the level of criticality and the element of the chain that is compromised, the mechanisms must be one or other. This is a critical process in which the security of the device and the system can be compromised.

- Service provision & end-user operation
- Technical support & maintenance

Attack to registration procedures

A lack of registration procedures, or insecure registration mechanisms, could lead to attackers registering fraudulent devices or preventing the registration of genuine devices. Devices must be registered in the appropriate authentication IoT platform services after device initialization in the product line and before final user provisioning in order to grant them access.

- Device programming.
- IoT platform development.
- Service provision & end-user operation.
- Technical support & maintenance.

Use of recovered or repurposed components

Organizations may opt to reuse components or parts that have already gone through the regular supply chain flow; this could be done for reasons such as cost optimization. The usage of components that have already been retired and may have not been properly validated for reinsertion in the supply chain poses a threat and could contaminate an otherwise secure batch of devices.

- Device recovery & repurpose.

Attack to manufacturing processes

Manufacturing pipelines are highly sensitive points of entry to the supply chain. Processes that do not implement adequate measures to regulate and monitor the access of personnel to the pipeline could cause serious vulnerabilities; this could in turn lead to other discussed threats such as sabotage or malware injection.

- Semiconductor fabrication.
- Component manufacturing.
- Component assembly & embedded software.

4. GOOD PRACTICES FOR SECURITY OF IOT SUPPLY CHAIN

4.1 SECURITY CONSIDERATIONS

One of the most significant objectives of this document is to address the main security considerations to adopt throughout the supply chain for IoT. During the creation of this study, a group of experts expressed their views on the main challenges they consider the global supply chain for IoT needs to overcome in order to deliver greater security.

As a result of this consultation, a non-exhaustive list of security considerations is shown in the following table. In the following chapter a more in-depth group of good practices is presented; to address these considerations and ensure not only the security, but also the overall quality of the IoT supply chain.

A security consideration that applies in a horizontal manner to all stages is the fact that those processes that are beyond the direct control of the organization (i.e. managed by a third party) are inherently challenging; audits and inspections can help with this consideration but are hard to enforce. Another horizontal security consideration can be found in the resilience of trustworthiness of the supply chain, that is, the ability to be able to provide continuous service of operation.

Stages	Security considerations	Description
Product design	Threat model	Identification and creation of a catalogue of potential threats.
	Secure building blocks	Usage of up-to-date and properly supported building blocks (e.g. cryptography, software libraries).
	Sabotage prevention	Monitoring of deliberate flaws in design introduced by insider threats.
	Physical-logical convergence	Ensuring adequate visibility of all requirements and needs for security engineers and other stakeholders (especially relevant in E2E security design).
	Recovery plan	Conceptual design must face and consider the definition of a recovery plan for future stages and secure mechanisms to implement it (compliant with the chain of trust).
	Combined security controls (SW and tamper resistant HW)	Define the integration between HW and SW when defining security measures. Security controls (e.g. secure boot, attestation) require the usage of tamper resistant hardware to fulfil the security requirements.
	Chain of trust definition	Chain of trust is necessary to ensure levels of trust between HW and SW elements.

	Resource constraints	Achieving a compromise between device resources (e.g. memory, computation) and other constraints such as cost or size that ensures devices are able to implement security measures while leaving room for future unexpected developments.
Semiconductor Fabrication	Hardware security mechanism	Integration of a hardware root of trust to serve as the trusted secure foundation of cryptographic operations.
	Scrap management	Management of residual and discarded materials to ensure parts are securely removed from the supply chain.
Component Manufacturing	Counterfeit components	Usage of authenticated parts to avoid security concerns introduced by fraudulent components.
	Defective components	Usage of properly tested parts that pass the quality requirements to avoid degradation of security.
Component Assembly + Embedded Software	Firmware access control	Enable secure mechanisms to control access to firmware for updates and other maintenance operations. Specially for its installation.
	Backdoors	Monitoring of suspicious behaviour and backdoors implanted in hardware or low-level firmware boot code.
Device Programming	Secure provisioning	Usage of end-to-end robust provisioning mechanisms guaranteeing the security of credentials and cryptographic information.
	Coding practices	Adoption of best practices such as code reviews and continuous integration of cybersecurity checks in the software development process.
IoT Platform Development	Development focus	Basing development efforts on a risk-based approach to achieve both adequate functionality and security.
	Dependencies management	Checks and review processes to ensure that dependencies and libraries are available, have not been tampered with and conform to security requirements.
	Network security	Secure network policies to minimize the risk of intrusion while exposing the required services in the public domain.
Service Provision & End-user Operation	Management support	Appropriate level of resources and support provided by the organization to ensure secure operation during the lifecycle of the IoT device.
	Convenience compromises	Appropriate balance of user convenience and intrusive security mechanisms that degrade the user experience.
	Usage by operators	Operators of IoT services are provided with adequate training to avoid introducing security risks that originate from misuse or misconfiguration.
	Adoption of security features	Monitoring and usage of techniques to increase the adoption rate of optional security features by end users.

		Technical support	Technical support throughout the life cycle of the product.
		Access control	Management of credentials (including revocation) and access permissions of devices to IoT platforms.
Distribution and logistics		Value-added resellers (VAR)	Certification of personalization services for IoT devices offered by third parties that may introduce unforeseen security risks.
		Protection against theft and counterfeits	Adoption of security measures to reduce the risk of property theft and replacement with counterfeit components in the distribution process and logistics chain.
		Device identity	Compose a device identity during device fabrication based on the combination of the different HW and SW components (e.g. board ID, secure element ID). This device identity composition helps to track and device fabrication tracking and can be used in the IoT platform access control.
		Tracking for registration	Define a proper device registration or onboarding to the IoT platform based on the tracking of the device in the different stages of fabrication.
Technical Support & Maintenance		OTA control tools	Adoption of mechanisms to ensure remote Over-The-Air control tools used for maintenance are properly managed and secured following the chain of trust.
		Patches	Usage of software version that sufficiently mitigates the threats exposed and the latest security patches to avoid risks from well-known security vulnerabilities.
Device Recovery & Repurpose		Data removal	Adoption of secure data removal techniques to avoid sensitive pieces of information remaining on the device.

4.2 GOOD PRACTICES TO IMPROVE SECURITY

Development of good practices for securing the supply chain for IoT is one of the key objectives of this study. The aim is to provide recommendations for the target audience to assist in countering and mitigating the threats that might impact the supply chain for IoT. Recommendations focus on covering the overlapping issues, as most practices are not effective across all industries and users.

To organise the domains in a logical manner, good practices were classified into the following three main groups: actors, processes and technologies. Please note that there may exist a degree of overlap between groups and some good practices could be classified into multiple categories due to the strongly integrated nature of the supply chain for IoT.

Actors: guidelines related to the principles that shape how actors in the supply chain are expected to think about, perceive and approach security in the supply chain for IoT; whether it is in the context of a clearly defined and previously agreed framework or from a personal

standpoint. Industry professionals (e.g. managers, engineers), end users and organizations can be identified as actors in the supply chain.

Processes: addresses security in the processes involved when an IoT project is designed, developed, deployed and maintained. These processes are not limited to the context of a single organization and include interactions between stakeholders, especially in those cases where trust cannot be clearly established.

Technologies: potential technical measures and elements that could be applied in order to predict, detect and reduce vulnerabilities and threats. These include hardware components, design recommendations, techniques, libraries or other software components to support the process throughout the entire supply chain.

