



**Smartare
Elektroniksystem**
ELECTRONIC COMPONENTS & SYSTEMS

 **INTERNET
OF THINGS
SVERIGE**

 **SVENSK
ELEKTRONIK**

Handbook for Development of Cybersecure IoT Products 2.0

Revision management

This is the second version of the handbook (published 2026), which will be updated on a regular basis.

Steering group

Magnus Svensson/Thorbjörn Ebefors,
Smarter Electronic Systems

Maria Månsson, Smarter Electronic Systems
Olle Bergdahl, IoT Sweden

Process leader and main author

John Lindström, Smarter Electronic Systems

Participating corporations and organizations

AFRY

Atlas Copco industrial technique AB

Eskilstuna Elektronikpartner AB

IoT Sweden

Luleå tekniska universitet (LTU)

Nexus AB

Prevas AB

RISE

Swedish Civil Contingencies Agency

SSF Stöldskyddsföreningen

Strainlabs AB

Svensk Elektronik

T2Data AB

Uppsala universitet

Weop AB

Xertified AB

Copyright and other rights

This handbook may be used and distributed without charge in its complete form. If figures, photos or parts of the texts are used in other contexts, the following reference shall be used: Handbook for Development of Cybersecure IoT Products 2.0, published by Smarter Electronic Systems and Internet of Things Sweden (2026).

Disclaimer

This handbook is based on the collective knowledge and experience of the working group over many years in the business. Although the working group has iteratively scrutinized the contents, it cannot guarantee that there are no errors. Although we expect that the contents of the handbook will be useful, the working group does not take any responsibility for errors or damage that may arise in areas that this handbook addresses.

Editing: Maria Bergenheim, IoT Sweden

ISBN: 978-91-989591-9-2

Foreword

Smarter electronic systems was a programme within the framework of the joint initiative by Vinnova, Formas, and The Swedish Energy Agency in strategic innovation. Its goal was to enable Swedish industry to achieve world-class sustainable development and competitiveness. As the agenda for the programme was being drafted, three main challenges emerged to ensure future requirements are met: leading-edge competence; competence supply; and an efficient value chain. Committees were formed to address each challenge, with work on this handbook was initiated by the Value Chain Committee. The first handbook, "*Smartare Elektronikhandboken*", was first published in 2018 and has been widely circulated. The handbooks are maintained by the Swedish Electronics Trade association. This publication, Handbook for Development of Cybersecure IoT Products 2.0, has been written by Smarter Electronic Systems and Internet of Things Sweden (IoT Sweden).

This second version of the handbook has been updated to cover legislation/regulations, use of AI/ML tools, and new AI-based threats.

The value chains involved in developing IoT products are complex. Many actors are involved who contribute in various ways to cybersecure IoT products released into the market. Synergy between object owners, users, and customers is important. In addition, close cooperation among development, manufacturing, test, maintenance/service and support is also required to deliver innovative, competitive, reliable and cybersecure IoT products. Thus, reliability, cybersecurity, producibility and maintainability must be designed into the IoT product. In particular, the interface between object owners and users at customers, development, research, manufacturing and maintenance/service, has been acknowledged to be decisive for how successful the IoT product will become over its lifecycle.

Efficient collaboration and cooperation result in lower manufacturing and maintenance costs over the lifecycle, faster time-to-market, as well as higher quality and cybersecurity levels. Further, the use of AI/ML-based tools in development and vulnerability scanning provide a positive impact, while the hostile use of similar tools to find vulnerabilities and weaknesses as well as plan for cyberattacks will have a negative impact on the lifecycle.

The Handbook for Development of Cybersecure IoT Products has been crafted by a working group of representatives from corporations and organizations that provided contributions over a broad range of knowledge and experience. It targets managers involved in product design, development, maintenance, and other areas that influence product specifications. The handbook, in combination with the "*Smartare Elektronikhandboken 2.1*" (The Smarter Electronic Handbook 2.1), enables effective knowledge transfer between participants developing IoT Products that are cybersecure over their entire lifecycle.

This is the second version of the handbook. We are happy to receive any ideas for improvements and extensions for the next version.

We hope that you will find the handbook usable in your daily work. It is authored by techies for techies, but we believe that also non-techies will find parts worth reading as business and legal aspects of IoT product development are included.

Please feel free to distribute the handbook among your suppliers and customers.

The handbook is downloadable from:

www.svenskelektronik.se

Best Regards,

The working group for the Handbook for Development of Cybersecure IoT Products 2.0

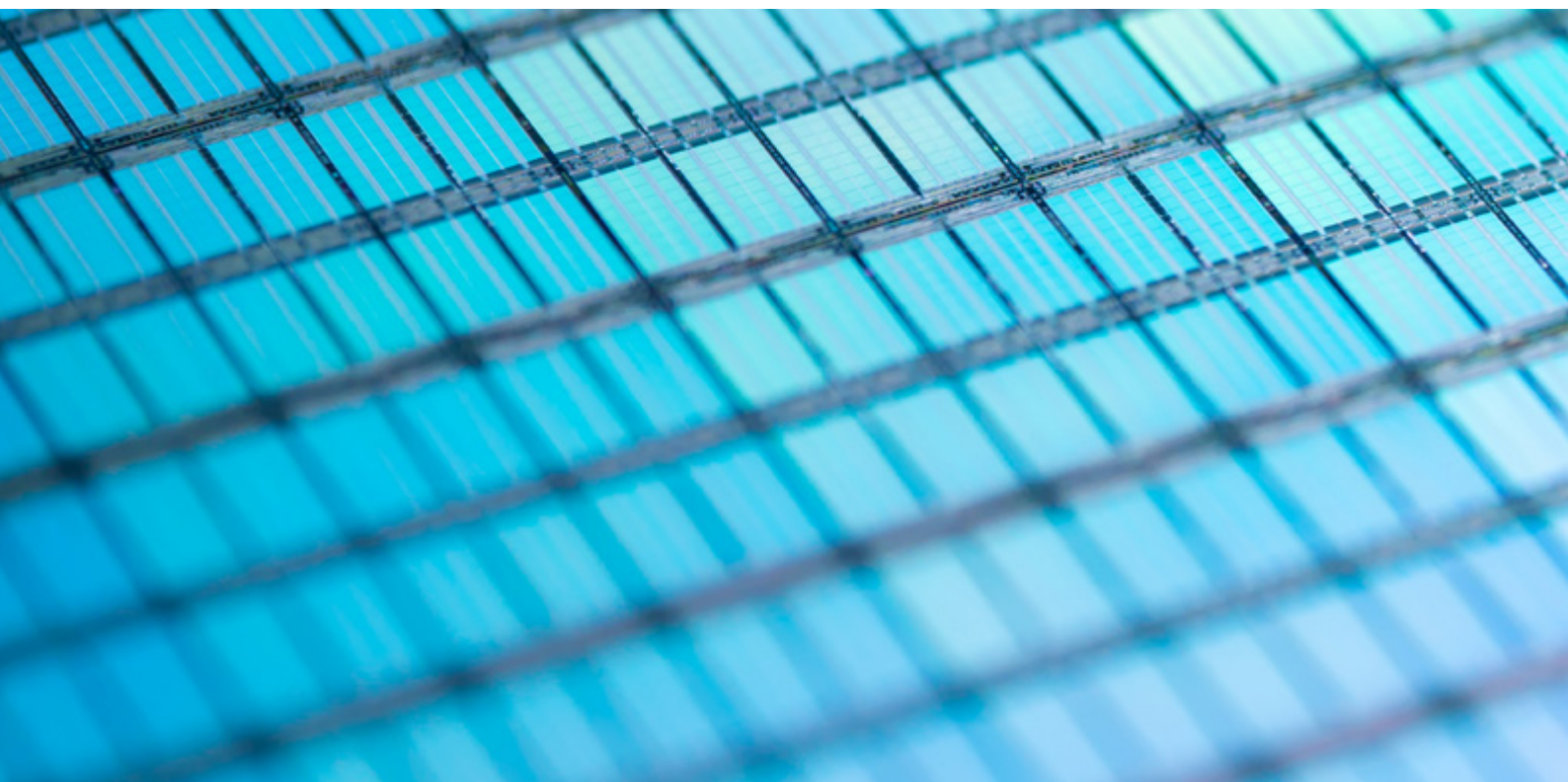
Summary

The Handbook for Development of Cybersecure IoT Products 2.0 aims to support primary and secondary stakeholders as it spans the entire lifecycle, and naturally includes the stakeholders and actors involved in all or part of the value chain from start to finish. To consider the lifecycle, requirement compilation/engineering and design require a broad and deep knowledge of how users will employ the IoT product as well as about technology from sensor level to cloud services. Cybersecurity, as well as additional holistic requirements, is a necessary part of the product specification and must be included in the functional requirements stipulated by product manager and users. In addition, it is necessary to understand how data and information generated in and around an IoT product can be used to create value through functions and services. It is also likely that such IoT products will need to be monitored, maintained, and optimized in an efficient and cybersecure manner.

This means that data and information extraction from the IoT product must be enabled and that updating, upgrading, re-configuring and optimizing can be done locally and remotely.

To do so, deep knowledge about the contexts where the IoT products are to be used needs to be combined with an understanding of how cybersecurity, and IT and OT infrastructures allow data to be transmitted and received, and how potential remote connections can be made from the outside. Thus, the management of suppliers and other stakeholders in an IoT product value chain may need to uncover and clear any obstacles to the above so that the IoT product can create and deliver good value for all involved.

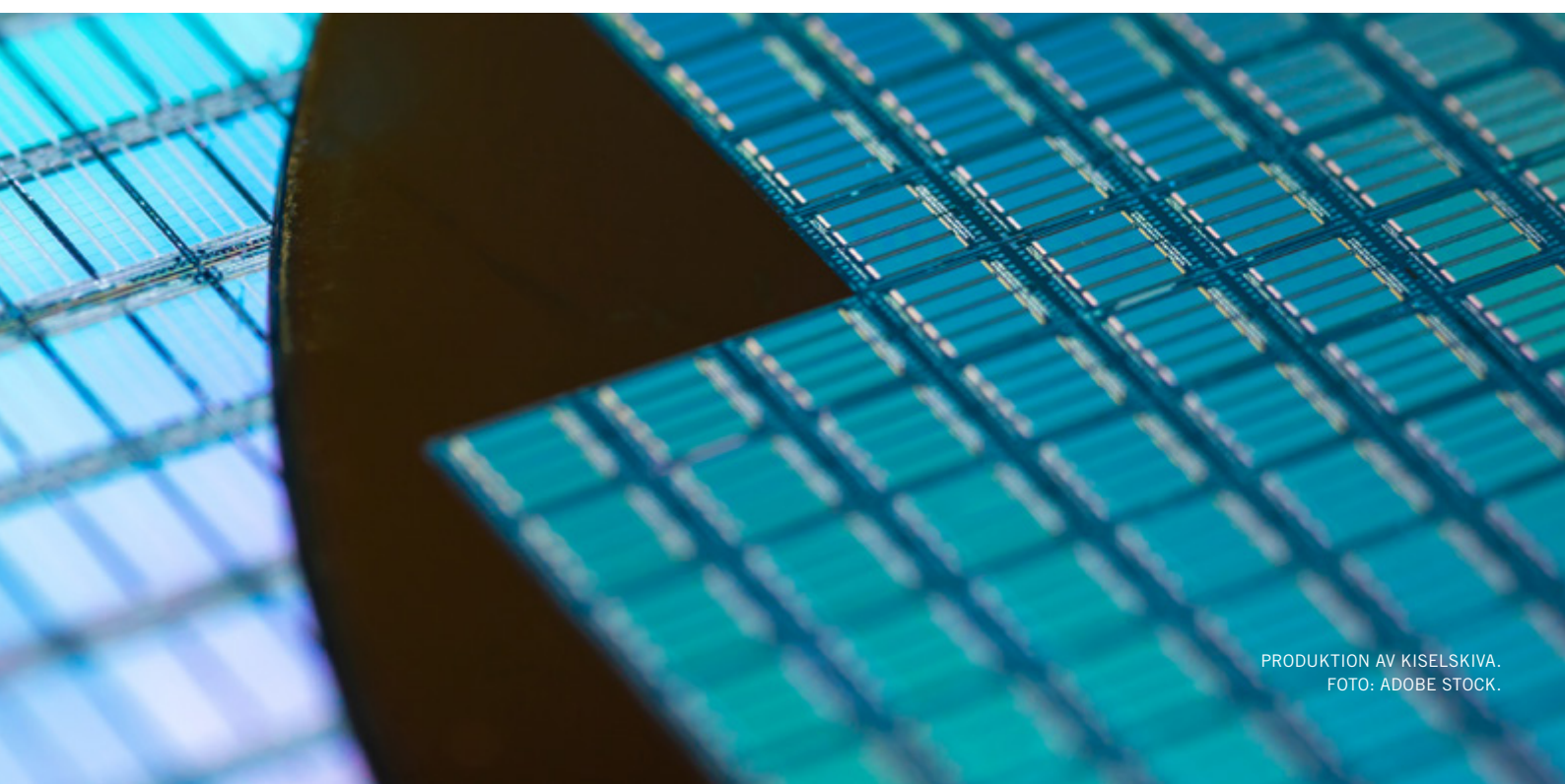
If IoT products create cybersecurity problems or risks in the contexts in which they are used, they are unlikely to be used for long no matter how good they are. Further, if it is impossible to protect them (as well as the IPR and data/information generated and stored), the expected lifecycle will be shorter. Simultaneously, protection required because of inadequate inherent protection and cybersecurity will result in higher cost and complexity for users. Moreover, extra protection will likely increase the complexity of how data is transmitted and received as well as how remote connections can be made.



Besides these many considerations, it is also necessary to understand the entire lifecycle and object owner's IT and OT environments. Please note that there is a substantial difference between IoT products intended for domestic (home) use and those used in professional contexts and critical infrastructures. IoT products for domestic use, which are often cheaper than those used in professional contexts or critical infrastructures, still need to be adequately cybersecure so as not to cause unnecessary risks. An additional difference is that, in domestic contexts, the expected knowledge threshold is lower in terms of being able to accomplish cybersecure installations and configurations. Rapid improvements in offensive AI-based tools that collect information and launch cyberattacks must be factored into the equation regardless of use and context.

The handbook addresses the processes related to the development of the IoT product, focusing on hardware and embedded software.

What is not addressed is the need for cybersecurity-related structures and processes at manufacturers and other stakeholders or actors in the value chain who help manage the IoT product throughout its lifecycle. This will involve aspects of support, service and maintenance, backup and restoring of data stored centrally, incident response planning, disaster recovery planning, and business continuity management if IoT products comprise server or cloud parts which may affect operations, availability or stored data and information. The more critical the applications and availability requirements, imposed by object owners and customers, the more robust and resilient these structures and processes must be to withstand cyberattacks and operational problems. EU legislation/regulations, such as NIS2, Cyber Resilience Act (CRA), Machinery Regulation (MR), etc., currently demand, and will continue to do so, many of the aforementioned areas or domains.



Contents

1. Introduction	8
1.1 Stakeholders	12
1.1.1 Primary stakeholders	12
1.1.2 Secondary stakeholders	16
1.2 To certify an IoT product...or not to certify it	19
1.3 Regulatory frameworks and legal requirements	21
2. Threats to IoT products, risks and principles	22
2.1 What assets do we want and need to protect?	25
2.1.1 Domestic assets	25
2.1.2 Professional environments	25
2.1.3 Critical infrastructure	26
2.2 Weaknesses and vulnerabilities	26
2.3 Use of AI/ML tools, AI agents and agentic AI in organizations using data from IoT products	28
2.4 Common threats	28
2.5 Risk analysis and risk mitigation	30
2.6 Principles for cybersecure design of IoT products	31
3. Before starting up a new project	34
3.1 Early stage	34
3.2 Requirement analysis	35
3.2.1 Industry standards and standards that can be useful and provide guidance to cybersecurity requirements	36
3.2.2 Practical functional and environmental requirements related to cybersecurity	38
3.2.3 General cybersecurity requirement for IoT products	40
3.3 Management responsibility	45
3.4 Cybersecure development environment and development process	45
3.5 Requirements on documentation	46
3.6 Test requirements	49
3.7 Maintainability over time	50
3.8 Quality level and what affects the level?	51
3.9 Requirements from industrialization	51
4. Supplier process to collate all requirements, achieve an adequate requirement specification and verify the requirements	52
4.1 Feedback and verification	52
4.2 Public procurement	53

5. Cybersecure development.....	54
6. Post development	58
7. Lifecycle monitoring of the IoT product.....	62
8. End (or a new start) of the lifecycle.....	66
9. Use cases	68
9.1 Use cases with concrete examples	68
9.1.1 Use case – domestic	68
9.1.2 Use case – industrial organizations or corporations with production and distribution processes.....	71
9.1.3 Use case – maritime industries	74
9.1.4 Use case – municipalities	76
9.1.5 Use case – critical infrastructures.....	78
10. Suggested reading.....	80

1. Introduction

The idea for this handbook, which set out as “*Smartare Elektronikhandboken 2.0*” was crafted to meet the increased global threat to IoT (Internet of Things) products. As the two handbooks are complementary, it is advised to read them both before starting new development projects related to IoT products.

The following general definition of “IoT product” will be used in the handbook: intelligent and connected units that communicate and transmit data over the Internet. The units are equipped with processors, sensors and software so that they can perceive their surroundings, communicate with it, and thus create a behavior adapted to various situations to be able to contribute and create attractive and helpful surroundings/environments, products and services¹.

The handbook arose from a need for increasingly cybersecure IoT products due to expanding malicious activity among hobby hackers, professional hackers as well as state-supported intelligence organizations that steal information, profit from or disrupt operations/processes, for instance at critical infrastructures, municipalities or counties, in target countries. In addition, new offensive AI-based tools can quickly find vulnerabilities, as well as plan and execute cyberattacks at relatively low cost and effort. These can no longer be dismissed, and we must adapt ourselves and our IoT products to such circumstances.

Below are scenarios for different contexts where IoT products may be used and possible consequences of not cybersecuring them:

Domestic (homes) – a cyberattack can cause connected fridges, stoves, heating systems, TVs and home computers to stop working or lock. In tenant-occupied buildings, common systems, such as building automation (control systems for water/sewage, heating, electricity, ventilation, locks, etc.) can be affected and, at worst, stop functioning.

Further, cars and garden equipment nowadays are often connected and need to be cybersecure no to cause physical damage or fires due to malicious overloading of components or systems.

In office spaces – as well as office computers, various IT systems and networks that may cease to function, elevators, locking/alarm systems and building automation control can be affected partially or fully. Conference room equipment can be tampered with and conversations recorded or tapped using the microphones in computers, mobile phones or conference equipment.

In production/distribution environments – the IT environment (used by offices and administrative processes) is often connected to the operational technology (OT²) environment (used by production and distribution processes). Production planning is often done and administered in the IT environment and subsequently sent to the OT environment where production or distribution is executed. An OT environment, which usually comprises many IoT products, may, like an IT environment, be affected by different types of cyberattacks that impact operational availability and integrity, quality of output, or completely stop/disrupt the operations. Indeed, the OT environment can be negatively affected if the IT environment is under cyberattack as no new order data is transmitted and no production/distribution data are received in return. Thus, production might stop when the buffered order data has been executed or produced and there is no new data to continue with. Such cyberattacks seriously affect, destroy, or wipe all data in the production equipment. Further, some production or distribution environments may experience serious issues caused by long unplanned stops due to material becoming stuck or stale inside piping or other equipment, which then needs to be fixed or replaced.

¹ <http://www.swedishembeddedaward.se/register-to-compete/definition-of-iot/#:~:text=IoT%2C%20the%20Internet%20of%20Things%2C%20is%20a%20collective,that%20communicate%20and%20deliver%20data%20across%20the%20Internet>

² OT – Operational Technology – to compare with IT – Information Technology

Examples of such material are pre-stages of pulp and paper, plastics or food. In addition, certain other environments exist, similar to OT environments, in health care but are referred to as MT³ not OT. Below in this handbook, we will use the term OT for all such environments as the main principles are the same for all these environments.

Critical infrastructures⁴ (production/distribution of energy, water production/wastewater management, telecommunications, roads/railways/ bridges/ ports/airports, food production/ distribution, etc.) – in a similar way to the above production/distribution environments, collaboration between IT and OT environments is necessary. The difference here is that stoppage in these OT environments can rapidly affect large parts of society. However, most of these OT environments should be designed to be able to continue to operate, without functioning IT environment, by using reserve procedures (and historic data).

For instance, if energy production/distribution is disrupted for more than 2–3 days, this will have a considerable impact as the lack of electricity and electronic communications will affect almost everything in the long term. Further, some of these OT environments are too sensitive to be connected to the IT environment (or Internet) and use their own networks or public services that employ high-grade security measures.

The need is increasing to cybersecure IoT products to ensure they work over time in domestic, professional and critical infrastructure scenarios and contexts.

Figure 1 shows that the increasing pace of digitalization, combined with the growing use of IoT products, outruns the development of related cybersecurity. Thus, the gap continues to grow bigger. However, the handbook will highlight a number of positive factors that can close the gap over time.

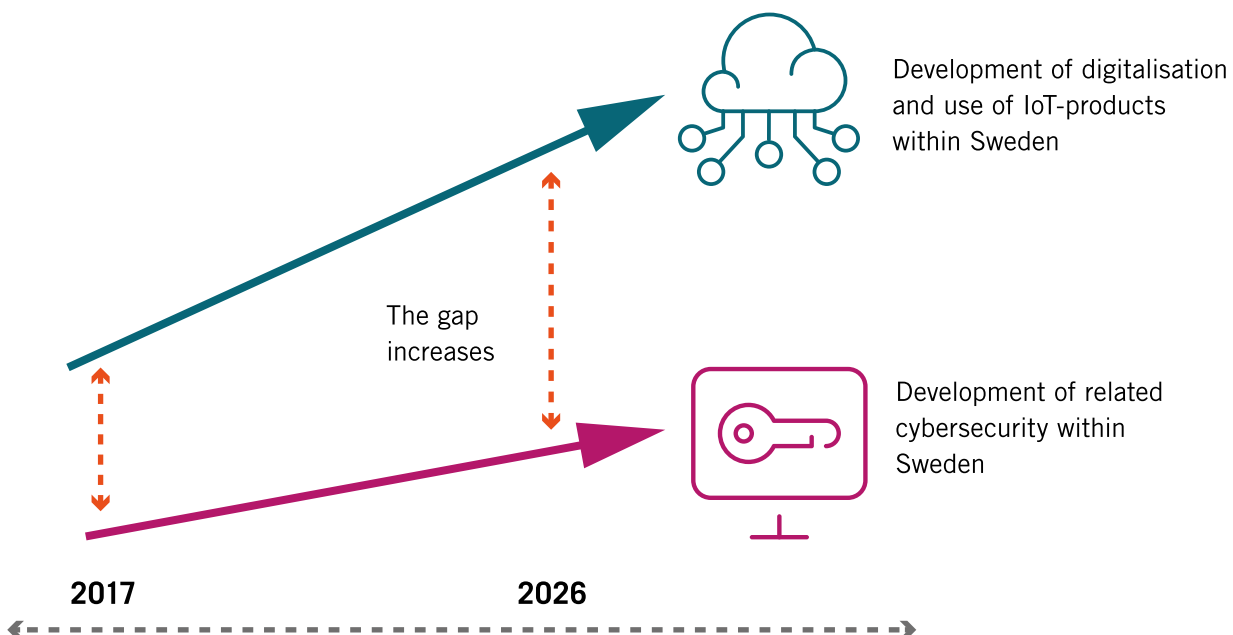


FIGURE 1 – INCREASING GAP BETWEEN SWIFTLY INCREASING DIGITALIZATION, COMBINED WITH INCREASED USE OF IOT PRODUCTS, AND THE DEVELOPMENT OF RELATED CYBERSECURITY IN SWEDEN.

³ MT – Medical Technology

⁴ The Swedish Civil Defence and Resilience Agency defines processes of importance for society where critical infrastructures are used according to: <https://www.msb.se/sv/amnesomraden/krisberedskap--civilt-forsvar/samhallsviktig-verksamhet/vad-ar-samhallsviktig-verksamhet/>

For many years, Smarter Electronic Systems and a number of actors have created and issued advice to the electronics industry on how electronics can be developed and manufactured by multiple actors collaborating in value chains. The latest piece of advice is available as the Smartare Elektronikhandboken 2.1, which focuses on the interface between development and manufacturing to achieve efficient collaboration in the value chain. The objective is better products with higher quality, lower manufacturing costs and faster time-to-market. Currently, we see a need to update and expand the advice with a Handbook for Development of Cybersecure IoT Products 2.0, as IoT products are an important part of the digitalization of our society and economy, where both things and people are connected, can communicate and report about their status and surroundings. Through this handbook, which complements the contents of the Smartare Elektronikhandboken 2.0, the IoT industry will be able to improve the cybersecurity of its products from the very start. Further, it should be possible to continuously improve and augment cybersecurity throughout the lifecycle. This requires properly considered initial design and planning for further development and maintenance so that updates, upgrades, and improvements can be issued and deployed over time. As cybersecurity is improved, the quality of IoT products will also improve due to new requirements and increased testing.

The primary stakeholders for the handbook, which are further described in section 1.1, are:

- Designers and developers (hardware and software), project managers, testers, documentation specialists and consultants
- Buyers
- Product owners
- Product managers
- Object owners

The secondary stakeholders for the handbook are:

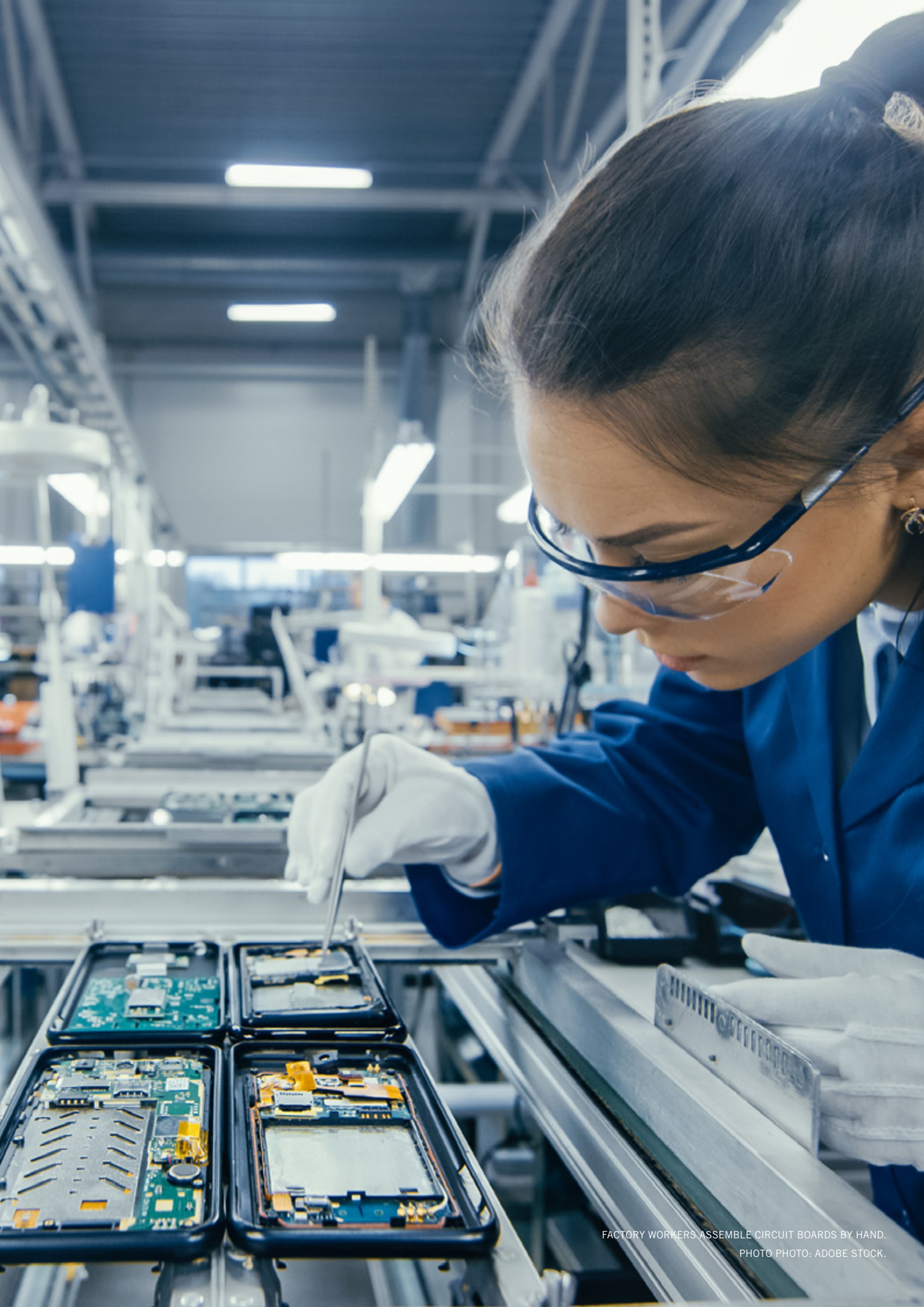
- Manufacturers
- Installers
- Maintenance, service and support as optimization services teams

- Recyclers
- Authorities, who themselves are users and potentially also have a regulatory review/inspection responsibility

Collaboration and communication among groups of stakeholders are essential for IoT products to be developed and cybersecured. Participants need to understand that in addition to cybersecurity concerns, if any requirements that affect the management of IoT product lifecycles are missing or deficient, then the long-term effects will be: higher costs, difficulties related to cybersecurity issues, and unnecessary friction between object owners at customers and suppliers. As it is in the interest of all stakeholders to avoid such a scenario, they need to collaborate on the set of requirements to enable rational life-cycle management for each involved stakeholder and other parties that may be involved. Some of the stakeholders need to understand which legislation and regulations that apply as well as the industry standards and best practices that are suitable (or required). The secondary stakeholders need to be involved early as well. They need to be informed and to be able to manage IoT products adequately during their phase of the lifecycle and ensure that their cybersecurity level is correctly commissioned and configured. A simple way to keep collaboration and communication alive is to document all that is of importance (and share it).

The focus and scope for handbook are:

- To address the lifecycle of IoT products and cybersecurity requirements for developing a new IoT product to enable a long lifecycle with high availability.
- To provide advice/checklists/standards/methods/best practices for use by hardware and software designers and developers (as well as their managers) who are not experts on cybersecurity. The emphasis is on the T in the IoT products.
- The scope extends to a moderate level of practical and structural advice concerning cybersecurity when developing IoT products. The advice should be easy to read and digest.



FACTORY WORKERS ASSEMBLE CIRCUIT BOARDS BY HAND.
PHOTO PHOTO: ADOBE STOCK.



- IoT products vary in extent and other limits, from local, with limited local functionality, to global, transmitting data to cloud services, where the data is used to optimize the IoT product's function as well as the process it is part of. The handbook addresses this and how hardware, local software, and configurations/settings can be continuously maintained in a rational and cybersecure manner.

Chapter 10 comprises explanations of technical terms and abbreviations used for IoT products.

1.1 Stakeholders

Many stakeholders participate in the value chains in which IoT products are developed and later used. Outlined below are a number of the stakeholders who can significantly impact the development and operational requirements used for the design of IoT products. The focus is on the stakeholders (or other actors) who participate throughout the lifecycle of the IoT, including decommissioning and recycling. The primary stakeholder group are designers and developers of hardware and software. A number of secondary stakeholders are also outlined.

1.1.1 Primary stakeholders

1.1.1.1 Designers and developers, project managers, testers, documentation specialists, and consultants

When an IoT product has progressed so far that a set of requirements has materialized, a suitable group of people is needed to develop it. It is common to bring in open-source code and open design of hardware, which may speed up parts of the process, but also requires sufficient competence to further develop and assess whether the potential open-source code or open design is safe, cybersecure and applicable for use. The stakeholder groups and sub-groups are briefly outlined below:

Designers and developers of hardware and software – designing and developing hardware and code, as well as using hardware and code developed by others, ensure that the right functionality (based on requirement specifications) is achieved and cybersecure. This is not easy and requires continuous training and intelligence gathering related to cyberattack progression and cybersecurity in general. Failing to do so may result in IoT products that become dangerous or non-acceptable

among customers when this is revealed. In cases where open design or open-source code is used, a manual review is often needed, with suitable tools, to verify that no malware has been inserted. This needs to be verified for each new version, and may be a considerable undertaking if open design or open-source codes are widely used. Further, hardware components, various chips or semi-conductors, and ready-to-use circuit boards that have been procured should be tested and verified so that they only do what they are supposed to do and not have any extra functions (this applies in particular if they have been developed/manufactured outside the EU in for example low-salary or non-democratic countries). Thus, designers and developers need to improve their testing and verification skills, not only for what they do themselves, but also for external hardware or software. They should add additional cybersecurity test cases and try to automate as much as possible. Automation enables rapid testing, coverage, and repeatability. Thus, the automation of development testing and increased use of test suites and/or test rigs simplify testing/verification of in-house and external development.

Developers of services, processes, and other necessary supporting structures – IoT products may vary from being merely a product with a warranty to those based on an advanced and value-creating business model. Developers of hardware and software can contribute to the development of such services and processes that together support the structures required for the IoT products to operate over time. However, as the development of services and processes differs somewhat from the development of hardware and software, other competences may be needed along with an understanding of the entire lifecycle, value chain, and how these need to be improved in years to come. As a basis for services and processes in the supporting structures, a mix of existing tools and services can be used together with ones developed locally. Examples of services and processes that can be conducted on-site or remotely include: support, service, maintenance, training/education (for own staff, customers or others in the value chain),

fleet management functionality with monitoring and added value creation, and efficient functions or services (see Chapter 7 below for more on this). A supportive self-help guide for problem solving, an FAQ, instructions, videos, virtual/augmented reality that can be consumed via the web or an app are all valuable time-savers for developers and users.

Project managers – a project manager is commonly assigned the responsibility for developing an IoT product based on a requirement specification. The expected outcome should have a certain level of cybersecurity and quality. To do so, resources are assigned together with a deadline. Supporting the project manager are roles such as product managers and other relevant parts of the value chain.