Each practice consists of a title, its relation to one of the three categories above, a description of the practice, and references to sources for further information. Standards are to be found in the Annex C of this document.

4.2.1 Actors

ACT-01 PRIORITIZE WORKING WITH SUPPLIERS THAT PROVIDE SECURITY GUARANTEES

There is an inherent threat in working with external suppliers due to the lack of control in their security measures, however, this is regularly a business reality that cannot be avoided. This threat can be minimized by favouring companies that implement standards such as the ISO 27036 and ISO 28000, or recommendations such as NISTIR 8259.[10] A company seeking certification approval is usually a sign that they are willing to seriously work towards improving supply chain security. Certification is usually a costly process that is not suitable for all organizations—organizations that are not standardized but have comprehensive security measures in place and are transparent about them (e.g. right to audit, contractual security requirements) should also be considered trustworthy.

ACT-02 WORK TOWARDS IMPROVING TRANSPARENCY

Transparency is crucial to control security in the supply chain. Stakeholders, especially suppliers, should be transparent, offering clear and detailed information about the operations and normal behaviour of the supplied products; and communicating all the relevant information to the next step of the chain. An increased level of transparency would have the desirable side effect of reinforcing trust between participants in the supply chain.

References   •   Standards: NISTIR 8276 - Key Practices in Cyber Supply Chain Risk Management

ACT-03 DEVELOP INNOVATIVE TRUST MODELS

Trust between the stakeholders is one of the most relevant and important challenges to consider for securing the IoT supply chain (e.g. how to assess the security of ODM (Original Design Manufacturers) binaries without source code). Each stakeholder should establish a minimum level of trust according to their needs and expertise, analysing the flux of data and guaranteeing the security and privacy within their services of products. Trust models define a framework to provide formal guarantees about the behaviour of the different parties and enhance security. The supply chain would greatly benefit from developing innovative trust models or adapting existing ones to focus on its specific necessities. It should be noted that

---

[10] For further information on these standards, please see Annex B.

there is no one-fits-all approach to trust. An approach based on consistent risk evaluation would allow organizations to evaluate the business impact to apply the proper technical measures and contractual obligations (e.g. audits).

References	• Standards: NISTIR 8276 - Key Practices in Cyber Supply Chain Risk Management

ACT-04 ADOPT THE VIEW OF SECURITY IN THE SUPPLY CHAIN AS A CONTINUOUS PROCESS

Security in the supply chain should not be characterized as an occasional activity or a state, as the assurances provided by actions in the security plane (e.g. penetration tests) decrease in value over time once they have been obtained. The concept of a process implies flow and formal consensus among stakeholders, as well as approval and acceptance. Security should be included in all stages of the supply chain as a continuous and iterative process.

References	• Standards: NISTIR 8276 - Key Practices in Cyber Supply Chain Risk Management

ACT-05 MAINTAIN AND TRAIN A QUALIFIED AND SKILLED WORKFORCE

As is the case with many technological fields, the IoT domain displays a fast pace of change. Maintaining a skilled workforce that has access to regular security training and the required resources to keep up to date with the field is of great importance to face the security challenges raised by the supply chain for IoT. Professional teams dedicated solely to security should be present in most organizations; those that lack the resources to maintain such teams should at least ensure that other technical teams have an appropriate degree of knowledge on security.

References	• Own sources: Questionnaire Analysis Report
	• Standards: NISTIR 8276 - Key Practices in Cyber Supply Chain Risk Management

ACT-06 PROMOTE A DEVELOPER WORK CULTURE FOCUSED ON A RISK-BASED APPROACH

Software developers sometimes tend to invest significant resources in pursuing extended functionality for the end product, which can have the undesired side effect of taking said resources from security-related tasks. This issue can be exacerbated by some decisions from the management layers, if they are detached from the development focus, a perfect example of this is unrealistic deadlines. Promoting a development process that considers risks when distributing resources and ensures that security receives the appropriate attention can have a significant impact in the security of the supply chain.

ACT-07 PROMOTE IOT SECURITY AWARENESS FOR USERS

A significant percentage of users lack knowledge about security configuration and are not fully aware of the impact of weak security. Vulnerable IoT devices in the possession of users can sometimes be used as an entry point to systems and services in the supply chain (e.g. servers used for provisioning or configuration). The burden of security should never be left as a responsibility to the user; however, organizations could benefit from investing resources in campaigns and actions to raise awareness on the importance of proper security. For example, this could take the form of marketing campaigns or carefully crafted configuration modules to provide guidance and a great user experience. In addition, manufacturers should be required to include a comprehensive user guide or manual, which provides instructions on the safe and

secure use of its products. In a related fashion, consumers should also be educated to ensure they view counterfeiting as an unacceptable and dangerous practice.

References • Standards: CMU SPL - Carnegie Mellon University's Security & Privacy Label

ACT-08 PROVIDE SECURITY PROMISES TO CUSTOMERS

Customers should be clearly and explicitly provided with comprehensive information related to security. This includes, for example, possible vulnerabilities that could be discovered during the life cycle of the product, or the relation of software updates that are deployed in devices on the field. The transference of this information to actors down in the chain is crucial to achieve continuous security. This practice is closely related to ACT-01 and ACT-02, it is, however, presented separately to highlight its nuances and relevance.

4.2.2 Processes

PRO-01 ADOPT SECURITY BY DESIGN PRINCIPLES

Security modules should be considered components of high priority and factored into the design process from the first stages throughout the entirety of the supply chain; this is to avoid the threat that originates when security modules are treated as an afterthought or considered of a lesser priority. Integration of a strong chain of trust should be a priority to ensure the integrity of hardware and software modules in IoT devices (please see TEC-06). Use of secure coding techniques and tests focused on security (e.g. penetration tests, vulnerability scanning) should be included in the appropriate stages of the IoT supply chain to implement and validate appropriate security features. A security baseline to cover the most important components of the IoT supply chain should be defined; such a security model should cover the security core elements: protection, detection and incident response. Human factors must also be taken into account at the design stage. Best practices must be enforced and followed rigorously to avoid undermined security because of poor user decisions. The inclusion of legal departments in the security and privacy assessments is another important practice that should be integrated into the design process. Moreover, security experts should be directly involved in the early conceptual design discussions with the product management team, so they can include their point of view in the selection of the materials according to their security requirements.

References • Own sources: Questionnaire Analysis Report
• Standards: ISO/IEC 11889 - Trusted Platform Module (TPM)

PRO-02 ESTABLISH AND IMPROVE DATA COLLECTION, MEASUREMENT TECHNOLOGIES, AND DATA MANAGEMENT

Not all stakeholders have the resources to perform security audits or analysis, so the majority perform trust assumptions at some point. It is desirable to minimize these assumptions when feasible, while maintaining privacy assurances for the end user. An advanced tool or mechanism to help with data collection and measurement would be of significant help in this regard. Initiatives like the International Data Spaces—an international initiative with links to the European Commission focused on improving methods and mechanisms for a more secure and trusted data exchange in business ecosystems—may also provide inspiration.