Testers – testers are needed not only for crafting test cases pertaining to the basic functionality, which should preferably be tested as a combination of automated and manual tests. This requires the knowledge and ability to craft test cases for advanced cybersecurity as well. The testers should conduct various forms of penetration tests, tests of availability/performance, and which information can be extracted/exfiltrated by different measures such as faulty logins. Hackers who might attack an IoT product use a plethora of tools, ranging from very simplistic to those based on advanced AI, which the tester needs to be aware of. Potentially, a shielded lab may be needed for such testing, using hacking tools to provide a comprehensive understanding of reality, to determine how test cases should be designed, and to detect how common cyberattacks might be designed, planned and executed.

Documentation specialists – documentation specialists also need to be able to understand recent and relevant cybersecurity for IoT products. If cybersecurity is not integrated into the description of the basic functionality, an extra chapter or appendix may be added to the manuals to outline how the architecture is set up and how to apply cybersecurity in and around the IoT product (if it is normally connected where many other objects and systems operate).

It is advisable to describe the inherent cybersecurity functionality, how to install/commission and configure it adequately, how to update/up-grade it, and how to verify that the cybersecurity functionality is correctly configured and working. For the latter, specific procedures or scripts may need to be developed and described.

Consultants – consultants are often added to strengthen the development team in design, hardware or software development, testing, documentation or project management, etc. Commonly, consultants split their time between different customers (and development teams), who may be suppliers of IoT products or similar, and may even be competitors, which requires certain matters to be addressed. Intellectual property rights, patent ideas, and patterns/copyright (i.e., IPR) must be protected such that cybersecurity is not negatively affected if consultants are team members or part of maintenance later on. Thus, secrecy and confidentiality agreements need to be established as well as guidelines on how to implement related cybersecurity and instructions/awareness.

Whether or not consultants should be on premise together with the rest of the team or work remotely is another consideration. Any consultancy agreement should require that consultants have good knowledge of cybersecurity when developing IoT products.

Others – development teams may comprise many different roles and categories of staff, ranging from CEO, CTO, CISO, development managers, program management, project management and sales representatives, who might present customer requirements, to cleaners and janitors who are in the proximity of the development team.

For all these, cybersecurity, and protection of IPR and secrecy must also be set up in a similar manner to the requirements for consultants.

1.1.1.2 Buyers

Initially, it is never easy to foresee how an IoT product is used, although a certain use is expected and prescribed. Solutions to new, and old, issues that were not part of the framing of the initial thought process will always appear and spur the continuous development of an IoT product. It is always advisable to listen and talk to customers and users regularly to remain updated on needs, how the IoT product is used, what can be improved and what might be missing. With respect to buyers, a number of part stakeholders may be involved who are not up-to-date and fail to understand how an IoT product should be used and what requirements are made by its surroundings. In such cases, it may be useful to offer help and ask questions to identify needs related to the IoT product and its future use. Potential part stakeholders at a buyer may be:

Procurement – procurement officers do not always have the required specialist knowledge and follow a simple or limited procurement process. In this context, support may be needed to ensure that cybersecurity is also included in the requirements from start as it is usually difficult and expensive to add these later on. Moreover adding cybersecurity requirements later will not render as good a result as when they are included from the beginning. To avoid issues and the high costs related to them, procurement officers should ensure that from the outset, the required competencies in IT, OT and cybersecurity are part of the process.

Function/process owners – these roles participate in processes and ensure that activities and tasks are executed using various forms of equipment and tools where IoT products may be present. In addition, IoT products may be part of monitoring such functions/processes to ensure that all work and quality exceeds expectations. Examples of such are controls for functions and processes and, for monitoring, sensors and cameras may be used.



RENEWABLE ENERGY SOURCES ARE IMPORTANT IN THE DEVELOPMENT OF IOT.
PHOTO: ADOBE STOCK.

Technology/development department – customers often have a department managing technology/development matters that can build up production and distribution lines and adapt technology for these. Employees in such departments often have good knowledge of both functions, processes and technology, which makes them an important part stakeholder to discuss with and interview.

Operations and maintenance/service – those who work in operations and maintenance/service are most in contact with the IoT products. The operations/use phase is also the longest phase of the lifecycle for an IoT product. These employees understand well how an IoT product can be efficiently installed, commissioned, configured, updated/upgraded, changed, decommissioned and generally maintained. These stages should be easy to execute efficiently, for instance by having a set of well-working fleet management functions, to lower the lifecycle cost of an IoT product. A low lifecycle cost makes an IoT product more interesting than competing IoT products and, in particular, if these lack fleet management functions.

Thus, it may be advantageous to talk to various part stakeholders at buyers as they may have minor pieces of information that complete the bigger picture. They are also a good source of ideas for how to lower the total lifecycle cost for customers.

1.1.1.3 Product owners

The company that owns the IoT product and releases it on the market is responsible for ensuring that CE marking conditions are fulfilled and that legal/regulatory requirements are met.

1.1.1.4 Product manager

On the supplier side of an IoT product, it is advisable to assign a role that is responsible for the product's requirement engineering (and perhaps for similar products in a family) throughout their lifecycles and is thus the pro-longed arm of the product owner. Having a clear responsibility and authorization to manage the IoT product makes it a lot easier from the start to define the right

requirements for development and subsequently add requirements until the end of the lifecycle. Commonly, product managers manage requirement engineering and continuous requirement collation as well as strategic development planning (e.g., in the shape of a roadmap). They also act as the link between customers, development, sales representatives, and other stakeholders. Further, requirement specifications are usually managed and compiled by a product manager.

1.1.1.5 Object owner

The buyer side may appoint object owners, who are responsible for IoT products or have budget responsibility to maintain them and other assets residing in production or distribution environments. After installation and commissioning, object owners are responsible for maintaining and updating the IoT products until they are decommissioned and end-of-lifed, or are transferred to another object owner. The object owners often work closely with function/process owners, who have the wider responsibility to ensure that what is to be accomplished is executed on time at the required quality and availability levels. Object owners may not always consider cybersecurity, but are increasingly forced to do so because it is necessary to plan for internal, external and remote access, redundancy, backup/restoration, and logging, etc.

1.1.2 Secondary stakeholders

No chain is stronger than its weakest link. If many secondary stakeholders are involved in the value chains, they will need both physical security and cybersecurity. This should be part of the value chain agreements, and the implementations should be reviewed regularly to avoid increasing risk exposure. Below are a number of potential secondary stakeholders, some of which are integrated into the supplier solution (developing the IoT product) where the supplier has integrated the entire vertical and horizontal value chain with the customer's IT solution. However, it is common to see a number of external parties acting as secondary stakeholders.

1.1.2.1 Manufacturers

If manufacturing is done internally and in their own factories, it is easier for manufacturers to maintain an adequate level of cybersecurity around and in the production environment while protecting the information necessary to produce an all, or parts, of IoT product. An IoT product may be very simple or advanced. Further, the line between when it is an IoT product and a cyber-physical system is unclear. One definition of cyber-physical systems is that they many co-operating systems (i.e., systems-of-systems) whereas the in-the-middle level OT systems control, participate, or in other ways affect a physical process. Regardless, the production environment must be protected to ensure that it is kept confidential, unauthorized changes in the manufacturing process or process parameters cannot be made, and processes run without disruptions and stops as these can negatively affect the output quality and lower output volume. Further, physical security in and at the perimeters of production facilities and factories need also to prevent burglars, theft, as well as sabotage of electric supply, ventilation systems or water pipelines.

If outsourced manufacturing is used, production facilities and factories need to have the same levels of physical security and cybersecurity as their own factories. It is different if standard components are outsourced compared to whether there is IPR, such as hardware designs, software or knowledge related to the production process, which must be protected and kept confidential. Thus, sometimes it is unsuitable to outsource outside of trusted production facilities and factories or to countries outside the EU, where political pressure or involvement may endanger the confidentiality of IPR.

Thus, an assessment of physical security and cybersecurity is recommended at least annually to ensure that outsourcing is executed as desired and that the physical security and cybersecurity levels are sufficient.

Outsourcing also requires that any external manufacturer contracted is regularly reviewed as a whole. This should be part of the procurement or supplier review processes.

1.1.2.2 Distributor

When manufactured, an IoT product can be stored and distributed fully or partly by a company's own means, or by using an external distributor or distribution solution. For simple IoT products, this is not very complicated, whereas for IoT products that may also carry spare parts/components or software and manuals requiring regular updates, it is also advisable to consider this to be able to maintain physical protection and ensure that no unauthorized persons can access the IoT products, spare parts/components, software or manuals. If a virus or malware is added to software updates or manuals (if these are executable or readable files), it can cause significant problems for object owners at customer and the supplier sites (no matter whether the distribution is manual via service/support staff or downloaded from a portal or cloud service). When hardware, software, and manuals, etc., are distributed, the processes are required to check/verify that no unwelcome or unauthorized elements are added.

Further, IoT products may have added services, such as maintenance, service, support and optimizations. Some of these services are executed on premise and some remotely using data that may be transmitted to a cloud service. If these services engage their own staff, external distributors/executors, and if any cloud services used are hosted by an external cloud service provider, the requirements for physical security and cybersecurity need to be applied here. See more on this further below.

1.1.2.3 Installers

If the customer or supplier does not conduct the installation and commissioning, it is common to use external installers. Like any distributors, these need to have adequate physical security and cybersecurity if they have a supply in stock and use this for the installation. They also need to keep any software required in their own portal or cloud service. Installers need continuous education and training on the IoT product and its installation, configuration and commissioning.

They also need to build and maintain general awareness about cybersecurity (both physical and cybersecurity). If the IoT products are to be installed in sensitive operations or processes that require very high availability, the installers need to ensure that no one else can access the IoT product or its various components. Further, installers need to know what to do when they decommission and replace old IoT products with new products or other solutions. Potentially sensitive data, configurations, control data, etc., must be wiped or removed so that no one else can detect what the IoT product has been used for or provide data about the old operational environment (i.e., networks, IP addresses, connections). Some IoT products may need to be destroyed/dis-mantled completely if it cannot be verified that all sensitive data and configurations have been completely wiped or removed. A product manager or object owner should interview the installers about potential improvements of the installation, configuration and (de)commissioning.

1.1.2.4 Crews providing add-on services – service, support, maintenance and optimizations

Common value-adding services for IoT products in value chains are support, service, maintenance and optimization of hardware or software, and the processes where IoT products contribute. Further add-on services, such as re-engineering of processes and integrations with other solutions, are common. Valuable ideas can often be found for improving IoT products among the part stakeholders here as they manage the IoT products during the longest phase of the lifecycle and can clearly see flaws and areas for improvement, and can compare them with the competitors' IoT products and solutions. At the service and support phase, when some IoT products may be replaced, it is important to ensure that sensitive or IPR-related data or information is erased. This situation is similar to the one for installers. A product manager or object owner can have a fruitful exchange of ideas and learn about flaws and potential improvement opportunities related to how IoT products behave while in operation.

Add-on services can be provided on-site or partly remotely (using remote access and tools). If on-site, there must be insurance that no viruses or malware are brought in, and the providers and the customer's users need to agree on how to maintain the cybersecurity of the processes. In many instances, files or other external items on external lap-tops, USB sticks/disks or mobile phones are not allowed, and other secure procedures are needed. The staff at customer site also need to ensure that the service providers only do what they are allowed to do and not collect data or information from the competitors' equipment and solution environment or about processes and process parameters they should not have access to. The trend to increasingly do more remotely through external connections, such as low-level or high-level VPNs, saves time and costs as travel distances to may be long at while the time to provide the service is relatively short. This means that customers need to maintain strong control of whom they allow to access remotely and have a standardized approach to such access. Such a standard may encompass time limitations, access only during normal business hours, and removal of inactive user accounts. For acute problems, rapid activation for external connections with a short life span can be put in place. Further, suppliers often collect data in a central cloud service to help part stakeholders at customer sites with process analysis outcomes or operational details, process optimization and process parameters, to find signs of wear and tear as well as maintenance needs or equipment replacement. In addition, maintenance, updates of software upgrades and re-configurations are often carried out this way too. Some customers want to have their own local servers in own data centers (on-premise) and not use external cloud services or the supplier's central servers. However, this depends on factors such as: who owns the data, who can do what with the data, who has access to the data, all of which should be part of any agreement. In the future, ownership of, and access to, data will become increasingly critical and be central to data-driven business models. This will become even more important through the increasing use of AI/ML,

AI-agents and agentic AI. Thus, the locations where the data and information are stored must have suitable physical security and cyber-security. This goes for whether storage is local, in a cloud service or on supplier servers.

1.1.2.5 Recyclers

IoT products need to be partly or fully recyclable as they near the end of their physical life-cycle. Instructions for how to do this should be in the user manual and marked on any original packaging. As IoT products are to be recycled, they firstly need to be wiped or emptied of any data and information. Some parts need even to be physically destroyed or dismantled. This is because certain types of memories and disks can be hard to wipe/erase completely. Further, no IPR of high sensitivity or value should end up with competitors or those who want to hack their way in. In such cases, memories or disks need to be shredded or crushed. When this is done, remember to facilitate the next step i.e., recycling. Thus, it is advisable to provide clear instructions and refer to similar rules, instructions or policies of the object owner or user organizations concerning the management of data or information at the end of the lifecycle. See also Section 3.5 and Chapter 8 for more on this matter. Object owners and users usually have a process for recycling. If there are deviations from the normal process or instructions, it needs to be brought up with management.

Please remember that if an IoT product is deposited in a general bin at a recycling facility, it is beyond the control of the owner. If necessary, additionally cybersecure and protected storage may be required before recycling.

1.1.2.6 Authorities – who are users and/or have regulatory review responsibility

Authorities may have a dual role in contexts where IoT products are used. They can be users in various forms of critical infrastructures and may also be the regulatory reviewer that visits and reviews actors who use IoT products in their processes. Thus, they need a sound knowledge of cybersecurity related to IoT products and the contexts in which they are used.

Examples of such authorities in Sweden are The Swedish Food Agency (water production), The Swedish Post and Telecom Authority, The National Electrical Safety Board and Swedish Civil Defence and Resilience Agency. Those who use IoT products include The Swedish Transport Administration (road network, railways, and waterways), Swedavia (airports), municipalities (road network, water and sewage systems, buildings, and health/elderly care) and counties (health care, buildings, and a lot more). Further, the National Cyber Security Centre (NCSC) will subsequently assume collective responsibility for cybersecurity in Sweden and the current activities at the Swedish Civil Defence and Resilience Agency be transferred to it.

1.2 To certify an IoT product... or not to certify it

Why should an IoT product be certified? More obvious reasons include legal or regulatory requirements, e.g., GDPR and CE marking in the EU (as well as the upcoming EU Cyber Resilience and Cybersecurity Acts), or industry requirements, which are expected to be able to market the product. Further, in the UK, which is a large market in Europe but outside the EU, UKCA marking for products is required from the December 31, 2024, similar to CE marking. See below for more on these industry requirements in the bullet list. Further, certain customer segments may have specific requirements, or more or less have to buy certified products, to demonstrate that they fulfill the requirements stipulated in the next step of a value chain (from authorities or customers). In addition, boards of directors and owners of businesses or organizations have become more aware of this issue and sometimes initiate various cybersecurity-related certifications, e.g., ISO 27001 or IEC 62443, for their own business or organization. Subsequently, they need to review which equipment, IoT products, software, etc., that they use and market themselves, and provide certifications that may be required pertaining to these. Thus, a certain measure of proactivity has been sparked with the intention to provide advantages in business development and

marketing, so that, at a later stage, their offering will not be filtered out early in the sales process (or disqualified as offering) because verified cybersecurity levels are too low.

Certifying an IoT product costs time, effort, and money. Thus, this needs to be thought through to provide greater output value than input in the process. Before beginning a certification procedure, good practice is to query colleagues and friends in the same business as well as certification auditors (for the appropriate standard) to determine the cost of certification and the calendar time required.

Certifying an IoT product may provide advantages as some tasks or processes can be minimized or eliminated. These includes sets of queries from customers, as part of qualification steps or pre-procurement information collection, as procurement staff can easily read or access clear information about which certifications the IoT product has. This step alone can minimize input of 10–100 hours each time as queries are seldom identical. Further, well-selected and appropriate standards provide a clear view of the cybersecurity status.

Below are examples of standards for cybersecurity that are applicable to IoT products in a number of businesses or segments:

- **Domestic/consumers** – ETSI TS 103 645/ TS 103 701, ETSI EN 303 645, and SSF 1120-1
- **Intelligent cities and buildings** – Swedish Association of Local Authorities and Regions, information security related to property management & IoT, 'Arkitektur-gemenskapens' reference architecture for IoT (for smart city och digital twins)
- **Health care** – IEC 81001-5-1, and MDCG 2019-16 (medical technology equipment)
- **Food and beverage including production and distribution of clean water** – IEC 62443 3-3, 4-1 and 4-2
- **Financial** – PCI-DSS
- **Vehicles** – ISO 21434 and UNECE R155

- **Municipalities, counties, and government agencies** – Swedish Association of Local Authorities and Regions/RISE, (KLASSA for IoT), SSNF Robust och secure IoT (city net in Sverige), Traficon (Finnish transport and communications networks)
- **Critical infrastructure** – IEC 62443 3-3, and ISO 27019
- **General**
 - ISO/IEC 27400 (IoT security and integrity), SSF 1120 (theft protection for connected IoT products), SSF3523 (digital locks), ioXt Alliance (certification program for secure IoT products), and IEC 62443 3-3, 4-1 and 4-2
 - EU Cybersecurity Act, a framework comprising cybersecurity requirements for certification
 - EU Cyber Resilience Act, which sets requirements for the inherent cybersecurity of a product during its whole lifecycle
 - EU Radio Equipment Directive (RED), which will apply to all IoT products that can (wirelessly) communicate electronically August 2024
 - ISO 27017/18 (security for cloud service environments as data generated by IoT products are often stored in such services)
 - ISO 27032 (guidelines for Internet security)

Within the scope of this handbook, we will remain close to certain standards that are suitable and provide support during an IoT product's lifecycle, and use these for support, for instance, in Chapter 3 and its requirement analysis.

1.3 Regulatory frameworks and legal requirements

The EU NIS2 Directive, i.e., Directive on Security of Network and Information Systems, has been Swedish law for several years. The foundation for the directive is demands made on organizations that deliver services of importance to society to implement systematic risk and cybersecurity measures whereby security-related incidents are to be reported and managed adequately. In coordination with NIS2, a number of other new and updated regulations and directives have been issued by the EU (see example in Figure 2, page 23). Many of these are directly interconnected. Thus, these frameworks, directives, and acts, need to be thoroughly analyzed to create a unified set of requirements going forward. Some EU legislation and regulations are accredited in each EU country and may differ somewhat (e.g., NIS2), whereas others apply at EU level, and are not accredited, and may be altered/adapted slightly in each country. Further, the EU's Eco-Design for Sustainable Products Regulation (ESPR) will require digital product passports for hardware and software (i.e., Bill of Materials or BOM). If possible, have the BOMs compiled automatically, as part of the build or CI/CD-pipelines etc.

Examples of complimentary directives to the NIS2:

- **CER** – Critical Entities Resiliency Directive. Requirements for organizations involved in operations that are critical for society. Overlaps with the NIS2.
- **DORA** – Digital Operational Resilience Act. Requirements for resilience in the finance industry.
- **CRA** – Cyber Resilience Act. Requirements for technical equipment, with many overlaps/connections with NIS2. Further, it is relevant for IoT products in general.
- **AI Act** – requirements for responsible use of AI.
- **Data Act** – requirements that customers can access data in products and services.
- **RED** – Radio Equipment Directive. Primarily requirements for equipment with any kind of radio communications technology.
- **MDR/IVDR** – EU regulation concerning medical technology products including those for in vitro diagnostics.
- **Machine Directive** – Requirements to ensure that machines in any form are not dangerous to use. In the future, the directive will also address cybersecurity, AI use and other technology challenges in the area.

Among these, it is likely that the GDPR, NIS2, AI Act, Data Act, CRA and RED apply to IoT technologies in many areas. In cases where IoT is used as part of a machine, the Machine Directive will likely apply as well. Medical technology products are highly restricted, with strict cybersecurity requirements. NIS2 and the others focus on creating cybersecurity in the supply chains and making demands on suppliers. In practice, all parties who expect to provide products and services to NIS2 organizations need to adapt to the requirements although their own organization may fall outside the scope of NIS2. Additional requirements highlighted by NIS2 are incident response management, resilience to issues/disruptions, coordination with authorities that are responsible for regulatory review, vulnerability management, ability to measure the efficiency of cybersecurity efforts, management responsibility, and the need for competence at management level.

The NIS2 permits sanctions of up to 2% of global turnover or € 10 M to be imposed on non-compliant organizations.

2. Threats to IoT products, risks and principles

Below, we assign IoT products and the data and information to be protected in various environments the label “assets”. These assets may be in the actual IoT product or in direct proximity, and thus be affected by the function of the IoT product or the ability to launch a cyberattack through it. This will be further outlined in section 2.1.

IoT products can be used in many unforeseen contexts and applications. The handbook mainly addresses IoT products used in the following contexts, although many others exist, such as airspace, space, and military ones:

Domestic (homes) – connected home electronics ranging from smart building automation systems and lock/alarm systems, toasters, fridges/freezers, TV, gaming platforms, watches/clocks, to modern connected vehicles.

Professional environments – building automation systems and lock/alarm systems, industrial production/distribution, maritime environments with vessel functions or platforms, health care ranging from acute care to elderly care, food and beverage production/distribution, remotely by driven or completely autonomous vehicles used in various transport processes, etc.

Critical infrastructure – functions or services critical to society⁵. In professional environments and critical infrastructures, IoT products are seen by many professionals as one of the largest threats to their operations. Thus, it is crucial that future IoT products have inherently good, or very good, levels of cybersecurity so that this labelling can be removed.

Figure 2 indicates how overarching legal requirements to voluntary standards and experiences can affect an IoT product in addition to the requirements posed by object owners on customers and suppliers themselves or other stakeholders in the value chain. The IoT products shown are categorized as domestic (homes), professional environments, and critical infrastructures. Many more exist, but are outside the scope of the handbook. The point is not that there are more, but to understand that requirements do not only originate from object owners at customer corporations but also from different groups or types of IoT products of varying sophistication that may or not be connected to networks. In addition, cybersecurity and availability/resilience requirements may differ significantly between IoT products targeting domestic use and those used in professional or critical infrastructure contexts. Thus, a customer must be prepared to pay more for IoT products that target professional or critical infrastructure environments than for those targeting domestic use. Further, installing IoT products designed for domestic use, because they are “cheap” and “solve the problem”, into the other environments is not advisable and will likely be neither particularly cheap or create value in the long run.

New AI-based threats need to be considered as new AI models may have the capacity to quickly find vulnerabilities, propose attack vectors, and plan and execute large-scale attacks. Further, it may be possible to “reverse engineer” AI models to find bad code or vulnerabilities inside components and systems (and not just in the surfaces or interfaces).

⁵ See for example: <https://soff.se/samhallssakerhet/vad-ar-samhallsviktig-verksamhet/>

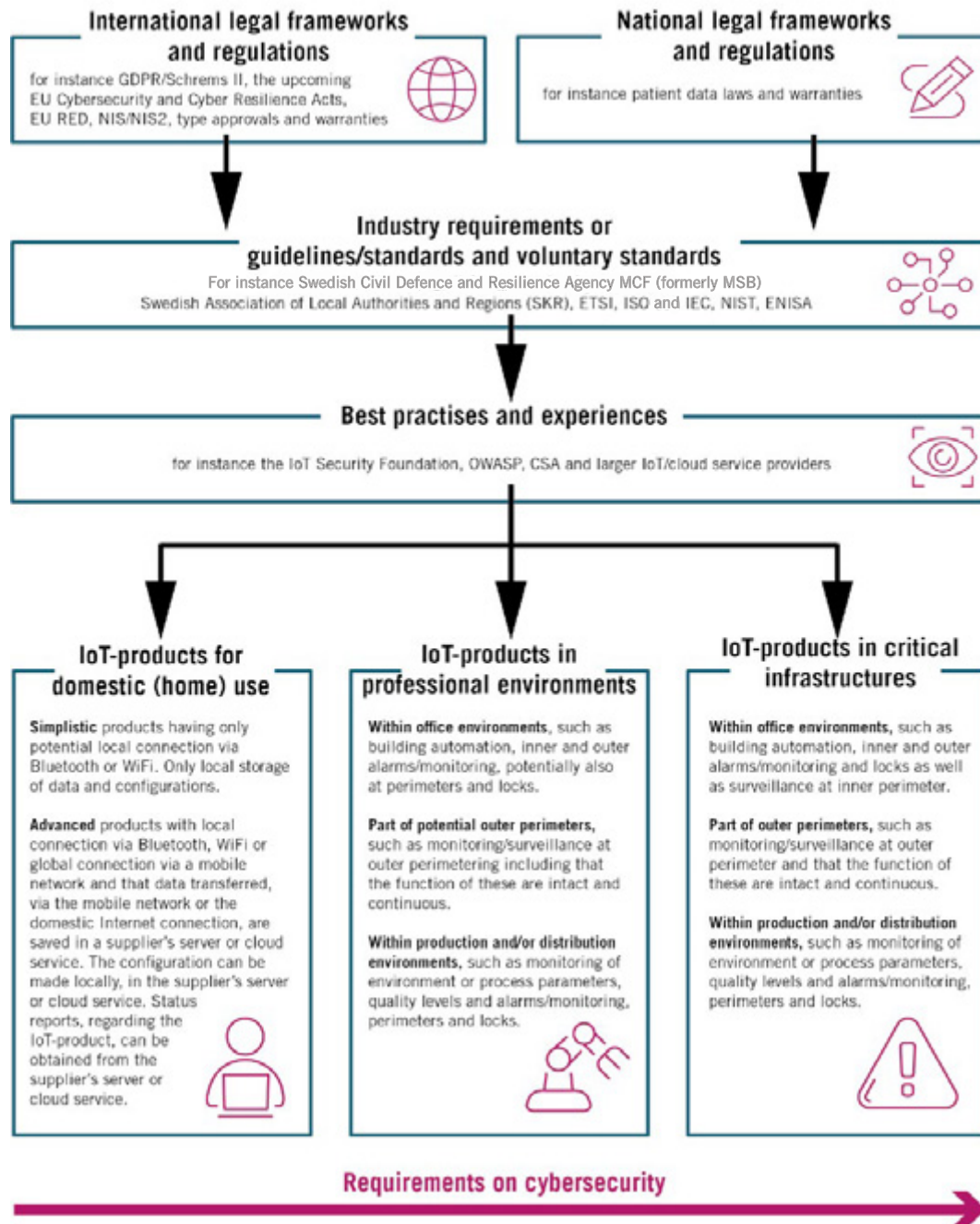


FIGURE 2 – IMPACT OF INTERNATIONAL AND NATIONAL LEGAL FRAMEWORKS AND REGULATIONS, INDUSTRY REQUIREMENTS/GUIDELINES/STANDARDS AS WELL AS BEST PRACTICES AND EXPERIENCES ON IOT PRODUCTS IN DOMESTIC (HOME) CONTEXTS, PROFESSIONAL ENVIRONMENTS AND CRITICAL INFRASTRUCTURES.



THERE ARE MANY ASSETS IN THE HOME THAT NEED TO BE PROTECTED IN VARIOUS WAYS.
PHOTO: ADOBE STOCK.

2.1 What assets do we want and need to protect?

Section 3.2 outlines different areas, or rather consequences, which are commonly discussed as assets are to be protected: confidentiality, integrity, availability, trust and traceability. There are more, but these are sufficient to start with. All should be kept in mind when considering and mapping out the assets in the IoT products or in their proximity that need to be protected to avoid likely consequences. Below, several such assets are described in brief.

2.1.1 Domestic assets

Which domestic assets are worth protecting? Data intrusion carries the threat of destroying buildings by causing fires or flooding. But data is also available about residents. Accessible via microphones/speakers and cameras, this is data that owners want to be kept confidential and its integrity ensured. During the cold parts of the year, electricity and heating systems need to function so that water piping does not freeze and cause water damage. Further, throughout the year, water and sewage, ventilation, electricity and the internet etc. should also function well. Poorly protected equipment for internet access may be an entry point to various systems and potential sensors, information about the home network's set up, and information about more or less everything that is connected to the home network. If a fridge and freezer that are not protected from water leakage are surreptitiously turned off, water damage may result. Further, a low-quality connected toaster, which is on continuously, may cause a fire. In addition, based on the data collected about the residents, attackers can analyze whether they are at home or not. To do this, data from water and electricity meters and the fridge can be used unless these are cybersecure. At worst, this may lead to unwanted visitors when residents are out. If there is an unsecured alarm system, it can be tested to check if it is activated, used to reveal what response times various sensor readings or a triggered alarm have, if sensors work and are activated, and if sensors can be shut down when desired.

There are many examples of why IoT products or solutions, often referred to as smart products, used in domestic environments must be physically secure and cybersecure.

2.1.2 Professional environments

Professional environments comprise many assets that need protection, such as data about: processes where IoT products are used as well as process parameters and configurations/recipes, buildings and their support systems, the topology of the network and the type of equipment installed in the network. Further, there may be details about operational processes, what is produced and distributed, and how this is executed. The latter might be open IPR or IPR that is confidential. In addition, for most operations it is vital to run production and distribution processes without disruption to ensure that products are of the desired quality and that nothing extra is added (unwanted software or components or other types of ingredients). Information about how well production or distribution processes operate, or do not operate, can provide information that affects markets and thus must be protected. IoT products which are poorly installed, or erroneously configured, are of considerable concern for many cybersecurity professionals in professional environments. IoT products with inadequate cybersecurity levels will become highly dependent on the cybersecurity level in the surrounding network being upgraded continuously over time. The function of an operation's IoT products and processes may be related to the trust object owners in customer organizations place in the supplier's ability to deliver as well as the supplier brand. This trust in certain cases is extended to authorities who have regulatory review/inspection responsibilities. Trust can probably take a hit or two, but in the short term sales may be lost. A severe loss of trust may be harder to cope with in the long term.



FIGURE 3 – EXAMPLES OF A SUBSET OF INFORMATION AND DATA THAT CAN BE SENSITIVE AND NEED EXTRA PROTECTION IN RELATION TO THE WHOLE SET OF INFORMATION AND DATA.

2.1.3 Critical infrastructures

Critical infrastructures comprise assets that need protection, which are subject to national laws and regulations, and must have suitable physical protection and cybersecurity. The assets may contain highly interesting data and information about the processes, facilities and networks they are used in. Commonly, these processes must be highly available, often around the clock, and the integrity of processes, recipes, configurations, etc., must be upheld and not be possible to change by unauthorized persons. Critical infrastructures require a high level of confidentiality as well, but availability and integrity are paramount.

Figure 3 asserts the need for mapping out the data and information that are sensitive and must be particularly protected. Further, there may be a need to map out the processes, systems and services that must maintain a high level of availability and integrity. IoT products are often part of a larger scheme than only the IoT product itself.

In summary, all contexts, ranging from domestic to critical infrastructures, must consider which assets should be protected. Common responses are: data and information, availability and integrity of various equipment and processes, the trust of object owners and partners, brands, etc. Thus, a supplier of IoT products needs to understand its customers' contexts and develop suitable protection through instructions and processes in combination with functionality to achieve the required level of protection and cybersecurity.

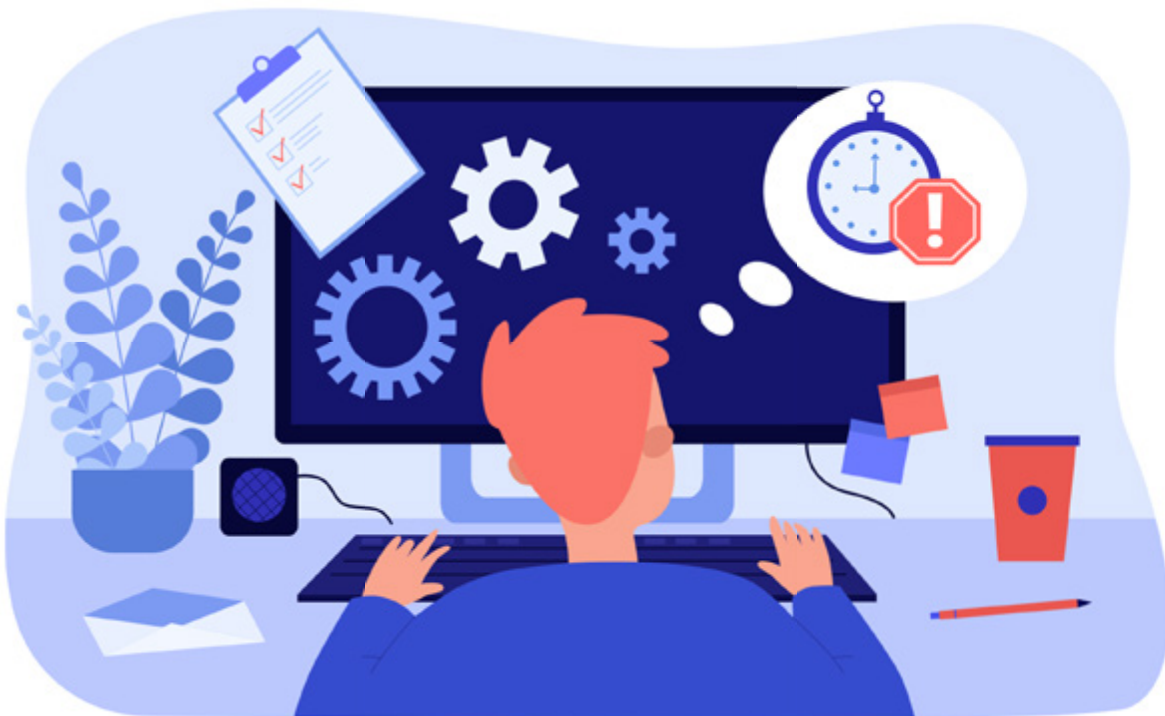
They also need to understand the legal and regulatory requirements that directly or indirectly have an impact now and in the future. Further, knowledge of what to protect and secure must be understood and turned into development requirements. Additional structures and processes may need to be developed to achieve suitable protection and cybersecurity.