References • Standards: NISTIR 8276 - Key Practices in Cyber Supply Chain Risk Management

PRO-03 CREATE SUPPLY CHAIN INTEGRITY METRICS

The concept of integrity in the context of the IoT supply chain is arguably very wide. Most interpretations could agree that it is related to the state of the supply chain operating in an unadulterated manner, being free of counterfeits, malware or other influences that may reduce visibility and accountability (e.g. not being able to properly trace firmware updates). Metrics can be created and monitored continuously to provide visibility on the state of the supply chain. These metrics could be tied to the specifics of the current supply chain or be more horizontal in nature. Metrics could be designed mainly in the earlier design phases and be adjusted in an iterative and continuous fashion depending on the evolution of the supply chain. Examples of such metrics could include the distribution of firmware versions that are currently deployed in the field.

| References | • Own sources: Questionnaire Analysis Report |
| | • Desktop research: Electronics Supply Chain Integrity Enabled by Blockchain[11] |

PRO-04 DEVELOP THREAT MODELS FOR THE IOT SUPPLY CHAIN

Threat models should merge the concepts of both physical safety and digital security that are intrinsic to cyber-physical systems. The development process includes dividing the supply chain into functional blocks and listing the assets in those blocks, to later detect critical assets and blocks. To this end, a knowledge base of attack tactics and techniques such as MITRE ATT&CK or the threat model presented in this report may serve as the foundation to develop combined (safety-security) threat models. This also should include, besides threats of attacks, unintentional incidents that may also impact security, safety and performance resulting from errors in managing the increased complexity of systems coming from the addition of IoT. Risk assessment methodology should be applied in order to assess the relative importance of the threats depending on the criticality of the domain and implement actions (e.g. optimizing the resources available, preparing contingency plans) to protect the different stages in the supply chain—motivation behind the cyberattacks (e.g. financial gain, terrorism) should also be considered to define cost-effective protections and security controls. Furthermore, a significant amount of IoT elements present a lack of accountability for the tasks they perform. This is due to the absence of logging in most IoT devices because of hardware constraints or additional costs. A risk assessment for the whole IoT supply chain setup should be performed to identify components where logging components are necessary.

| References | • Desktop research: IoT cybersecurity guidelines, standards and verification systems, a caba white paper[12] |
| | • Desktop research: Microsoft Threat Modeling Tool |

PRO-05 IDENTIFY THIRD-PARTY SOFTWARE

The usage of third-party software introduces a degree of uncertainty that acts as a threat to the security of the supply chain. These software components must be documented as part of the supply chain security process, including the criteria followed for its selection; organizations should prefer those that have passed an evaluation and certification process, and include a maintenance plan. A comprehensive analysis of the source code is recommended for open source cases where a reputable community of maintainers and industry stakeholders cannot be identified—a possible approach to cover vulnerable code is to deploy a custom layer on top, although this forces the organization to follow the updates of the original developer. To help with the software identification process, organizations may use software tools specialized in

[11] Xu, Xiaolin, Fahim Rahman, Bicky Shakya, Apostol Vassilev, Domenic Forte, and Mark Tehranipoor. 2019. "Electronics Supply Chain Integrity Enabled by Blockchain." ACM Transactions on Design Automation of Electronic Systems 24 (3): 1–25. https://doi.org/10.1145/3315571 .
[12] Khan, Faud, and David Rogers. 2019. "IoT Cybersecurity Guidelines, Standards and Verification Systems." In . CABA.

Component Analysis such as OWASP Dependency-Track, which is a tool to generate SBOMs (please see related practice PRO-13). Scanning products may also be leveraged to identify software components and vulnerabilities; source code scanning tools are available for internal and open source components, while binary scanning tools can be applied in the context of closed source. It should be noted that open source tools can play a significant role in IoT security as transparency and openness are highly important. The open source community is also efficient when finding flaws and promptly fixing them. The industry benefits greatly when fixes for vulnerabilities discovered in open source tools in the context of a private organization are released back to the open source community.

References	• Standards: NISTIR 8276 - Key Practices in Cyber Supply Chain Risk Management

PRO-06 ESTABLISH A COMPREHENSIVE TEST PLAN

All IoT solutions should include a comprehensive testing plan to verify that the product displays the expected features in both the software and hardware. Acceptance testing should occur independently from any previous testing that could have taken place in earlier stages in the supply chain. A fraction of the devices should be inspected in the last part of manufacturing and subjected to cybersecurity testing to detect misconfigurations or errors.

References	• Own sources: Questionnaire Analysis Report
	• Desktop research: IoT cybersecurity guidelines, standards and verification systems, a caba white paper[13]

PRO-07 IMPLEMENT FACTORY SETTINGS THAT USE SECURITY BY DEFAULT

A significant percentage of customers tend to ignore security features due to convenience reasons or a lack of technical knowledge; this usually results in vulnerabilities that could be avoided with an appropriate usage of the security features already included in the devices and products. Security by default should be the approach for the manufacturers and suppliers, so customers that need to disable security have to do so in a conscious and explicit manner. This approach would be based on a consistent security model that is mandatory to be applied and ensure that data is properly collected, manipulated and transferred.

PRO-08 COMMIT TO PROVIDING SECURITY PATCHES FOR A CERTAIN PERIOD OF TIME

Legacy IoT devices based on unmaintained software are a threat to the integrity of the supply chain. Extended support and a timely delivery of security patches should be factored into the design and planning of an IoT product—this includes proper dimensioning of resources (e.g. memory) to support future updates. Manufacturers should have the obligation to deliver security patches at least until the end-of warranty time, and preferably until the end-of-support time. In any case, the period of time that the manufacturer commits to provide the security patches should be explicitly and clearly indicated in advance to procurement, and available at no additional cost during use.

PRO-09 INTEGRATE SECURE SCRAP MANAGEMENT PROCESSES

Materials and components produced in the manufacturing and fabrication stages that fail the quality tests or are not deemed ready for production due to any possible reason should be processed and disposed of in a secure fashion (e.g. avoid leaving the defective units in unsecured containers). This is to avoid the threat of malicious actors gaining access to said

---

[13] Khan, Faud, and David Rogers. 2019. "IoT Cybersecurity Guidelines, Standards and Verification Systems." In . CABA.

components, which could be released on the market for free, or serve as valuable assets to study and discover vulnerabilities or produce counterfeits through reverse engineering.

PRO-10 USE SECURE DATA REMOVAL TECHNIQUES

Devices are usually restored back to factory settings and cleared of all private user data during the decommissioning and recovery stages. Insecure data removal practices (e.g. a simple deletion process that does not overwrite all storage sectors) may leave traces of private user data in the persistent storage that may be later recovered using specialized software tools by another user with access to the device. Secure data erasure techniques should be integrated into these stages to ensure that all private user data and configuration data are effectively removed in a safe manner. Some of these techniques should be taken into consideration way before the data removal such as the cryptographic erase, that means that this good practice should be adopted from the beginning of the supply chain.

References
- Own sources: Questionnaire Analysis Report
- Desktop research: Guidelines for Media Sanitization[14]

PRO-11 CREATE COMPREHENSIVE DOCUMENTATION RESOURCES

Build a comprehensive set of documentation resources to combat human errors that include clear guidelines or action points to implement at each deliverable, particularly on the aspects of configuration management and restoration following a failure. This is a critical issue as the absence of said resources is a threat to the supply chain; moreover, the presence of sub-par documentation could actually be actively harmful. The support and end-of-life stages are especially vulnerable to this threat. ENISA could play a significant role in this regard by hosting and maintaining a repository of resources such as list of flawed software stacks to be avoided by vendors, or a list of secure components and proven combinations to be used as a guideline in the design stage.