2.2 Weaknesses and vulnerabilities

Assets may have inherent weaknesses and vulnerabilities from the start. Alternately, these can arise later due to poorly developed updates or upgrades or the discovery of a combinations of issues. New AI-based tools can and should be used to find these vulnerabilities. The weaknesses and vulnerabilities may reside in the hardware, or its potential firmware, operating system, platforms, and the code or applications that are run on top of these. Further, various processes used to manage and maintain IoT products may cause weaknesses or vulnerabilities through inadequate remote access solutions, e.g., low- and high-level VPN (virtual private network, an encrypted tunnel from one point to another). Or updates or on-site maintenance may introduce non-controlled software and equipment that enable causing a virus or malware to enter.

It is generally easier, to fix security weaknesses and vulnerabilities in software than in hardware. In domestic contexts, however, it is common to have poor or almost no protection of equipment connected to the Internet as well as poor segregation of networks (i.e., separation and segmentation) used for building automation, child monitoring, work, alarms, etc. A segregation of the network(s) makes it harder for viruses and malware to gain access and may also, enhance the bandwidth needed for high loads on the network in addition to the improved security. IoT products designed for domestic contexts are often able to update themselves, in terms of firmware and software, if this is configured at the installation. Otherwise, firmware and software need to be manually upgraded on a regular basis. Further, it is common that IoT products for domestic use provide poorly designed cybersecurity in hardware, firmware, platforms, or the software run on top of these. An area where improvements have been made, but is still inadequate, is to enforce the change of standard configurations and passwords during installation

and commissioning. Unless these are changed, it is a rather straightforward process to take over the IoT product and use it for unwanted activities if it can be accessed by unauthorized persons. Such activities may include: creating disorder; extortion by encrypting the data, information and systems; causing systems and IoT products to be inaccessible; using IoT products as part of bot-nets for DDOS attacks that target Internet-based services such as banks or payment systems (SWISH and BankID, in Sweden) or web sites for booking train tickets. If there are unprotected IoT products for domestic use that comprise microphones, speakers, or cameras, it is advisable to ensure these do not contain weaknesses or vulnerabilities and that these cannot be used to collect data/information about the residents and their movements. Recent and newly initiated EU legislation/regulations require that IoT products should be well designed and secure from the time of installation (i.e., secure-by-design and secure-by-default) and be secure all over (i.e., defense-in-depth).



MANY ASSETS IN THE HOME NEED PROTECTION. PHOTO: ADOBE STOCK.

IoT products for domestic use share many commonalities with those targeting professional environments or critical infrastructures. In the latter, it is more important not to expose weaknesses or vulnerabilities through poorly designed functionality and inadequate cybersecurity. The level of cybersecurity also applies to the required networks, external connections and the processes related to installation, configuration, commissioning and aftermarket support, service and maintenance until decommissioning and deinstall. In professional environments and critical infrastructures, it is essential to ensure that information about the networks and network equipment in which IoT products are used, is not leaked through poor design or cybersecurity and used as part of cyberattacks.

NOTE! To learn more about weaknesses, vulnerabilities and what is actually exposed externally (i.e., the Internet), users can turn to the TOR web browser in combination with the search tool Shodan (this should not be made from a computer in a secure network). There it is easy to view, in different geographic areas, equipment that is obviously exposed and potentially unsecured, making it possible to connect to. This search will list a considerable number of web cameras, sensors, and building automation systems, etc. Many cheap, efficient tools are available for various types of hackers on the Internet and on Darknet. More on this further below.

A general weakness for many IoT products is that the user manual (or other documentation provided) outlining how to install, configure and commission, does not comprise anything about how the cybersecurity around the IoT product should be set up. Nor do they demonstrate how to install, configure or commission the IoT product in a cybersecure manner. Further, often missing is how to maintain an IoT product's cybersecurity during its entire lifecycle. Thus, it is advisable either to integrate this into the user manual or add an appendix to such a manual. A rule of thumb is that the lower the inherent level of cybersecurity, the higher the protection level around it is required.

2.3 Use of AI/ML tools, AI agents and agentic AI in organizations using data from IoT products

To optimize and improve organizations and their processes, AI/ML-based tools are increasingly used together with AI agents and agentic AI, using data from the organization and its IoT products. For all this to work well in a secure manner, it is advised to classify data, make ontologies and data/information models, set up adequate protection and access rights, devise an AI policy. It is also important to update organizational strategy, and continuously review/maintain protection and access to prevent attacks and minimize the effects of such. The concept of an AI policy, combined with a related strategy update is new to many organizations and may require some thought and effort.

2.4 Common threats

Commonly, different threats are categorized as less malicious, e.g., hobby hackers and malicious actors such as professional hackers and those supported by national states, whose purpose is to make money, steal information and IPR, or to disrupt or destroy operations. Unfortunately, the latter two categories have significantly increased their malicious activities at the same time as the level of sophistication has increased substantially during the past five years, with an increase projected in the coming years. New AI-based threats add to this. Cyberattacks or attempts to intrude are launched around the clock and are largely automated by malicious actors looking for access points and what can be stolen or damaged. Subsequently, these actors make a (business) plan and, depending on their purpose or intent, they craft a schedule for what to attack or infiltrate to collect information over time. Professional hackers and those supported by states are highly skilled and knowledgeable, in many cases well ahead of many IoT product suppliers and suppliers of firmware and operating systems etc.

Another threat, mainly posed by professional hackers or state-sponsored actors, is to hack into an IoT product's development environment or distribution chain to plant hostile code or a hardware component that later provides a way in (i.e., backdoor) as the code is distributed to the target environments. This is often denoted as a "supply-chain attack". Another way to plant hostile code is through open-source code (there are various frameworks) that have not been adequately reviewed before addition to the code base. Lead developers should be appointed who review the open-source code and its continuous updates, and who approve these before addition and use. The provenance of open-source code should also be reviewed. No open-source code of unclear origin should be used. Later, it is difficult for developers using such open-source code to detect hidden backdoors or code that send out selected data about the users, processes, and environment/networks. If open-source codes, or code packages procured from vendors, are signed and appear safe, it can be demanding to review all (and do so continuously) even with the help of review tools. It is difficult for installers and users of IoT products to detect faults, in particular if the update or upgrade packages distributed are signed and appear safe in testing before being installed.

Sometimes hostile code can be time-activated and dormant, simply opens up a window to the outside that enables hostile actors to decide what, how and when to attack. The use of open design for hardware presents the same type of problem. Open designs need to be reviewed, and any assembled components or circuits should be carefully reviewed and tested before use.

An additional threat is staff (or inhouse consultants) and those involved in the value chain of an IoT product until it is decommissioned and deinstalled. Most often, mistakes or low levels of competence are what open up weaknesses or vulnerabilities and allow these to remain in the IoT product environment. In rare cases, disgruntled staff may consciously disrupt processes, commit sabotage, or steal data, information or IPR, and sell it to hostile actors. Whereas malicious inhouse attacks occur, mistakes by staff (or inhouse consultants) are more frequent.

In addition, these multiple threats must be thoroughly considered and outlined in a risk analysis.

The threshold for threats is low, and it is relatively cheap to rent hackers or buy time slots in cloud services or bot nets designed for hacking or disrupting organizations and their processes.



Hacker tools cost from a few dollars to thousands of dollars, depending on what can be accomplished with the tool. Such tools can be purchased on the Internet, Darknet or from firms specialized in providing them to actors like the police, intelligence services and others who can pay. Thus, the relation between the cost of a cyberattack and the impact it might have means that low-cost tools can cause major costs, damage or destruction. Further, owners of IoT products and owners of organizations where IoT products are used need to ensure their IoT products are not part of botnets or other hostile campaigns.

Some IoT products are connected in different networks but do not communicate outbound, some communicate outbound, and others are installed in isolated islands, disconnected from the network where they are used. Those residing in isolated islands may sometimes have a mobile connection outward to be able to transmit data, receive updates or upgrades, or access remote support or maintenance. In such cases, it is recommended that users consider whether they should have a process for opening up remote access rather than keeping it open continuously. It is common to put “problematic” equipment in islands if it is old, outdated, and has too low a level of cybersecurity to be allowed in the organization’s network. If the only need is to transmit data in one direction (e.g., outbound), data diodes may be used. However, these are fairly expensive and may not always be a viable option. One vulnerability that can be used by various actors is the support, service and maintenance of IoT products, where it is possible to find ways to plant hostile code, malware or viruses. Thus, processes for support, service and maintenance must be reviewed to ensure that these do not open up weaknesses. Moreover, organizations should always ensure that new updates, upgrades, components or spare parts are verified “clean” before being installed. Verification may be needed for downloaded software packages, external laptops, USB sticks or disks. Thus, the supplier of the IoT product and other involved parties need to provide cybersecure support, service and maintenance processes.

2.5 Risk analysis and risk mitigation

Risk analysis, which involves estimating and calculating the probability of, and potential impact of how an asset’s weaknesses and vulnerabilities can be used in the scope of a threat. Thus, a risk analysis needs to involve several actors in a value chain. Initially, it is likely that the IoT product supplier’s development organization will be most involved in risk analysis efforts and attempt to foresee how the rest of the value chain may affect the IoT product. Hopefully, this will lead to a number of functional and cybersecurity requirements as well as test cases for the product manager to consider. After some time in use at customers, the value chain of an IoT product will start to learn what works, what does not work, and what can be improved. Consequently, suitable actors in the value chain participating in installation, support, service and maintenance should become involved as should any part stakeholders of interest at the customer end (where the IoT product is used). At business customers, object owners, maintenance managers and OT security responsible staff collect feedback, experiences and potential improvements, which a product manager can transform into requirements for the further development of the IoT product. For business and domestic customers, user groups or similar may be a source of recommendations for new requirements. Listening to customers is also a way to avoid discontented users or stakeholders, who may make their discontent public nothing happens in terms of development and improvements. New AI-based tools to detect vulnerabilities should be used defensively to quickly fix any open vulnerabilities before an attacker uses them. Further, some suppliers pay those who find weaknesses/vulnerabilities to prevent them from ending up in hacker groups on the Internet or Darknet.

Figure 4 shows how data and information from different organizations can be seen in risk levels and the approximate impact the exposure of these can render in a wider perspective. The potential impact of the risks related to availability or integrity, for instance, is not included in of Figure 4.

Simple as well as complex methods are available for risk analysis. It is probably better to start by using a simple method and to increase sophistication as required. Examples of such methods can be found in books and standards/guidelines addressing risk assessment/analysis/mitigation: ISO-27005 and 31000, NIST risk management framework and CIS risk assessment method. Please note that whatever method is used, all related parties should be involved who need to, and can, contribute. A common failing is to involve too few of these, which may result in the overall risk assessment being inaccurate. Further, risk analyses are to be executed continually (at the start of all development projects at IoT product suppliers and at least annually at the customer site) and more often if the surrounding environment, i.e., the risk profile, rapidly worsens. It is necessary to scan an IoT product for vulnerabilities (and preferably its surrounding environment too) regularly and, if possible, automatically.

2.6 Principles for cyber-secure design of IoT products

Supporting principles, general and specific, exist for many aspects of the design and development of IoT products. Design-for-x or x-by-design thinking has been around for a long time, particularly related to engineering product development. These principles have been enhanced as demanding business models have transformed engineering products to become part of the Internet of Things, or extensive cyber-physical systems, or even more comprehensive systems (e.g., systems-of-systems). Examples of such business models are: products with loosely connected services, products with integrated services, PSS (Product-Service Systems) and functions or functional products. These should all be of interest to suppliers of IoT products.

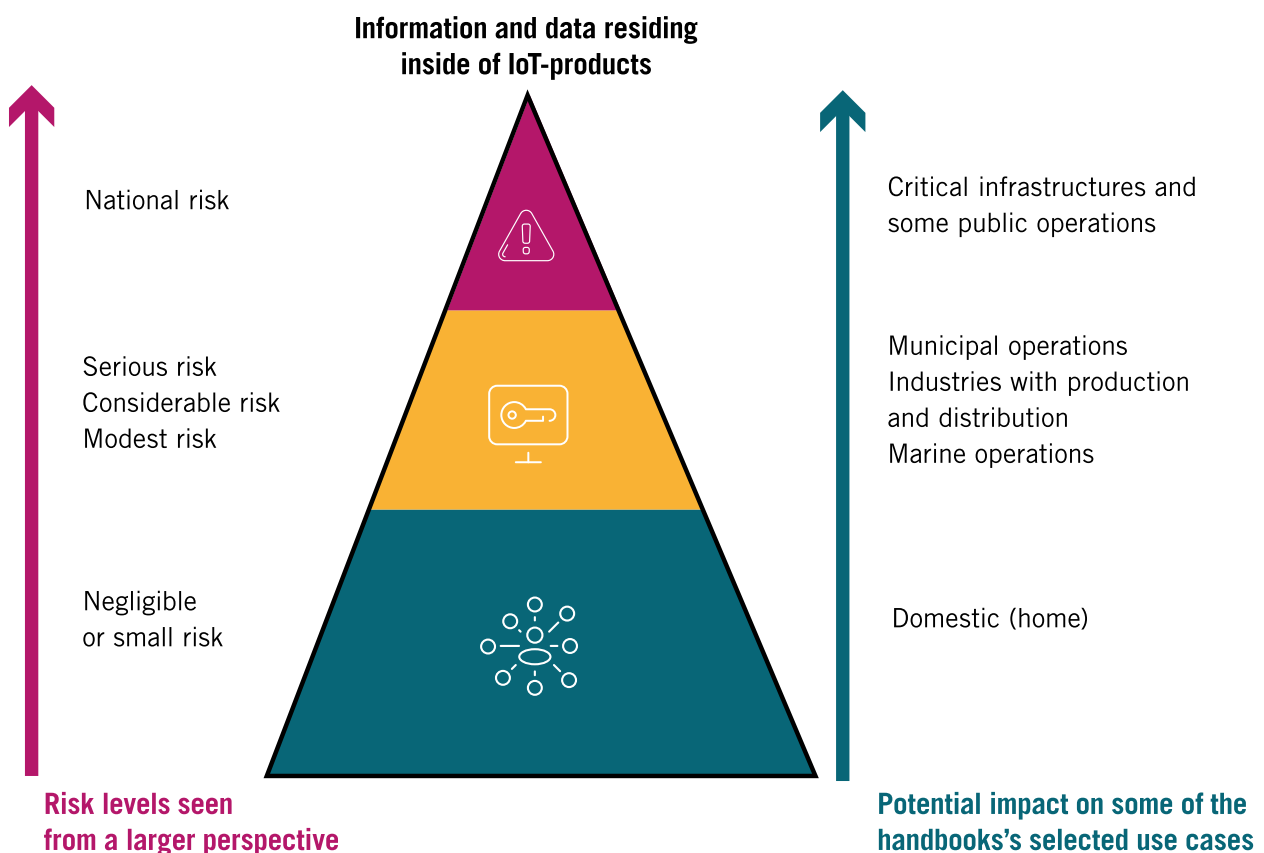


FIGURE 4 – INFORMATION AND DATA IN IOT PRODUCTS. RISK LEVELS FOR DIFFERENT USE CASES (SEE CHAPTER 9) FROM A WIDER PERSPECTIVE.

Pertaining to cybersecurity, EU and ENISA have launched the principles of security-by-design, privacy-by-design, secure-by-default, and defense-in-depth. The foundation for these is that cybersecurity requirements shall be part of the initial set of requirements, as otherwise add-on cybersecurity will become more expensive and likely not as effective. Further, personal information (processed, stored and/or communicated) shall be protected from beginning to end of the personal information's lifecycle in that system. This concerns mainly general software and systems, but also IoT products. Additional design principles are of interest, such as Stallings and Brown⁶ who propose minimizing the attack surfaces of networks, software, people and via physical access. Stallings and Brown outline 13 principles including: least level of rights/authorization; separation of rights/authorization (i.e., that a single user can only do certain tasks alone whereas some tasks require two users to be involved); least number of common mechanisms; isolation; encapsulation; modularization; use layers/levels; and open design.

The zero-trust model, which is frequently used, also needs to be considered as it requires that each part of a system has its own adequate level of cybersecurity and is not dependent on

any other parties' level of cybersecurity. Hence, the slogan "never trust, always verify" i.e., never trust anyone before successful verification. An IoT product can, or should if needed, be divided into different trust zones depending on which parts or components the IoT product comprises. Indeed, to be able to create separation and maintain a high level of availability and protect data/information, such separation zones may be necessary. Chapter 3 will further address this aspect. If the requirement engineering while developing IoT products uses the contents from Chapters 2 and 3, both of the above design principles will be considered. Chapter 3 details a number of standards, most of which address at least security-by-design⁷.

Another, but not new, principle or paradigm is the micro-services paradigm, which is being used frequently as many suppliers of IoT products and larger systems have realized that keeping all software code in one or a few blobs is not efficient as it increases costs and time consumption related to maintenance and testing unnecessarily (as all code needs to be tested even when minor are made changes).



RISK ANALYSIS SHOULD BE CONDUCTED REGULARLY DUE TO CHANGES
IN THE SURROUNDING ENVIRONMENT.
PHOTO: ADOBE STOCK.

⁶ Stallings, W. and Brown, L., Computer Security: Principles and Practice, 4th edition, Pearson, USA, 2018

⁷ <https://www.enisa.europa.eu/news/enisa-news/how-to-implement-security-by-design-for-iot>

To mitigate this problem, “containers” or similar are used for small, independent micro-services (which should be easy to replace and have well-defined service descriptions) that collaborate with other such micro-services using well-defined protocols and interfaces. Strategic thinkers have added common base functionality for cybersecurity, administration and fleet management in an underlying platform that all micro-services use. The idea is here that if one changes one micro-service, it is only that one that needs to be thoroughly tested as well as that it works as it should with the others via the defined protocols and interfaces. Thus, there is no need to test all code, i.e., all micro-services, if one or a few of them are changed. However, changes to the underlying platform need to be tested as well as a number of selected micro-services depending on what the changes are related to.

Therefore, to continue developing IoT products where the software code is in one or a few blobs is neither an efficient nor profitable way forward. The risk is that not doing this will impair innovation speed and tie up resources with no resulting benefits.

With many such underlying platforms for IoT and automation available, the difficult task is to select the most suitable, for now and in the future. If the code is developed properly, the underlying platform can be changed. And a common underlying platform in a development organization can render excellent scaling effects such as knowledge, and automated test suites can be re-used for new projects and IoT products. Further on, AI agents and agentic AI are expected to be used extensively in IoT products architectures. Therefore, this must be well thought through and in a secure manner.

For hardware, similar methods can be used, such as when it is possible and suitable to break down larger parts into exchangeable modules and components that have well defined interfaces and standardized functionality (i.e., compatibility).



3. Before starting up a new project

This handbook aims to cover the entire lifecycle of an IoT product. This affects requirement analysis, potential infrastructure and processes, and the structures related to an IoT product. Several aspects need to be considered before starting a new project and from the start of the lifecycle. Unless these aspects are properly considered, initial development/project costs might appear reasonable, but the entire lifecycle cost and profitability might be excessive. This risk often occurs when the initial design and conceptualization do not consider later cost drivers and potential obstacles.

In brief, the following will be addressed in this chapter:

- Early stage with business development, ideas, and concept development
- Requirement analysis – collection and analysis of functional and holistic requirements, laws/regulations, industry standards and voluntary standards, best practices, design principles (see section 2.3) etc.
- Management responsibility – to provide the conditions required
- Development environment and development process
- Documentation
- Testing
- Maintainability over time
- Quality level
- Industrialization
- Development
- Post development – maintenance/service/updates and support as well as optimization and training packages. Commonly, this is the longest phase in a lifecycle
- Monitoring IoT products during their lifecycle. Usually, this phase is also long
- End of a lifecycle

3.1 Early stage – business development, ideas, and concept development

At the early stage, sensitive planning and decision-making related to IoT product's business needs to be protected and confidential. This does not directly impact an IoT product's final level of cybersecurity. Thus, what need be protected are: information and sketches/drawings as well as notes related to business development, ideas that hatch into concepts, selection of concepts and concept development, potential prototypes or demonstrators, concept evaluations, etc. This should be kept in as a small group as possible to maintain confidentiality before proceeding to the next stage.

Therefore, an organization's IT environment and development environment need cybersecurity to be able to protect data and information related to:

- Early business development and later stage business development with business modelling considerations
- Idea generation, concept generation and selection of concepts for future development
- Concept development – protection of ideas, sketches, drawings, and as business modeling/planning
- Prototypes and/or demonstrators
- Protect early requirement analysis results, which may be generated from prototypes or demonstrations as well as the experiences arising from these

Further, all involved need to avoid talking about or discussing the early stage's contents or results. They should act responsibly and handle such information with extreme caution during visits to customers, in the car from work to home when stopping to go shopping, while traveling for work, or commuting to and from work on public transport.

Thus, all this may require such information to be encrypted and protected by additional means in the organization's environments and when it is off-premise on laptops, mobile phones, and USB disks or are e-mailed. When using AI/ML tools internally, ensure to keep any sensitive data internal and protected, and avoid sharing such data in public AI/ML services.

3.2 Requirement analysis – collect and analyze functional and holistic requirements from stakeholders, legislation and regulations, industry standards, etc.

A number of general, governing requirements for cybersecurity, i.e., the CIA+TP, are further described below that may impact the entire IoT product's design and adaptation to various circumstances during its lifecycle. Specifically, the developer of an IoT product needs to understand the contexts, processes and data/information that will be present during its use. It is advisable to ask customer users about the level of availability (e.g., availability classification) required and what data/information should reside in the IoT product. Examples of data/information security categories are: open, internal, confidential, strictly confidential, and whether personal data or data about critical infrastructures/state security will be part of the scope.

CIA + TP:

- **C (Confidentiality)** – what needs to be protected/kept confidential and how?
- **I (Integrity)** – how to prevent unauthorized changes in the IoT product or the data/information residing in it?
- **A (Availability)** – what are the requirements for availability, robustness and resilience (i.e., be able to operate in case of serious issues)?
- **T (Trustworthiness)** – what is required to uphold trust related to the IoT product, from customers, the surroundings, and the own organization?
- **P (Provenance)** – traceability (i.e., provenance) of the data/information that resides in the IoT product and is later transferred to other systems for storage and analysis? The IoT product's configurations and settings may be affected here as well. Changes made to the IoT product's hardware and software need to be traceable in the development environments e.g., by using “tags” in software code and version numbering or similar arrangements.

In IT environments, the order of importance for the starting triad is commonly CIA, whereas in OT environments and critical infrastructures the order of importance is often AIC, with the TP attached at the end. Thus, it is important to know whether the IoT product will be used in IT or OT environments, or in critical infrastructures.

With respect to the data/information generated in or around an IoT product, and that may be of value to analytics, or add-on services and extra functionality pertaining to maintenance/monitoring/optimization, it is advisable to first analyze business-related, legal and contractual matters such as:

- Who will own the data that will reside in the product?
- Where will this data be stored? Are there any legal or other aspects to consider?
- What may the data be used for?
- Who may use which data and when?

Depending on the outcome of these questions, it is advisable to separate different types of data to ensure that the above questions can be answered clearly and to prepare for future business development (which may take off as everyone understands the possibilities of using data for different purposes).



CYBERSÄKERHETSTÄNKANDET BÖRJAR REDAN NÄR MAN BÖRJAR PLANERA EN NY PRODUKT OCH ÄR INGET MAN LÖSER ENBART I SLUTANVÄNDARFASEN.
FOTO: ADOBE STOCK.

Please remember that the EU Data Act requires that data be made accessible to customers. An example of such a separation is:

- Data related to persons (because of GDPR in the EU). If this data is kept separate, it is easier to develop the functionality needed to follow up compliance with various laws and regulations.
- Process and quality data which concerns the activities or processes where IoT products are used. These data can be used to optimize functions and quality levels in processes (by measuring processes input and output – broken down to sub-processes and/or whole processes).
- Maintenance-related data, which pertains to wear and tear, and the need to maintain IoT products and their environment, and is collected via sensors, cameras, counters, etc. This is commonly provided by IoT product suppliers as add-on services in addition to collecting

data about fleets to detect general problems or weaknesses that need to be designed out or corrected through improved maintenance processes, etc. Additional related functionality may include enabling reduced load (graceful degradation) or emergency shutdown capability to prevent a complete breakdown.

3.2.1 Industry standards and standards that can be useful and provide guidance on cybersecurity requirements

Legislation and regulations may entail obligatory requirements, whereas other requirements may be voluntary or imposed by the industry an organization operates in. All of these may be basis for general, physical security, and cybersecurity requirements. Some physical security requirements may be related, or linked to, cybersecurity requirements.

An IoT product may need an outer physical security protection/perimeter. Or it may be locked inside a cabinet/room to prevent physical tampering by those without authorized access and authorization level. Further, a number of best practices can efficiently benefit from the past experiences of others to avoid unnecessary effort and costs. Such best practices may be a source of cybersecurity requirements pertaining to an IoT product. Below is a summary with high-level guidance on these. However, all product development groups need to do their homework and find out what is required by, and applicable to, their IoT product in the contexts and industries of interest.

- **Product rules/regulations and laws** – CE-marking including RED and other type approvals as well as extended warranty. In addition, there will be requirements for ecologic design including digital product passports in EU. Requirements often differ in EU, USA, Australia and Asia.
- **Laws on safety/security/cybersecurity**
 - GDPR (and Schrems II) or similar legislation/ regulations in other parts of the world
 - EU Cyber Resilience Act (cybersecurity requirements for products throughout the entire lifecycle)
 - EU Cybersecurity Act (framework for cybersecurity certification)
 - EU AI and Data Acts (responsible use of AI and making data accessible for customers)
 - Patient data legislation
 - National safety/security protection legislation
 - The EU NIS2 directive, which concerns critical digital services related to (an extended) society. If necessary, to be complemented by EU CER or DORA depending on context type
 - EU Machinery Regulation
- UN Resolution MSC.428(98) concerning marine/shipping sector, which can be more easily read in the IACS UR E22/26/27
- Swedish legislation 2018:1174 concerning information security for digital services critical to society
- **Industry standards** – examples include:
 - ETSI TS 103 645/TS 103 701 (IoT security for consumers)
 - ISO/IEC 27018 (protection of personal data in cloud services)
 - Healthcare - IEC 81001-5-1, MDCG 2019-16 (medical technology devices)
 - PCI-DSS (protection of credit/payment card data)
 - SSF 1120-1 (IoT – connected devices – requirements and testing)
 - SSF 3523 (digital locks – classification, requirements and testing)
 - IEC 62443 3-3/4-1/4-2 (pertains to automation/ control systems in various industries). Likely to be harmonized with the requirements of the EU CRA and currently a missing normative standard for the EU
 - ISO 21434 (cybersecurity in vehicles)
 - ISO/IEC 30141:2018 (reference architecture for IoT)
 - ISO/IEC 27400 (IoT security and integrity)
 - NIST Cybersecurity for IoT
 - IMO's MSC-FAL.1/Circ.3 guidelines for cybersecurity in marine/naval environments (concerns class action related to vessels, crafts and platforms). DNV-RU-SHIP Pt.6 Ch.5 and Lloyd's Register Cyber Safe for marine (both these are based on IMO guidelines and on IEC 62443 3-3/4-1/4-2). See also IACS E22/26/27
 - Swedish Civil Defence and Resilience Agency's recommendations for industrial control systems and IoT as well as cyber-physical systems (critical infrastructure).

The Swedish Food Agency's recommendations, based on those from the Swedish Civil Defence and Resilience Agency, are used in regulatory audits/reviews of production and distribution of clean water, for example

- ENISA's recommendation on IoT/ cloud/ critical infrastructures and development and use of these (industry and critical infrastructures)
- Swedish Association of Local Authorities and Regions/RISE: KLASSA for IoT
- Swedish Association of Local Authorities and Regions: Informationsäkerhet inom fastighetsområdet & IoT
- Swedish Association of Local Authorities and Regions: Informationssäkerhet i fastighetsorganisationen
- Swedish Association of Local Authorities and Regions: Vägledning för IoT-tjänster (Eng: Guidelines for IoT services)
- ioXt Alliance (certification program for secure IoT products)
- SSNF: Robust och säker IoT (stadsnät) (Eng: Robust and secure IoT city network)
- Traficon (Finnish transport and communications networks)
- **Best practices and more** – examples include:
 - GOV.UK (Consumer IoT Security)
 - IoT Security Foundation – search their global web site under “Publications”
 - OWASP IoT Verification Standard (advice for development of cybersecure software and the most commonly used weaknesses/ flaws used by hackers)
 - Cloud Security Alliance (cloud and IoT) – search their global web site under “Research”
 - IBM (cloud and IoT) – search their global web site for best practices and advice
 - Microsoft (cloud and IoT) – search their global web site for top-10 lists and best practices

- Google (cloud and IoT) – search their global web site for best practices
- IoT Security Institute (regarding smart cities and critical infrastructures)

3.2.2 Practical functional and environmental requirements related to cybersecurity

If functional- and environmental requirements are not related to other matters, and can be considered stand alone, they are easier to manage. However, such requirements are related to other matter like cybersecurity or physical security/safety. To manage the latter, design principles and modularization can be used as can standardized components/parts, micro-services, AI agents and agentic AI, as the requirements are broken down into smaller parts.

Functional requirements concern what the IoT product is designed to do. They should be practical and well designed to facilitate efficient management throughout the lifecycle and to optimize lifecycle costs as much as possible. Developing functional requirements into functionality at a later stage is complicated and expensive. Poor service and maintenance functions will discourage customers and their users from adding functions or replacing IoT products whose lifecycles end. This is an important aspect for suppliers of IoT products to consider. For example, look at recent car models that make it difficult to change a headlamp bulb without expert help.

Practical functional and environmental requirements include:

Operational environment – the operational environment for IoT product impacts on the design in terms of external protection and cybersecurity. A rugged industrial environment places its demands as do the requirements for an IoT product that resides in a more or less unmonitored and unprotected environment outdoors, indoors

or in domestic environments. Thus, physical attacks and cyberattacks may lead to unavailability or destruction in exposed environments. Physical access may also lead to cyberattacks by connecting through unsecured/unprotected interfaces or simply by removing a hatch to access electric contact points or memory cards in the interior of the IoT product.

Hardware requirements – Even in what appears to be a secure environment, the IoT product needs to be protected from physical access and destruction and not be easily opened. The least requirement is to attach a seal or sticker on any openable hatch above memory cards and/or electric contact points. An alternative is to recommend that the IoT products be installed in a fully controlled environment with physical locks (i.e., in a locked room or cage/cabinet).

A simple plastic cover, which can easily be bypassed, may result in a break-in that is not detected soon enough. To prevent this, a built-in function could send an alarm and perhaps even deactivate the IoT product in the case of a physical attack or destruction attempt (in particular, if the IoT product can be used to launch a wider cyberattack on a network).

IoT products that are vulnerable and unprotected should reside in a network that is not connected to the main network. Examples of such are connected car heating poles at parking lots, external alarm systems, external lock systems without monitoring, etc.

Related to the environment – the ability to exchange/replace old hardware components or refurbish them for continued use (i.e., refurbishing or re-manufacturing) should be considered for the IoT product's lifecycle. When the primary lifecycle for an IoT product reaches its end of life, it is often possible to find a new lifecycle in other contexts, where requirements may be lower, and scrapping or destruction can be avoided (i.e., repurposing or downcycling). However, the IoT product needs to be wiped clean of all data, information or configurations, etc., before it continues a new lifecycle elsewhere.

Information flows – As it is likely that data and information will flow through the IoT product during its lifecycle, it is necessary to consider where flows should be stored or buffered on their way to processing. Such flows need to be cybersecure.

There is an example above of how to segregate data and information in an IoT product related to personal data, process- and quality-related data, as well as maintenance and fleet management-related data, to facilitate transparency pertaining to: data ownership, and how and when it can be used.

If cloud services or the suppliers' own central servers are used to store data and information, it becomes a somewhat more complicated than if it is stored at the customer site in a data warehouse or local server. This needs to be carefully considered as many interesting business development projects remain to be explored based on data and information. If there are strict requirements for one-way communications, data diodes or similar can be used to control data flows.

Interoperability and compatibility – how should the IoT product fit into different object owners' target environments and what demands will this make on the design? Design can be affected by: how data/information can be exfiltrated through networks and firewalls; how data/information should be stored/shared in a cybersecure manner; what data formats and communications protocols are needed; should it be possible to export data and information to different formats; how easy should backup and restore (import) be; how should authorized persons be able to connect from the outside and which functionality do they need, etc.

Knowledge in the operations environment – if the IoT product is simple, the knowledge required to operate it should be acquired via training. If the IoT product and its function is complex, the supplier or some other actor in the value chain may need to provide extra training. Depending on the context, support and service can be provided remotely through a cybersecure connection or onsite.

Further, training and education packages can be provided. In addition, external actors can participate through a cybersecure video link, and virtual/augmented reality (VR/ AR) can be used for training and trials before operational go-live.

Cybersecurity in the distribution chain – how should an IoT product and its components or parts simply and effectively be distributed to customers initially and then later during the lifecycle without compromising the IoT product's physical or logical contents? Consider this and ensure that the IoT product and spares or components are intact at arrival at the customers and users.

Efficient installation, configuration, and commissioning – if this is considered properly, time and travel can be saved. Such a process, which commonly has several steps, needs to be cybersecure. Consider if it is possible to automate parts or entire steps by using fleet management functions with plug-and-play, autoconfiguration of local settings, and network connections, through preinstalled central settings combined with automatic or manual commissioning. Much can be achieved here, cutting costs for customers and users with multiple IoT products, by using a high degree of automated process steps, and the IoT product becomes very attractive. Some of the advantages of using central management, or fleet management, include fewer errors and the ability to easily change IoT products swiftly if or when needed.

Cybersecurity during operation and maintenance – an IoT product needs to be designed to be operated and maintained in a cybersecure manner until the end of its lifecycle. Usually, data and information about the process, quality outcomes and maintenance needed to be optimized, but the IoT product also needs to be designed so that this can be executed effectively either onsite or remotely (i.e., what can be done or prepared remotely) combined with what can be automated.