References
- Desktop research: Guide for Security-Focused Configuration Management of Information Systems[15]

PRO-12 DEVELOP OR ADAPT STANDARDS FOR THE SUPPLY CHAIN FOR IOT

Currently no standard would perfectly fit the purpose of securing the supply chain for IoT across all industries. Although some IT security standards could be applied, there are limitations, depending on the industry. Some standards, such as ISO27001 or the recent NERC CIP-013-1, could arguably be considered quite open or generic. For certain domains or industries, some standards are too abstract and perceived as difficult to understand and apply in the context. Moreover, there is arguably a gap between the standardisation bodies and the development community. Development of new standards or adaptation of existing ones would contribute towards giving coherence to the security management for the global supply chain for IoT and improving the integration of security information across all actors. One of the most important challenges related to this issue is finding building blocks for the supply chain that are meaningful and general enough to be applied in a horizontal fashion, thus reducing the cost of entry of implementing a standard for small and medium companies.

[14] Kissel, Richard, Andrew Regenscheid, Matthew Scholl, and Kevin Stine. 2014. "Guidelines for Media Sanitization." NIST SP 800-88r1. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-88r1 .
[15] Johnson, Arnold, Kelley Dempsey, Ron Ross, Sarbari Gupta, and Dennis Bailey. 2019. "Guide for Security-Focused Configuration Management of Information Systems." NIST SP 800-128. Gaithersburg, MD: National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-128 .

PRO-13 PROVIDE SOFTWARE BILL OF MATERIALS (SBOMS) FOR IOT DEVICES

A SBOM describes the software components used as building blocks of any given product in an exhaustive fashion, including both open source and commercial packages or libraries. These lists increase visibility into the product and enable both the manufacturer and external users to check for known vulnerabilities and validate the device from a security standpoint, helping to reduce the vulnerability gaps that may enable attackers successfully leverage a vulnerability for malicious purposes. Increased product visibility may also lead to increased trust between actors of the supply chain. SBOMs should ideally be available for all IoT products of any given organization, regardless of the fact if they are commercially distributed or not. SBOMs can serve as a building block for the implementation of a configuration management and versioning system; these systems support the evolution of software components, improving traceability and enabling users and organizations to establish a timeline of software versions. This can, in turn, be used to revert to previous stable states in case of unexpected issues.

| References | • Desktop Research: Software Trustworthiness Best Practices[16] |

4.2.3 Technologies

TEC-01 ESTABLISH AND IMPROVE PLANNING AND MANAGEMENT OF DEVICE UPGRADEABILITY AND OBSOLESCENCE

The need to modernize and improve the quality and functionalities of the devices usually leads to IoT solutions where several generations of devices and software coexist, which need to be updated in order not to become obsolete and avoid dealing with different levels of security and safety. The scope of the supply chain should be extended towards the end-of-life of any connected device, especially if OTA updates are involved. The update of IoT devices is difficult since the products are usually based on various packages from different sources and using different tools and third-party components. The planning and management of these updates is something very important to consider.

| References | • Standards: NISTIR 8276 - Key Practices in Cyber Supply Chain Risk Management |

TEC-02 LEVERAGE EMERGING TECHNOLOGIES FOR SECURITY CONTROL AND AUDITING

Emerging technologies could help provide visibility into the supply chain for IoT and should at least be evaluated. Organizations should first assess their viability from a security standpoint before committing to an application. Examples of such technologies include Blockchain, that can be used to provide strong integrity guarantees in traceability systems; and artificial intelligence (AI), which could help support professionals in the process of decision-making for a wide range of issues. For example, Device Fingerprinting (DFP) is an example application of AI where device identity is derived from its network activity without the need of reading an unequivocal identity. However, organizations should factor in the fact that AI does not provide absolute performance guarantees and should be used as a complementary tool in a significant number of cases.

---

[16] Buchheit, Marcellus, Mark Hermeling, Frederick Hirsch, Bob Martin, and Simon Rix. 2020. "Software Trustworthiness Best Practices." An Industrial Internet Consortium White Paper.
https://www.iiconsortium.org/pdf/Software_Trustworthiness_Best_Practices_Whitepaper_2020_03_23.pdf .

TEC-03 USE HARDWARE MECHANISMS TO PROVIDE INTERNAL VALIDATION

Integrate hardware obfuscation techniques into the circuit design processes to protect against threats such as reverse engineering and overproduction. These techniques are based on adding key inputs that are not critical to the actual functionality of the circuit but are used to validate the operation; the output of said circuits would not be correct in the presence of an invalid key. The secret keys should not be known to the untrusted foundries and OSATs and should be activated later in the fabrication process by the IP owner. In a related fashion, transport keys and/or activation keys should be used to protect from theft during transport (between entities or sites).

References   • Desktop research: DesignCon 2020 - Keynote – Design for Security: The
                        Next Frontier of Smart Silicon[18]
                      • Standards: IEEE 802.1AR-2018 - Secure Device Identity

TEC-04 FAVOUR THE ADOPTION OF SLAS THAT REQUIRE THE PRESENCE OF SOFTWARE INTEGRITY MEASURES

Secure boot and firmware signing are security measures that provide a degree of protection against tampering. In the case of firmware signing the hash of any given firmware image is signed using a private key that is only available to the genuine provider of the software; the public key is later used by the device to verify the integrity of firmware images. Secure boot refers to the practice of cryptographically validating the entire chain of software components that take part in the device boot process starting from an immutable root of trust. This integrity measures must be used during device manufacturing (when firmware is flashed in first boot) and during maintenance (in OTA) these cryptographic operations must be done in conjunction with a tamper resistant hardware in the framework of the chain of trust (being the tamper resistant hardware the root). These two measures can be integrated into existing Service-Level Agreements with third-party suppliers. It is also worth mentioning that GlobalPlatform members are working towards developing security standards that define a series of security foundations (SRFs) (e.g. root of trust, secure firmware installation)—these could be used to provide visibility of the security features in the chips. This integrity measures must be used during device manufacturing (when firmware is flashed in first boot) and during maintenance (in OTA); ii) these cryptographic operations must be done in conjunction with a tamper resistant hardware in the framework of the chain of trust (being the tamper resistant hardware the root).

References   • Own sources: Questionnaire Analysis Report
                      • Desktop research: TCG Guidance for Secure Update of Software and
                        Firmware on Embedded Systems[19]

TEC-05 INTEGRATE IDENTITY MANAGEMENT SYSTEMS FOR IOT DEVICES

The ability to uniquely identify every IoT device is crucial and has deep repercussions related to visibility and accountability in the supply chain. Identity management systems should be integrated into the supply chain to provide these unique identifiers. These are usually included

[17] Xu, Xiaolin, Fahim Rahman, Bicky Shakya, Apostol Vassilev, Domenic Forte, and Mark Tehranipoor. 2019. "Electronics Supply Chain Integrity Enabled by Blockchain." ACM Transactions on Design Automation of Electronic Systems 24 (3): 1–25. https://doi.org/10.1145/3315571 .
[18] Savage, Warren. 2020. "Design for Security: The Next Frontier of Smart Silicon." DesignCon 2020.
[19] Trusted Computing Group. 2020. "TCG Guidance for Secure Update of Software and Firmware on Embedded Systems." Version 1.0 Revision 72.

in the wider context of Identity and Access Management (IAM) systems that regulate the lifecycle of the device identity and provide authentication and authorization services.