Cybersecurity at the end of the lifecycle – at some point, an IoT product and its parts/components need to be decommissioned, destroyed and recycled without compromising any IPR, data and information (settings, recipes/programming, operational data such as IP addresses, etc.). For such situations, a fleet management function can be provided and used for decommissioning while securely removing any IPR, data and information. On completion, the status should be reported back to the fleet management system for logging and traceability. Further, if physical destruction is necessary, it needs to comply with the policies of customers and their users. However, as a supplier, it is advisable to include instructions for how to best do this, unless the producer is responsible for destruction and recycling. Where such responsibility exists, an internal supplier instruction should be available to ensure proper destruction and recycling.

3.2.3 General cybersecurity requirement for IoT products

Each IoT product and the contexts it is used imposes specific cybersecurity requirements. This needs to be discussed and analyzed, in terms of impact, together with customers and users. Moreover, an understanding of the surrounding world is required in terms of threat, wars and war conditions, legislation and regulations. To provide an insight into what can be categorized as general cybersecurity requirements, we look at the structure provided by IEC 62443 part 3-3 and security level 1 (of 4, where 4 is the highest). It is probable that level 1 will be slightly upgraded or that a new level will be added to match the requirements of the EU CRA. An industry may have enforceable requirements for components and systems that are critical and can impact the environment. Such an example is the maritime industry, with class action, which applies to newly contracted vessels and installations from 1 January 2024⁸. It is likely that other industries, also on shore, will start to do similar actions. However, some industries such as transports, air and space already have some cybersecurity requirements and regulations.

⁸ Check IACS UR E26/E27 - <https://iacs.org.uk/news/iacs-adopts-new-requirements-on-cyber-safety/>



SYSTEMADMINISTRATION UTFÖRS AV EN SPECIALIST.
BILD AV EN IT-TEKNIKER SOM GÖR INSPEKTIONER I ETT DATACENTER.
FOTO: ADOBE STOCK.

In IEC 62443 part 3-3 and its lowest security level 1, which in general applies to cybersecurity of systems, there are a number of groups comprising requirements according to below.

Please observe that this is only an example to outline what already exists, mainly for professional environments, and what is possible to certify towards if there is a need or requirement to do so. Regarding additionally critical environments, the security levels 2-4 can be applicable and of interest to review. In Sweden, different industries have various industry specific guidelines and sets of requirements (see for instance Swedish Civil Defence and Resilience Agency's and Swedish Association of Local Authorities and Regions' publications in chapter 10 and section 3.2.1) which may provide a foundation to start with.

Below, briefly outlined on a high level are what the security level 1 comprises. This is worth to check out and then to also consider what is relevant for the specific context:

- **Identification and authentication controls with:**

- Identification of users.
- Authentication levels and which level of authentication that different user groups or roles have (e.g., users with the right to view, user with the right to change, administrators). Further, administration from an unsecure or external network may require 2- or multifactor authentication.
- Identification and authentication of software processes and devices.
- User management.
- User groups/roles.
- Ability to change and manage authentication method.
- Management of wireless access.
- Requirements for being able to change strength/length of passwords and whether passwords should be visible or not at login.
- Ability to manage how non-successful login attempts are handled (how many are allowed, temporary lock,

only administrative accounts are locked and need to be enabled again, manage length of time-outs before new login attempts can be made or the number of attempts made during a certain period of time).

- Manage and change system messages.
- Allow or disallow access from untrusted/unsecure networks.

- **Management and control of use through:**

- Requirement for authorization (who has rights to do what) for human users according to the principles of division of responsibility and least privileges.
- Control/management of wireless use and access.
- Control/management of portable or mobile devices (in connection with the IoT product or its networks).
- Ability to limit the use of dangerous/malicious mobile code (such as Java script, Active X, PDFs, etc).
- Ability to lock sessions (e.g., time-based or user-controlled).
- Ability to terminate remote connections (time-based, inactivity, or by a local supervising user via a button).
- Ability to manually approve any remote connections and terminate such.
- Audit logging (time-stamped, what is relevant to log and needs to be logged according to requirements based on law, standards, or customer object owners).
- Ensure there is adequate storage left for audit logs (depends on amount and duration of logging).
- Ability to control who can access audit logs and ensure that these are protected (and cannot be altered by anyone).
- Required actions in case of audit logging failure – what to do and how to call attention and rectify it?
- Time stamping of each log entry.

- **System integrity including:**
 - Integrity of communications in unprotected networks (to notice if any communications are altered).
 - Protection against dangerous/malicious code (everywhere or at points with incoming or outgoing communications).
 - Ability to verify that the cybersecurity functionality works (i.e., to have a set of functions, procedures, scripts or similar that can be executed to show/verify that everything works).
 - Validation of input.
 - Failsafe functionality if normal operations are not possible due to a cyber-attack (and ability to return to a failsafe state).
 - Integrity protection of sessions (e.g., use of unique session IDs for each session).
- **Data confidentiality including:**
 - Protection of communications and storage confidentiality (through encryption).
 - Apply authorization for access/read.
 - Requirements for updated and adequate encryption algorithms, key lengths, certificates, processes for managing keys and certificates.
 - Ability to upgrade algorithms and keys with additions if/when tougher requirements are needed.
- **Limit data flows with:**
 - Segmented networks (logical/physical or both) where the IoT product is operated.
 - Zone protection to monitor and control communications at the perimeter of the segment (i.e., compartmentalization), with “deny-by-default and allow-by-exception”. Ability to manually stop communications between zones. Further, ability to operate in island mode.
- Ability to hinder peer-to-peer communications or similar solutions (i.e., only have approved communications in the solution and in/out of segments).
- Partitioned application/services/data (to achieve independence and protected zones).
- **Response times at events through:**
 - Audit logs that are readable (read only) for authorized users (humans or tools).
- **Ensure availability of resources with:**
 - Protection against DOS attacks or similar issues– the IoT product should operate in degraded mode during such attacks.
 - Resource management – the IoT product should reserve adequate system resources for security-related functions to prevent system resources being occupied (i.e., at maximum load) by the other functions.
 - Backup functionality – backups of critical data and audit logs made without affecting normal operations (and stored at a location that is available but not on-line, i.e., delinked).
 - Functionality for restore and recovery/restart – it should be possible to restore and recover/restart the IoT product in a known and safe state after disruption or error.
 - Ability to provide extra power source inlet (i.e., two or more different power sources plugged in) when availability demands are high. Switching from primary to secondary power source should not affect the IoT product’s cybersecurity.
 - Ability to configure and change settings or configurations of networks and security level – the IoT product should be configurable (via an interface) so that its network and security parameters are aligned with recommendations from the supplier (executed locally or centrally via a cloud service).

- The principle of least functionality – unnecessary functions/services, ports, protocols, etc., will be disabled, forbidden or removed from the IoT product.

If an IoT product has its own cloud service, or connects to one externally, AI/ML services, or a server at another location to store data, fleet management functionality, updates, report function, optimization functionality, etc., additional requirements will be in place to protect these. If these are available via Internet, it is possible to get an overview of potential cybersecurity requirements from Cloud Security Alliance, Microsoft, IBM, etc.

Further, it might be necessary to manage which software may be executed on the IoT product (i.e., device) via secure and trusted boot and “chain of trust” from hardware, via operating system to apps. In such cases, additional strengthening, such as secure boot, may be needed. This method is designed to ensure that a device only executes trusted software. The method verifies the integrity of software that is uploaded during the bootup phase. Commonly, secure boot is implemented as part of an IoT product’s bootup software and is based on using

cryptographic keys to verify the integrity/origin of software before uploading. Cryptographic keys should be securely stored in a hardware module (e.g., a trusted platform module (TPM)). As the IoT product starts up, the bootup software (i.e., boot firmware) checks the signature for the start manager (i.e., boot loader) using the stored keys. These keys may need to be rotated/updated at regular intervals. If the signature is valid, the start manager is allowed to execute. Subsequently, the start manager repeats this process for the operating system and all other software being loaded. Thus, a secure boot prevents that malicious code is started on an IoT product, as it verifies the software before loading and execution, and ensures that only trusted software can be executed. This helps protect against malicious software, boot kits and other types of threats that depend on being able to execute its code on a device (i.e., the IoT product).

Thus, many already exist to bring in and consider, and then use, that to determine what is relevant for the IoT product to be developed (or to improve existing products). It is not necessary to come with this alone, and considerable progress can be made by reading and considering everything that already exists in writing.



3.3 Management responsibility

– what matters need to be clarified and sorted out?

The management of organizations developing IoT products has a number of matters to attend to and take on responsibility for. It also has to ensure that the other actors or stakeholders in the value chain are onboard as well, including customers and their users. One matter to address is what makes the IoT product function well, short-term and long-term, with a suitable level of cybersecurity. It is hard for a development team to collaborate with many actors and stakeholders in a value chain around requirements that cross organizational borders. Thus, management needs to step up and address such matters to avoid expense and insecurity at a later stage.

Certain requirements, often referred to as holistic, affect all parties and cross over all borders. Certain infrastructure needs to be available or existing infrastructure needs to become interoperable or compatible. Finally, certain processes and set-ups of assets/equipment need to be standardized. Examples of such assets/equipment are: the IoT product, cloud service(s), certificate infrastructure with a root certificate and revocation lists, federation of identities (permit an authorized identity to log into multiple services as the organizations behind trust each other and add the user identity to their list of authorized users), and access, etc. Further, incident management and how related information and updates are to be sent to customers need to be considered.

Management should also start to think in terms of total lifecycle cost instead of initial development cost. This affects the requirement collection/analysis/engineering, decision-making and design, all of which might result in higher initial development costs but which would lead to improved profitability later in the lifecycle. Such long-term savings derive from the IoT product being well-planned from the beginning, with future development plans and architectural decisions factored in by management. The use of design principles in the requirement collection/analysis/ engineering stage may provide better future results, too.

3.4 Cybersecure development environment and process

Two questions to start with are:

- What IPR do we have that should/needs to be protected?
- Why should we make an effort and develop IoT products if others then just can take our: blueprints; documentation; descriptions of services, processes or structures; the code; or plant a virus or malicious code or designs that will destroy everything later?

If the above two questions are relevant, additional questions need to be raised about what the development environment comprises (i.e., development, test and documentation) and who has access to, and can work with, what: Who is authorized to access parts of the development environment (onsite or remotely)?:

- Who is authorized to access parts of the development environment (onsite or remotely)?
 - Who is authorized to access the development environment and which tools are they allowed to use there?
 - Does everyone need to access the software code, hardware designs or service designs, and in particular outside the organization's internal network and outside normal work hours (e.g., week-days between 08:00–19:00 o'clock)?
 - Do countries other than Sweden need to access the development environment (and is it possible to open up specific temporary access if such remote work is needed)?
 - Who is authorized to check code in and out of the main branch or make changes to drawings or blueprints etc.?
 - Is a code or design review required before any code, drawings/blueprints, service or process descriptions is checked into the main branch?
- Is specific protection required for development documentation and other materials such as product/service/process documentation,

IPR/drawings/blueprints, documentation of production process/method (if this needs to be confidential and is considered confidential or strictly confidential)?

- What cybersecurity requirements exist for collaboration tools, i.e., secure communications and document sharing. What level of protection level documents, authentication levels, etc. require?
- At some point, a decision needs to be made, or a development process/methodology selected, that resolves the issues. Here, it is important to consider cybersecurity from the start. It is advisable to use a development process that ensures that the initial set of requirements is adequate before starting development to avoid costly mistakes. The set of requirements will likely change during development, as in most projects, and will evolve through a structured change management process. Using the same development process/methodology to resolve all issues may not result in an optimal outcome. Knowledge and experience of using several such development processes/methodologies is beneficial due to the complexity of developing IoT products, which may comprise hardware, software, services, processes, cloud services, AI/ML, data/oral communications, and data analytics.
- What requirements should be imposed on the development process/methodology? It needs to be able to run a number of parallel sub-processes but still be able to coordinate them so that they progress timely and do not run ahead and close the design room for the other sub-process due to design choices made.
- Here, it is possible to anticipate parallel sub-processes for: hardware, software (local, central and/or cloud-based, AI/ML tools as well as AI agents and agentic AI), services and processes (ranging from service, support, maintenance to optimization functionality based on data), operational management (to build the structures and infrastructure

needed by the IoT product to operate in the long term and make incremental improvements in performance and availability).

It is an advantage if as much as possible of what is relevant is in the initial set of requirements and so avoid poorly designed (or impossible) additions later on.

- What requirements are imposed on the development/test environment and selection of test data in general?

It is always advisable to manage and control the physical security and cybersecurity of development environments. Developing a product, investing effort and money, and then learning that something very similar is being launched, is frustrating, especially when you know that you developed and funded it all.

Those who develop services, processes and other structures, may take advantage of the development environment where the hardware and software is developed. They can benefit from the existing model for setting up access rights, authorizations, authorization to make changes, version management backup, etc.

3.5 Requirements on documentation

– various user guides and manuals

It is necessary to include the cybersecurity of IoT products in the documentation. However, this is often not the case. Further, this is also necessary if the IoT product is to be certified. Even if not, it is always advisable for all target contexts, from domestic to critical infrastructures. Balanced documentation including cybersecurity may comprise:

- The IoT product's function outlined. Provide a comprehensive view of the entire "system" and how cybersecurity (plus any required physical security) should be set up schematically. Which roles will log in, to where, and what will they do?



GOOD CYBER SECURITY DOCUMENTATION PROVIDES BETTER SUPPORT IN THE INSTALLATION, CONFIGURATION AND UPDATES OF IOT PRODUCTS. PHOTO: ADOBE STOCK.

- Recommend that customers and their users cybersecure their operational environments – what might that look like? Is their own physical and logical network segment needed as relevant protection (e.g., firewall/gateway with buffering of data) or is it just a sub-component of another system?
- What happens if the IoT product is operated in a non-recommended environment – who is responsible?
- How to complete a cybersecure installation, configuration, and commissioning?
- How to transmit any data outward? Data diodes?
- Do the customers and users need to make firewall openings (i.e., which ports, protocols, etc. are needed for the operation) and what requirements for authentication and secure communications are imposed by the IoT product? All this needs to be explained in the documentation. If 2-factor authentication or other types of multi-factor authentication are required, e.g., for administrators, this may require that such solutions are installed, and acquired if none are available in-house.
- How to verify that an IoT product's cyber-security is correctly set up and configured? Is there a specific function, procedure, script, or other way to verify this? This is a common requirement for certification.
- Will support and maintenance be provided from remotely via the Internet or other networks? Is it possible to build maintenance and update functionality into the IoT product, which is initiated, for instance, as the IoT product connects to a cloud service to transmit data and retrieve configuration changes made centrally? Another option is to have an external VPN connection, which must be authorized and set up according to customer policies.
- Is local cybersecure support and maintenance needed on-site? If so, cybersecurity needs to be ensured so nothing is compromised by bringing in malware/viruses on software updates or via the use of an external laptop, mobile phone or USB sticks, etc.

For such purposes, a to cybersecure process is needed, ensuring that no malware or viruses get into the target environment. This should be complemented with training for the service engineers who carry out on-site service and maintenance.

Thus, the appropriate documentation, including cybersecurity, needs to be available to provide guidance during installation, configuration, commissioning, and updating, etc., throughout the lifecycle. A further benefit is that support technicians will receive fewer queries and can focus on more important tasks instead.

At the end of the lifecycle, or cease of use by a customer's object owner, instructions are required on how to delete and wipe IPR and data/information, and how return to factory settings or other void contents. Everyone involved appreciates an IoT product that offers this function, especially if it provides a final verification note that all data and information etc. has been deleted/wiped and/or replaced.

Further, recycling instructions for the IoT product are needed in case some parts may need to be destroyed or separated from each other. Please note that this all applies to all locations where IPR and data or information etc. are stored. This may include not only the IoT product itself, but also cloud services or servers, and any intermediary steps used to transmit data from the IoT product. Users at customer sites commonly follow IT and OT policies with rules and an information security lifecycle management scheme which stipulate how to decommission and end of life various assets in the IT and OT environments. In some cases, full physical destruction may be required of memory cards, disks or other parts to ensure that nothing of value in terms of IPR, data or information, is exfiltrated to competitors or other parties.



3.6 Test requirements

IoT product tests are important for the functionality and to ensure that the cybersecurity level is adequate. It should be possible to plan, depending on available competencies and knowledge, so that developers and testers cooperate and ensure that certain functionality is built into the development and test environments (which may require some time and effort).

Thus, various forms of automated test suites, and test rigs, etc., should be part of the initial requirement specification. Further, the test suites and rigs need to be continuously improved during the IoT product's lifecycle.

Finally, all functional and cybersecurity requirements must be testable.