TEC-06 INTEGRATE A STRONG ROOT OF TRUST

A root of trust is the first item in the chain of trust of a device; it is commonly implemented using a dedicated hardware component that provides a set of cryptographic capabilities and primitives that can be assumed as trustworthy by the device. These components are usually tamper-resistant on a hardware level and can be used as the foundation for security measures such as firmware signing or secure boot. Software alternatives with lower costs also exist, although they are significantly more vulnerable, and thus they are, in general, fit for a limited scope of applications. Actors in the IoT supply chain (e.g. OS providers, application developers) should base their contributions in this security foundation when possible.

| References | • Desktop research: TCG Guidance for Secure Update of Software and Firmware on Embedded Systems[20] |
| | • Standards: ISO/IEC 11889 - Trusted Platform Module (TPM) |

TEC-07 IMPLEMENT MECHANISMS FOR REMOTE UPDATE

The capability to apply updates in a remote and automated fashion for devices in the field is critical in the security process for the supply chain. The stages of the lifecycle of most IoT devices are not discrete, that is, further development can occur once the device has been deployed; and vulnerabilities with impact on supply chain systems can be discovered at a later date, or as a result of data gathered from an actual attack. The ability to react quickly to changes in the environment and deploy updates for remote devices shall be included and considered from the earlier stages of design. Furthermore, these mechanisms shall be secure to prevent misuse and malware injection.

| References | • Desktop research: TCG Guidance for Secure Update of Software and Firmware on Embedded Systems[21] |

TEC-08 INTEGRATE AUTHENTICATION MECHANISMS INTO CIRCUITS

To support traceability and maintenance, device authentication is mandatory. Physical Unclonable Functions (PUF)—a primitive based on the physical characteristics of a circuit that derive from its fabrication process and provide unequivocal identification—is one of the most significant options available. This means that PUF can be used to determine if a given device is genuine, improving the traceability of devices throughout the supply chain. Advantages of PUF include resistance to invasive attacks, which require the attacker to face the complex prospect of modifying the physical characteristics of the circuit. It should be noted that, in addition to PUF, other technologies such as Trusted Execution Environments (TEE) can be used to this end. Closely related to this good practice is the recommendation of properly leveraging traceability data that may be already included by silicon manufacturers in their chips.

| References | • Desktop research: Via PUF Technology as a Root of Trust in IoT Supply Chain - Global Semiconductor Alliance[22] |

---

[20] Trusted Computing Group. 2020. "TCG Guidance for Secure Update of Software and Firmware on Embedded Systems." Version 1.0 Revision 72.
[21] Trusted Computing Group. 2020. "TCG Guidance for Secure Update of Software and Firmware on Embedded Systems." Version 1.0 Revision 72.
[22] Kyung Lee, Teddy. 2020. "VIA PUF Technology as a Root of Trust in IoT Supply Chain." Global Semiconductor Alliance (blog). 2020.

TEC-09 CONSIDER THE CYBERSECURITY POSSIBILITIES INTRODUCED BY HARDWARE-SOFTWARE COLLABORATION

Hardware-software collaborative schemes are an approach that focus on covering the cybersecurity gap left by security measures that operate solely on the hardware or software layers. Hardware measures can benefit from the context provided by the current state of the system on a software level; while vulnerabilities in software measures can be covered when the software is able to communicate with specialized hardware components, especially in those cases where the attacker gains privileged/root access. It could be argued that trusted execution can be achieved only by combining hardware and software. Examples of applications of these schemes include secure storage for PUF-based keys and security assurances for untrusted kernel extensions. The security of IoT devices can be significantly improved by implementing these schemes in those cases where it is feasible to do so, however, this is usually an endeavour that requires high technical expertise.

References	
	• Desktop research: A PUF and software collaborative key protection scheme[23]
	• Desktop research: Hardware-software collaboration for secure coexistence with kernel extensions[24]

[23] Li, Changting, Zongbin Liu, Lingchen Zhang, Cunqing Ma, and Liang Zheng. 2018. "A PUF and Software Collaborative Key Protection Scheme." In Information and Communications Security, edited by Sihan Qing, Chris Mitchell, Liqun Chen, and Dongmei Liu, 291–303. Cham: Springer International Publishing.
[24] Oliveira, Daniela, Nicholas Wetzel, Max Bucci, Jesus Navarro, Dean Sullivan, and Yier Jin. 2014. "Hardware-Software Collaboration for Secure Coexistence with Kernel Extensions." SIGAPP Appl. Comput. Rev. 14 (3): 22–35. https://doi.org/10.1145/2670967.2670969 .

5. GUIDELINES AND CONCLUSIONS

This chapter reflects the general conclusions extracted from the analysis of the good practices and standards. Conclusions take the form of a set of guidelines that represent high-level recommendations and an entry point to the expanded set of good practices. They are intended to serve as super categories—all good practices have been classified under one of the guidelines—and a quick reference to the comprehensive list of good practices, which may be difficult to parse.

Each guideline presents a set of related good practices that can be categorized under said guideline and a set of standards that are relevant and strongly related. Please note that although other standards could be relevant in the context of any given guideline, only the ones that are considered the most pertinent are mentioned.

5.1 FORGING BETTER RELATIONSHIPS BETWEEN ACTORS

This guideline addresses the security issues that may arise from problems and frictions in the communications and relationships between actors in the supply chain. The set of actors may include, for example, integrated device manufacturers (IDM), foundries, outsourced semiconductor assembly and test companies (OSAT), software development houses, logistics companies or cloud service providers.

These issues may be malicious in nature or have their origin in misunderstandings or lack of coordination. Some problematic examples that can be identified include errors in design due to lack of visibility into the components provided by suppliers, or overproduction of a product outside of the boundaries of an established contract.

The opportunities for organizations to improve security are clearer when they look beyond their own operations. The use of the connections that exist between the links of the supply chain to share key information will increase the efficiency of all actors in the chain. The increase of visibility is an important benefit from a security perspective, which will help to define a better security design of the supply chain and the device consequently, in the conceptual phase.

While vertical collaboration—between suppliers and customers—is more common, horizontal collaboration between supply chain actors is also desirable for certain aspects of the security, such as the creation and establishment of industry regulations or other common frameworks.

Good practices to consider	- Prioritize working with suppliers that provide cybersecurity guarantees. - Work towards improving transparency. - Develop innovative trust models. - Adopt the view of security in the supply chain as a continuous process. - Favour the adoption of SLAs that require the presence of software integrity measures. - Provide security promises to customers.

Most pertinent standards	• ISO/IEC 27001: Requirements for an information security mgmt. system (ISMS) • ISO 27036: Information security for supplier relationships

5.2 CYBERSECURITY EXPERTISE SHOULD BE FURTHER CULTIVATED

Problems that have their origin in errors in the usage, design and implementation of controls and mechanisms related to the security domain can usually be difficult to detect and assess, especially when compared to problems in the actual functionality of the device. This is exacerbated by the moderately recent nature of the IoT industry, as best practices and past experiences are not as firmly established as in other industries.

Members of any layer of an organization (e.g. engineering, management, and marketing) may be inclined to neglect security training and education, falsely assuming that "it won't happen to me or my organization". However, security issues tend to be pervasive and severe, and as such, the lack of knowledge in this area needs to be adequately addressed.

It should also be noted that superficial security knowledge may lead to a false sense of security and could become a threat. Training deficiencies, lack of standard procedures and limited supervision usually have a direct correlation to significant security vulnerabilities in a later stage of the product.

Good practices to consider	• Maintain and train a qualified and skilled workforce. • Promote a developer work culture focused on a risk-based approach. • Promote IoT security awareness for users.
Most pertinent standards	• NIST 8276: Key practices in cyber Supply Chain risk management.

5.3 SECURITY BY DESIGN

The design of an IoT device or product is a complex process that requires careful planning and risk management. Early decisions made during the design phase usually have impactful implications on later stages, especially during maintenance. Complexity originates in a significant amount of cases from particular characteristics of the IoT domain; for example, the tendency of devices to be constrained in terms of resources, which may impose limits to the implementation of security measures or upgradability during lifecycle.

Security goals can often fail—even in the presence of good design—if there is a lack of tools that enable stakeholders to understand and assess security issues. Although some degree of flexibility is desirable, organizations should also be vigilant to ensure a well-planned strategy is adequately executed even in the face of possible shortcuts that could falsely appear to be more efficient in terms of resources.

IoT is applied to solve business problems, thus the high-level customer requirements should be included as the main input to assess the security aspects of products and services.

Furthermore, the fact that cybersecurity is not perceived as an added value in IoT mass products should be taken into account, as it usually slows the adoption of security technologies by all stakeholders.

Good practices to consider	• Adopt security by design principles. • Establish and improve data collection, measurement technologies, and data management. • Create supply chain integrity metrics. • Leverage emerging technologies for security control and auditing. • Establish and improve planning and management of device upgradeability and obsolescence. • Implement mechanisms for remote update. • Develop threat models for the IoT supply chain.
Most pertinent standards	• ISO 20243: Mitigating maliciously tainted and counterfeit products.

5.4 TAKE A COMPREHENSIVE AND EXPLICIT APPROACH TO SECURITY

The majority of security threats detected during any stage of the IoT supply chain—all except those where the impact is negligible—should be explicitly addressed by organizations. This could be applied to all domains but is crucial in the IoT context due to the increased number of devices and deployment characteristics, which usually include public spaces and unattended operation.

Preconceptions and biases related to security should ideally be considered during risk management. Data and designs can be analysed and validated from multiple points of view, and human intervention should be carefully monitored when feasible. The cost of reacting to a security breach is usually higher than the cost of adequately addressing the issue in a proactive fashion.

Good practices to consider	• Identify third-party software. • Establish a comprehensive test plan. • Implement factory settings that use security by default. • Commit to providing security patches for a certain period of time. • Integrate secure scrap management processes. • Use secure data removal techniques. • Use hardware mechanisms to provide internal validation. • Integrate identity management systems for IoT devices. • Integrate a strong root of trust. • Integrate authentication mechanisms into circuits. • Consider the cybersecurity possibilities introduced by hardware-software collaboration. • Provide Software Bill of Materials (SBOMs) for IoT devices.

	• Create comprehensive documentation resources.
Most pertinent standards	• ISO 11889: Trusted platform module (TPM) • IETF RFC 8520: Manufacturer usage description (MUD) • IEEE 802.1AR-2018: Secure device identity for local and metropolitan area networks • ISO 20243: Mitigating maliciously tainted and counterfeit products.

5.5 LEVERAGE EXISTING STANDARDS AND GOOD PRACTICES

Existing standards, previous cases and relevant legal frameworks are a cornerstone of a successful IoT supply chain implementation. Organizations can benefit greatly from dedicating resources to studying the current landscape and adapting the existing best practices to their particular case. This approach should also be applied to the internal interactions in an organization, as documentation resources and processes developed by a department can usually turn out to be critical assets for other teams.

Standards are created by bringing together all interested parties. All actors in the supply chain for IoT should make progress towards new or adapted standards in those cases where gaps are detected, as all of them will benefit from standardization through increased safety and quality of their products and services. Governments are important actors that should also be taken into account. The industry should work towards solving security and trust issues before government regulation forces a more unpalatable solution.

Security standards implemented at every stage of the supply chain reduce the attack surface—simple measures usually have a big impact in this reduction.

Good practices to consider	• Develop or adapt standards for the supply chain for IoT.
Most pertinent standards	• GSMA SAS-UP: Security accreditation scheme for UICC production. • CMU SPL: Security and privacy label.

BIBLIOGRAPHY

Boyens, Jon M. 2020. "Key Practices in Cyber Supply Chain Risk Management: Observations from Industry." Preprint. https://doi.org/10.6028/NIST.IR.8276-draft .

Boyens, Jon M., Celia Paulsen, Nadya Bartol, Kris Winkler, and James Gimbi. 2020. "Case Studies in Cyber Supply Chain Risk Management: Summary of Findings and Recommendations." NIST CSWP 02042020-1. Gaithersburg, MD: National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.02042020-1 .

Buchheit, Marcellus, Mark Hermeling, Frederick Hirsch, Bob Martin, and Simon Rix. 2020. "Software Trustworthiness Best Practices." An Industrial Internet Consortium White Paper. https://www.iiconsortium.org/pdf/Software_Trustworthiness_Best_Practices_Whitepaper_2020_03_23.pdf .

Cascella, Roberto. 2019. "Challenges of Cybersecurity Certification and Supply Chain Management." ECSO - EUNITY Workshop, January 24.

Emami-Naeini, Pardis, Yuvraj Agarwal, and Lorrie Faith Cranor. 2020. "Specification for an IoT Privacy and Security Label." Carnegie Mellon University.

Fagan, Michael, Katerina N Megas, Karen Scarfone, and Matthew Smith. 2020. "Foundational Cybersecurity Activities for IoT Device Manufacturers." NIST IR 8259. Gaithersburg, MD: National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8259 .

Filkins, Barbara, and Doug Wylie. 2019. "SANS 2019 State of OT/ICS Cybersecurity Survey." https://radiflow.com/wp-content/uploads/2019/06/Survey_ICS-2019_Radiflow.pdf .

Guin, Ujjwal, Daniel DiMase, and Mohammad Tehranipoor. 2014. "Counterfeit Integrated Circuits: Detection, Avoidance, and the Challenges Ahead." Journal of Electronic Testing 30 (1): 9–23. https://doi.org/10.1007/s10836-013-5430-8 .

IoT Security Foundation. 2019. "Secure Design Best Practice Guides." Release 2.

IoT Security Foundation. 2020. "Consumer IoT: Understanding the Contemporary Use of Vulnerability Disclosure - 2020 Progress Report."

Johnson, Arnold, Kelley Dempsey, Ron Ross, Sarbari Gupta, and Dennis Bailey. 2019. "Guide for Security-Focused Configuration Management of Information Systems." NIST SP 800-128. Gaithersburg, MD: National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-128 .

Khan, Faud, and David Rogers. 2019. "IoT Cybersecurity Guidelines, Standards and Verification Systems." In . CABA.

Kissel, Richard, Andrew Regenscheid, Matthew Scholl, and Kevin Stine. 2014. "Guidelines for Media Sanitization." NIST SP 800-88r1. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-88r1 .

Kyung Lee, Teddy. 2020. "VIA PUF Technology as a Root of Trust in IoT Supply Chain." Global Semiconductor Alliance (blog). 2020.

Li, Changting, Zongbin Liu, Lingchen Zhang, Cunqing Ma, and Liang Zheng. 2018. "A PUF and Software Collaborative Key Protection Scheme." In Information and Communications Security, edited by Sihan Qing, Chris Mitchell, Liqun Chen, and Dongmei Liu, 291–303. Cham: Springer International Publishing.

Liao, R, and Z Fan. 2020. "Supply Chains Have Been Upended. Here's How to Make Them More Resilient'." In World Economic Forum. Vol. 6.

National Cyber Security Centre. 2018. "Supply Chain Security Guidance." National Cyber Security Centre. https://www.ncsc.gov.uk/collection/supply-chain-security .

Oliveira, Daniela, Nicholas Wetzel, Max Bucci, Jesus Navarro, Dean Sullivan, and Yier Jin. 2014. "Hardware-Software Collaboration for Secure Coexistence with Kernel Extensions." SIGAPP Appl. Comput. Rev. 14 (3): 22–35. https://doi.org/10.1145/2670967.2670969 .

Ray, Sandip, Eric Peeters, Mark M. Tehranipoor, and Swarup Bhunia. 2018. "System-on-Chip Platform Security Assurance: Architecture and Validation." Proceedings of the IEEE 106 (1): 21–37. https://doi.org/10.1109/JPROC.2017.2714641 .

Ross, Steven J., Ed Gelbstein, Jane Whitgift, Vasant Raval, Rajesh Sharma, Indrajit Atluri, Hemant Patel, et al. 2017. Internet of Things. Vol. 3. ISACA Journal. ISACA. https://www.isaca.org/resources/isaca-journal/issues/2017/volume-3 .

Savage, Warren. 2020. "Design for Security: The Next Frontier of Smart Silicon." DesignCon 2020.

Staalduinen, Mark van, and Yash Joshi. 2019. "The IoT Security Landscape." TNO.

Telecommunications Industry Association. 2020. "Securing the Network and Supply Chain with Industry-Driven Standards." TIA Position Paper. Telecommunications Industry Association.

The Linux Foundation. 2019. "Project Alvarium: Enabling Data Confidence Fabrics to Scale Trust Across Heterogeneous Systems." October 29. https://alvarium.org/ .

The Ponemon Institute. 2019. "Third Party IoT Risk: Companies Don't Know What They Don't Know." https://sharedassessments.org/blog/2019-iotstudy/ .

Trusted Computing Group. 2020. "TCG Guidance for Secure Update of Software and Firmware on Embedded Systems." Version 1.0 Revision 72.

U.S. Department of Defense. 2016. "DoD Policy Recommendations for The Internet of Things (IoT)." United States. Department of Defense. Office of the Chief Information Officer. https://www.hsdl.org/?view&did=799676 .

Xu, Xiaolin, Fahim Rahman, Bicky Shakya, Apostol Vassilev, Domenic Forte, and Mark Tehranipoor. 2019. "Electronics Supply Chain Integrity Enabled by Blockchain." ACM Transactions on Design Automation of Electronic Systems 24 (3): 1–25. https://doi.org/10.1145/3315571 .

Yang, Kun, Domenic Forte, and Mark M. Tehranipoor. 2017. "CDTA: A Comprehensive Solution for Counterfeit Detection, Traceability, and Authentication in the IoT Supply Chain." ACM Transactions on Design Automation of Electronic Systems 22 (3): 42:1–42:31. https://doi.org/10.1145/3005346 .

A ANNEX: MAPPING OF THREATS TO GOOD PRACTICES

This annex includes a multidimensional matrix with a list of good practices, the most relevant threats related to the given good practice, and the stages of the supply chain for IoT most likely to be involved.

A.1 ACTORS

Principles that shape how actors are expected to think about, perceive and approach security.

Good practice	Threats	Supply chain stages
Prioritize working with suppliers that provide cybersecurity guarantees.	• IP theft. • Sabotage. • Grey markets. • Tampering and counterfeits. • Overproduction and cloning. • Attack to manufacturing processes.	• Product design. • Semiconductor Fabrication. • Component Manufacturing. • Component Assembly + Embedded Software.
Work towards improving transparency.	Majority of threats.	All of them.
Develop innovative trust models.	• IP theft. • Sabotage. • Grey markets. • User errors. • Tampering and counterfeits. • Overproduction and cloning. • Attack to manufacturing processes.	• Product design. • Semiconductor Fabrication. • Component Manufacturing. • Component Assembly + Embedded Software.
Adopt the view of security in the supply chain as a continuous process.	• Technological evolution during device life cycle. • Compromise of network. • Use of unpatched devices and systems. • Disruptions in cloud services. • User errors. • Undetected software or hardware disruptions of the devices. • Attack to registration procedures.	• Service Provision & End-user Operation. • Technical Support & Maintenance. • Device Recovery & Repurpose.
Maintain and train a qualified and skilled workforce	• Compromise of network. • Use of factory authentication settings. • Use of unpatched devices and systems. • Exploitation of inadequate physical enclosures. • User errors.	• Product design. • IoT Platform Development. • Component Assembly + Embedded Software. • Device Programming. • Service Provision & End-user Operation.

Good practice	Threats	Supply chain stages
	• Undetected software or hardware disruptions of the devices. • Exploitation of debug interfaces. • Lack of recovery procedure. • Attack to registration procedures.	• Technical Support & Maintenance. • Device Recovery & Repurpose.
Promote a developer work culture focused on a risk-based approach.	• Compromise of network. • Use of factory authentication settings. • Implications due to standard and regulation non-compliance. • Malware insertion. • Reverse engineering for malicious purpose. • Exploitation of debug interfaces. • Failure of recovery procedures. • Attack to registration procedures.	• IoT Platform Development. • Component Assembly + Embedded Software. • Device Programming. • Technical Support & Maintenance.
Promote IoT security awareness for users.	• Grey markets. • Technological evolution during device life cycle. • Use of factory authentication settings. • Use of unpatched devices and systems. • User errors. • Tampering and counterfeits. • Magnetic field attacks. • Attack to registration procedures.	• Service Provision & End-user Operation. • Technical Support & Maintenance. • Device Recovery & Repurpose.
Provide security promises to customers.	Majority of threats.	• Service Provision & End-user Operation. • Technical Support & Maintenance. • Device Recovery & Repurpose.

A.2 PROCESSES

Addresses security in the processes involved when an IoT project is designed, developed, deployed and maintained.

Good practice	Threats	Supply chain stages
Adopt security by design principles.	• Compromise of network. • Use of factory authentication settings. • Use of unpatched devices and systems. • Exploitation of inadequate physical enclosures. • Implications due to standard and regulation non-compliance. • Malware insertion. • Reverse engineering for malicious purpose. • Exploitation of debug interfaces. • Failure of recovery procedures. • Attack to registration procedures.	• Product design. • IoT Platform Development. • Component Assembly + Embedded Software. • Device Programming.
Establish and improve data collection, measurement technologies, and data management.	• Compromise of network. • Use of factory authentication settings. • Use of unpatched devices and systems. • Undetected software or hardware disruptions of the devices. • Malware insertion. • Tampering and counterfeits. • Exploitation of debug interfaces. • Magnetic field attacks.	• Product design. • IoT Platform Development. • Component Assembly + Embedded Software. • Device Programming. • Service Provision & End-user Operation. • Technical Support & Maintenance.
Create supply chain integrity metrics.	• Sabotage. • Compromise of network. • Use of factory authentication settings. • Undetected software or hardware disruptions of the devices. • Malware insertion. • Tampering and counterfeits. • Exploitation of debug interfaces. • Attack to registration procedures. • Attack to manufacturing processes.	All of them.
Identify third-party software.	• Use of factory authentication settings. • Use of unpatched devices and systems. • Implications due to standard and regulation non-compliance • Malware insertion. • Exploitation of debug interfaces.	• Product design. • IoT Platform Development. • Component Assembly + Embedded Software. • Device Programming.
Establish a comprehensive test plan.	• Sabotage. • Compromise of network. • Use of factory authentication settings. • Implications due to standard and regulation non-compliance. • Malware insertion. • Exploitation of debug interfaces.	• IoT Platform Development. • Component Assembly + Embedded Software. • Device Programming.

Good practice	Threats	Supply chain stages
	• Magnetic field attacks.	
Implement factory settings that use security by default.	• Compromise of network. • Use of factory authentication settings. • Malware insertion. • Exploitation of debug interfaces. • Failure of recovery procedures. • Attack to registration procedures.	• Product design. • IoT Platform Development. • Component Assembly + Embedded Software. • Device Programming.
Commit to providing security patches for a certain period of time.	• Technological evolution during device life cycle. • Use of unpatched devices and systems. • Disruptions in cloud services. • User errors. • Undetected software or hardware disruptions of the devices.	• Product design. • Service Provision & End-user Operation. • Technical Support & Maintenance.
Integrate scrap management processes.	• IP theft. • Grey markets. • Exploitation of inadequate physical enclosures. • Reverse engineering for malicious purpose. • Tampering and counterfeits. • Use of recovered or repurposed components.	• Semiconductor Fabrication. • Component Manufacturing. • Component Assembly + Embedded Software. • Device Recovery & Repurpose.
Use secure data removal techniques.	• IP theft. • User errors. • Use of recovered or repurposed components.	• Technical Support & Maintenance. • Device Recovery & Repurpose.
Develop threat models for the IoT supply chain.	Majority of threats.	All of them.
Create comprehensive documentation resources.	• Technological evolution during device life cycle. • Disruptions in cloud services. • User errors. • Exploitation of debug interfaces. • Attack to registration procedures.	• Service Provision & End-user Operation. • Technical Support & Maintenance. • Device Recovery & Repurpose.
Develop or adapt standards for the supply chain for IoT.	Majority of threats.	All of them.

A.3 TECHNOLOGIES

Potential technical measures and elements to predict, detect and reduce vulnerabilities and threats.

Good practice	Threats	Supply chain stages
Establish and improve planning and management of device upgradeability and obsolescence.	• Technological evolution during device life cycle. • Use of unpatched devices and systems. • Disruptions in cloud services. • User errors. • Undetected software or hardware disruptions of the devices. • Implications due to standard and regulation non-compliance. • Failure of recovery procedures.	• Product design. • Service Provision & End-user Operation. • Technical Support & Maintenance. • Device Recovery & Repurpose.
Leverage emerging technologies for security control and auditing.	• IP theft. • Sabotage. • Compromise of network. • Use of factory authentication settings. • Undetected software or hardware disruptions of the devices. • Malware insertion. • Tampering and counterfeits. • Exploitation of debug interfaces. • Attack to manufacturing processes.	• Semiconductor Fabrication. • Component Manufacturing. • IoT Platform Development. • Component Assembly + Embedded Software. • Device Programming. • Distribution & Logistics. • Service Provision & End-user Operation. • Technical Support & Maintenance.
Use hardware mechanisms to provide internal validation.	• IP theft. • Reverse engineering for malicious purpose. • Tampering and counterfeits. • Overproduction and cloning. • Attack to registration procedures.	• Product design. • Component Assembly + Embedded Software.
Favour the adoption of SLAs that require the presence of software integrity measures.	• Malware insertion. • Tampering and counterfeits.	• Product design. • Component Assembly + Embedded Software. • Device Programming.
Integrate identity management systems for IoT devices.	• Grey markets. • Technological evolution during device life cycle. • Disruptions in cloud services. • Undetected software or hardware disruptions of the devices. • Tampering and counterfeits.	• Product design. • IoT Platform Development. • Component Assembly + Embedded Software. • Device Programming.
Integrate a strong root of trust.	• Implications due to standard and regulation non-compliance. • Malware insertion.	• Product design. • Component Assembly + Embedded Software. • Device Programming.

Good practice	Threats	Supply chain stages
	• Tampering and counterfeits.	
Implement mechanisms for remote update.	• Technological evolution during device life cycle. • Use of unpatched devices and systems. • Disruptions in cloud services. • Undetected software or hardware disruptions of the devices. • Implications due to standard and regulation non-compliance. • Failure of recovery procedures.	• Product design. • Component Assembly + Embedded Software. • Device Programming. • Technical Support & Maintenance.
Integrate authentication mechanisms into circuits.	• Implications due to standard and regulation non-compliance. • Malware insertion. • Tampering and counterfeits.	• Product design. • Component Manufacturing. • Component Assembly + Embedded Software.

B ANNEX: SUMMARY OF THE MOST RELEVANT STANDARDS:

This annex includes a list of the most relevant standards and a high-level categorization depending on their field of application. The majority of these standards are generic and can thus be applied in the context of the IoT supply chain.

Information Management	Risk Management	Technical Standards
Information security management within organizations and third party relationships.	*Cybersecurity risk management for supply chain and CI.*	*Techniques and technical specifications for securing IoT devices, networks and systems.*
- ISO/IEC 27001 Requirements for an information security mgmt. system (ISMS) - ISO 27036 Information security for supplier relationships	- ISO 28000 Security mgmt. systems for the supply chain - NIST 8276 Key practices in cyber Supply Chain risk mgmt. - NIST CSF Framework for improving CI cybersecurity - CMU SPL Security and privacy label - ISO 20243 Mitigating maliciously tainted and counterfeit products - NISTIR 8259 Foundational Cybersecurity Activities for IoT Device Manufacturers. - NISTIR 8259A IoT Device Cybersecurity Capability Core Baseline. - NISTIR 8272 Impact Analysis Tool for Interdependent Cyber Supply Chain Risks. - Security Evaluation Standard for IoT Platforms (SESIP) v1.0 | GP_FST_070 - ISO 22384 Guidelines to establish and monitor a protection plan and its implementation - NERC CIP-013-1 Cyber Security – Supply Chain Risk Management	- IEC 62443 Secure industrial automation and control systems (IACS) - GSMA SAS-UP Security accreditation scheme for UICC production - IETF RFC 8520 Manufacturer usage description (MUD) - ISO 11889 Trusted platform module (TPM) - IEEE 802.1AR-2018 Secure device identity for local and metropolitan area networks - ISO/IEC 20243 Open Trusted Technology ProviderTM Standard (O-TTPS) - prpl Foundation Security Guidance for Critical Areas of Embedded Computing - ETSI EN 303 645 Consumer IoT Security - Better IoT https://betteriot.org/

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found at www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
1 Vasilissis Sofias Str
151 24 Marousi, Attiki, Greece

Heraklion office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

enisa.europa.eu