Various types of tests need to be compiled to achieve a solid and stable IoT product. Below are a number of groups for test requirements, which may be considered while drafting a test specification and test plan, to optimize test coverage:

- Planning and overview of test coverage – will the IoT product consist of different configurations of hardware, software, and cloud services/servers or other additional services?
 - How large a test matrix is required to achieve adequate coverage?
 - Porting to various platforms – are the target platforms similar or different?
- Functional testing
- Testing and review/walk-through of additional services, processes, and structures
- Tests to ensure that all functionality (and services, processes, and structures) are cybersecure
- Performance and scalability
- Test of documentation – is the set of documentation complete and correct?
- Test automation – test suites for cybersecurity, functional requirements, and performance/scalability/overloads. Old and new AI-based tools for vulnerability scanning should be used

- Test rigs – what is needed to efficiently execute the tests? Can the test rigs have prepared configurations which can automatically be set?

Penetration tests – for this an external party might be advisable – regular penetration tests are needed to ensure that the IoT product's cybersecurity protection level is hard to penetrate and adequate for the targeted operational environments.

- Vulnerability scanning – exposed parts of the IoT product and potential cloud services etc. should be regularly scanned for vulnerabilities
- Regression tests after bug fixing and changes. If test suites and test rigs are automated, this will be faster and more efficient

Issues discovered by penetration tests and vulnerability scans should generate a requirement for the development team or be managed through maintenance or upgrades. Today, this has to go fast and be done regularly (also outside of development cycles). Well-planned test automation accelerates testing and makes numerous test iterations possible. This way, manual testing can focus on test cases that are hard to automate. The result is good test coverage and time for multiple tests during a development cycle. If an organization builds IoT products on a platform, a sub-group of the testers can focus on testing the basic functionalities of the platforms. This allows testers to focus on the IoT product and not the underlying platform. A number of publications focus on the development cybersecure interfaces and APIs, and large cloud service providers and OWASP, with its Top-10 lists, share relevant reading and publications on their web sites. These can provide relevant input for developers and testers to craft test cases and test suites by describing common cybersecurity problems, weaknesses and cyberattack patterns.

3.7 Maintainability over time

– planning for updates, upgrades and migrations

The longest phase of an IoT product's lifecycle is usually when it has been installed and commissioned at the customer site until it is deinstalled and recycled, or continues life in another context. A competitive edge can be gained from an IoT product that can be supported, serviced, maintained, and updated in an efficient, cybersecure manner, not only in terms of self-preservation but also to enable the entire value chain to be profitable and maintain reasonable costs related to the IoT product's total lifecycle. To do so, a training and education package may need to be developed for internal and external use. Further training and education for users at customers can be considered an add-on service. If the attrition rate of employees is high, the training and education package becomes even more important.

Maintaining an IoT product is seldom straightforward and may require carefully planned, efficient and cybersecure milestones for the target contexts. An IoT product may comprise hardware, software in various shapes/forms and levels, an underlying software platform, a cloud service/central server, and a variety of manual or automated services and processes executed as a mix onsite and remotely. All these create complexity and requirements for maintainability.

For an IoT product to operate and function well during its lifecycle, it will need either adequate hardware capacity from the start in terms of processors, memory and storage, so that it is possible subsequently to add and upgrade the firmware, operating system, platform, software packages used, open-source software that grows, and application code. New, augmented demands on cybersecurity, which arise at regular intervals, will likely require that the hardware needs to endure significantly more load than in the initial situation. An alternative is modular, exchangeable hardware, but this means there will need to be enough modules later as they are required.

Many manufacturers cease production a few years after the initial model is released, and move on with new products and modules. Thus, this must be planned for. Starting with a hardware configuration that barely meets current capacity requirements will likely cause more problems and cost than if hardware with better capacity had been selected from start.

An inspiration, in particular from mechanical/electronic product development, are concepts like “design for maintenance” together with a number of related “design for X” concepts, such as “design for manufacturing”. If planning and executing maintenance and updates, etc. are difficult and complex, the IoT product will likely be unnecessarily costly and less competitive. If maintenance and updates are swift and straightforward, stop times in the operational environments will be shorter (unless redundancy is available to provide continuous operation).

Often forgotten in early-stage IoT product development are the data and information that are generated and stored for a long time. What data formats are used, and how can data be extracted and moved to another supplier's cloud service/server or AI/ML services if the object owner at customer site (i.e., the contractual party) owns the data and information and wishes to move it elsewhere in the future? Charging a hefty fee will not render goodwill and positive reviews when customers and users meet at industry meetings, conferences, or trade fairs. An IoT product with efficient functions for migration from one data format to another, and that makes it possible to extract and exfiltrate data and information (using meta data) to another context, customer perceptions, and reviews will greatly improve.

3.8 Quality level and what affects the level?

The quality-level of an IoT product is affected by many factors related to customer and user expectations and cost. In this handbook, the IoT product's lifecycle is central. Therefore, quality needs to be at an appropriate level, above customer expectations, until the end of the lifecycle.

Thus, the quality on installation and commissioning matters little if it deteriorates due to poor maintainability and inefficient, or late maintenance and updating. Cybersecurity, which is closely related to maintenance and sometimes also to time-critical updates, is part of the perceived quality. Thus, if cyber-security is or becomes too low, the IoT product may be disqualified from use in a number of contexts.

Further, weak ownership by object owners or lack of a budget for maintenance on the part of customers affects quality, directly and rapidly, of an IoT product (if maintenance and updates etc. are required). Many IoT products, and other production assets, with a harsh lifecycle and little or no attention and care may quickly deteriorate and cause disruptions in product and distribution processes, or other types of operations. In addition, a neglected IoT product may retain weaknesses over a long time, which at worst can be used by various attackers to cause disruptions, data leakage, maliciously encrypt the IoT product's data and information, etc. New AI-based threats can have major consequences in such contexts.

Similar to object owners not caring enough for IoT products, weak ownership by the product manager at the supplier may also transition an IoT product from being a premium choice to being last in the procurement processes' lists of ratings and will only be selected if the price is the lowest (if at all).

3.9 Requirements from industrialization

It is not easy to industrialize, or prepare an IoT product for more or less large-scale manufacturing, and get the rest of the value chain (to add value for customers) going. Indeed, it is difficult to do everything completely right from start, so bit of trial and error is required to pave the way. During industrialization, the many stages and actors/stakeholders involved expose an IoT product.

Thus, physical security and cyber-security are a must. The availability of reliable technicians and production workers is difficult to guarantee as well. If many are involved, the difficulty increases. An important issue is to determine what can be done inhouse and what should the other actors in the value chain contribute to achieve efficiency without risking the IPR as the IoT product is about to enter the market and meet users. If too many have access to sensitive information or secrets, the IPR are not likely to remain confidential for long. A further issue is whether the value chain may be allowed to be outside Sweden and the EU as this impacts physical security and cybersecurity. If dependencies on suppliers exist that may delay manufacturing/production (i.e., supply-chain problems or transportation squeezes like during the COVID years).

The requirement analysis should comprise a design for manufacturing requirements to ensure that the IoT product is as easy as possible to manufacture, assemble, quality test (after manufacturing/assembly) by using a test rig and/or test suite. Just manually testing a few, such as 3 out of a 1000, is not a good strategy. It is better to automate the final testing and cover every item. Then it is certain that all IoT products that meet the customers and users are approved for use. If volumes are small or mainly handmade, test automation is not as important as for large volumes, if the manufacturing/production is rational and simple, there will be fewer faults a lower level of scrapping or time-consuming post-operations to rectify faults. Unnecessary complexity in the manufacturing/production and testing of IoT products costs money and effort. Therefore, try to simplify and, if possible, automate as much as possible to achieve the greatest benefits. This is especially crucial if competitors do it.

4. Supplier process for collating requirements, achieving an appropriate requirement specification and verifying requirements

To address requirement engineering by collating and analyzing requirements in an ad hoc manner increases the likelihood that important aspects and requirements will be missed. Thus, IoT product suppliers need to have a clear and structured process (and perhaps also in the rest of the value chain) which regularly provides feedback on how the IoT product is performing and fulfilling customer and user expectations. It is not easy to collect a complete set of requirements, as outlined in the previous chapter. Many aspects need to be considered. Moreover, priorities often need to be set if the initial requirements are more extensive than the capacity (and timeline) of the first development cycle. Therefore, a process for structured collation and analysis of requirements is necessary. Further, requirements that are not selected for a development cycle should remain in the process for the next cycle or minor upgrade/patch. To support a product manager and all involved in developing an IoT product, a roadmap can be used to visualize, on a timeline, a given period's development cycles and what major requirements/changes it will comprise. Such a roadmap should be dynamic and updated based on what happens in: technology development, the organizations vision for the IoT product, customer needs and expectations, and the surrounding world. The roadmap is a good tool for regularly communicating with important stakeholders in the value chain so that they know the main plan and what to expect. Further, a road map can facilitate budget allocation and procurement planning for customers' object owners.

4.1 Feedback and verification

Some industries have developed frameworks, processes or instructions (and may also be subject to specific laws or regulations) to enable requirement engineering. If product managers and others involved in requirement engineering have a homogenous group of customers and users, it may also be possible to get regular feedback and verifications on roadmaps. Various methods can be used for feedback and verification, ranging from focus groups with current users, user group meetings at regular intervals, meetings with strategic/important customers as well as new or potential customers. Examples of handy frameworks are given in Chapter 10 (for instance for municipalities, counties, and countries, and marine users). It is likely that additional industries will create similar frameworks, etc., craft common requirement processes and enhance their quality. In Sweden, the Swedish Civil Defence and Resilience Agency has crafted a high-level guide for critical infrastructures, which may be applicable to any IoT products targeting such contexts. The EU and ENISA have also issued a number of useful guides on cybersecurity for IoT and automation/control systems as well as critical infrastructures. These guides target the private and public sectors.

The frameworks and other publications are recommended reading. However, also required is thorough and elaborated work by product managers and others involved to collate as complete a set of requirements as possible.

There is a further need to prioritize and scope the set of requirements on a timeline. There are no short cuts, but help is available, including this handbook, to grasp the issue and work in a structured and systematic manner. Often, because many of those involved may have different perspectives, it is of benefit for organizations to have a common process to enable structure and a systemic work processes. This will improve the ability to capture the big picture and achieve as a good a set of requirements as possible. Lone heroes, no matter whether they use a process or not, will have a tough time and will not be able to meet all stakeholder and people of interest to collate the requirements.

4.2 Public procurement

Concerning public organizations and operations in the EU, procurement of IoT products and add-on services requires that legislation on public procurement is applied (if the total amount exceeds a legal or selected limit). Procurement in line with public procurement laws will make it more difficult for IoT product suppliers as it

hinders and delays the often necessary frequent dialog between procurement specialists and those who install and later use IoT products. Thus, it will be difficult to execute feedback and verification of requirements rationally and effectively. As an IoT product is procured and is further developed, these initial barriers are no longer a significant problem, making it possible to conduct frequent dialog between the parties.

This should preferably be stipulated in the procurement contract as it benefits all parties. Seemingly, it is easier for standard IoT products than for specialized IoT products, where additional development is needed to achieve the requirements stipulated in the procurement. Due to the sometimes costly and demanding public procurement process, smaller suppliers of IoT products may opt out to the advantage of larger suppliers. However, smaller suppliers can join others and, in that way, lower their own costs and efforts required to complete a public procurement process. See Chapter 9 for concrete examples of set of requirements and background information related to different use cases.



THE IMPORTANCE OF GOOD STRUCTURE ON THE REQUIREMENTS OF CYBER SECURE IOT PRODUCTS. PHOTO: ADOBE STOCK.

5. Cybersecure development

The development of an IoT product is just a small, albeit important and recurring phase, in the IoT product's lifecycle. Usually, there is a number of development iterations over time, to make improvements and manage problems. These result in regular new releases and updates/ patches. These continue as long as the IoT product generates income and can be maintained and further developed. As profitability falls or turns negative, suppliers commonly raise the maintenance fee for customers (to continue support/ maintenance) and make an end-of-life plan. The product owner or product manager then communicates the plan to object owners at customers.

The development of a complex IoT product may encompass a number of parts, such as: hardware, software on different levels (firmware, operating system, applications, data-bases and more frameworks on top of this), cloud services/ servers, AI/ML services, manual or automated services conducted onsite or remotely, and various processes and structures. However, all this requires that the development process coordinates a number of usually parallel development sub-processes some of which need to have either loose or tight integrations. Unless these are well coordinated, have clear development contracts, or standardized interfaces for how they fit and function together, it is likely that problems will arise later on, with poor results, drifting costs and low value. The image shows a development environment comprising measurements and test tools for IoT products, with a focus on hardware and software integrations.

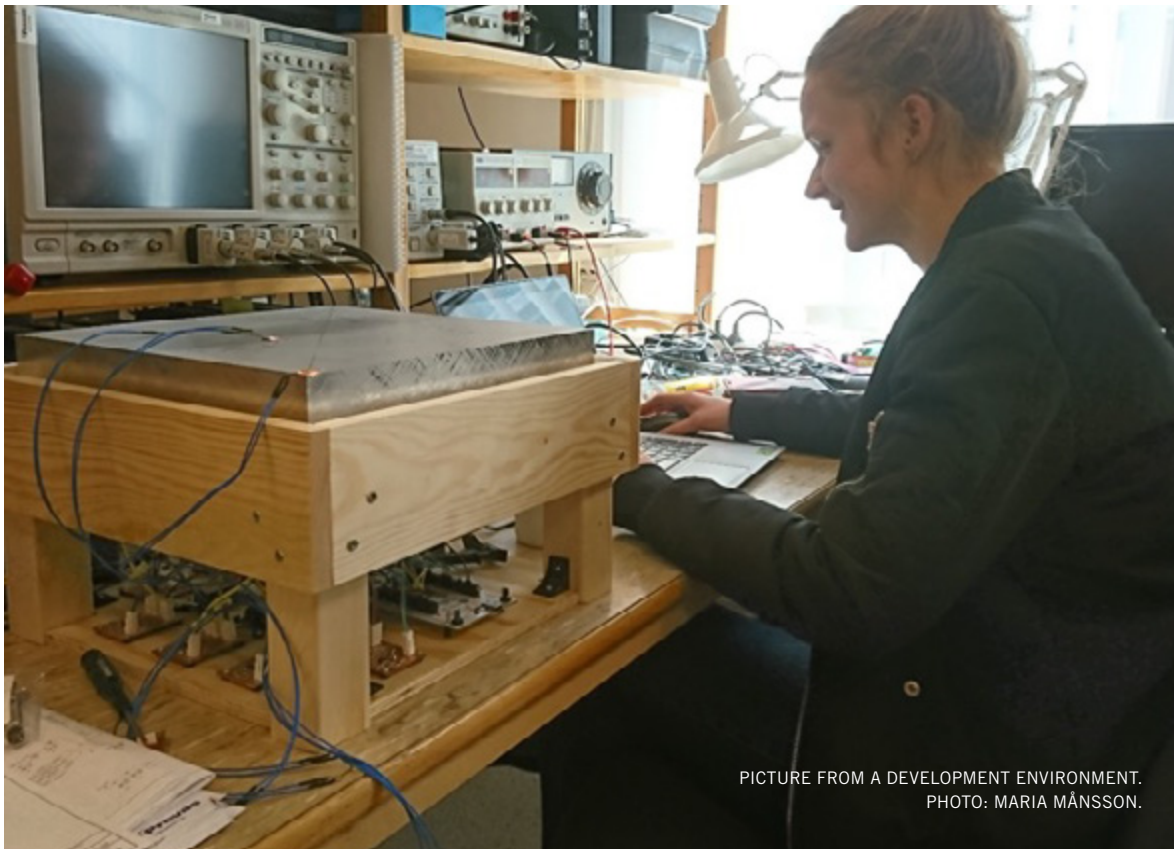
Besides working efficiently, an environment like that in the image needs to be cybersecure to ensure that the time, effort and money invested will not be accessed by outside parties who can simply steal/copy the ideas, blueprints/drawings, patterns, code, documentation, the IPR, and patent applications.

Further, unauthorized unwanted elements or code can be added, data stolen, and the development process disrupted. Moreover, even customer processes can be disrupted or equipment encrypted/destroyed later in the chain. Thus, a development environment must be protected. Security levels depend on what is in it, how much it costs to develop, and the profits that can be generated. There is a big difference between an IoT product that is projected to generate revenue of a few million SEK and another targeting billions of SEK in revenue. Other considerations include the target operational environments, i.e., domestic or critical infrastructures. An analysis is required to map out what needs to be protected, as well as weaknesses, threats and risks (see sections 3.4-3-6). Based on the result, cybersecurity for the development environment can be determined. Common ingredients are segmented networks, encrypted communications and data, access control, multi-factor authentication, and authorization schemes for what different roles can do and whether certain tasks require the four-hand principle (i.e., two people together to avoid collusion). Sometimes, development environments are divided into separated physical environments to be able to better protect the individual parts being developed.

However, this requires hands-on coordination and development contracts/interfaces for the parts that need integration.

Although, this is just the easy part. The harder part remains in the form of:

- Working in a cybersecure manner by not revealing any secrets to unauthorized persons and not opening up weaknesses or vulnerabilities through mistakes and poor cybersecurity awareness. IPR in the form of code, documents, manuals and blueprints/ drawings should have the appropriate protection and only be accessible and changeable in a controlled manner by authorized personnel.



PICTURE FROM A DEVELOPMENT ENVIRONMENT.
PHOTO: MARIA MÅNSSON.

In some cases, changes should only be made after an approval process or review (such as for software code or blueprints/drawings).

To achieve the above, the following may be needed:

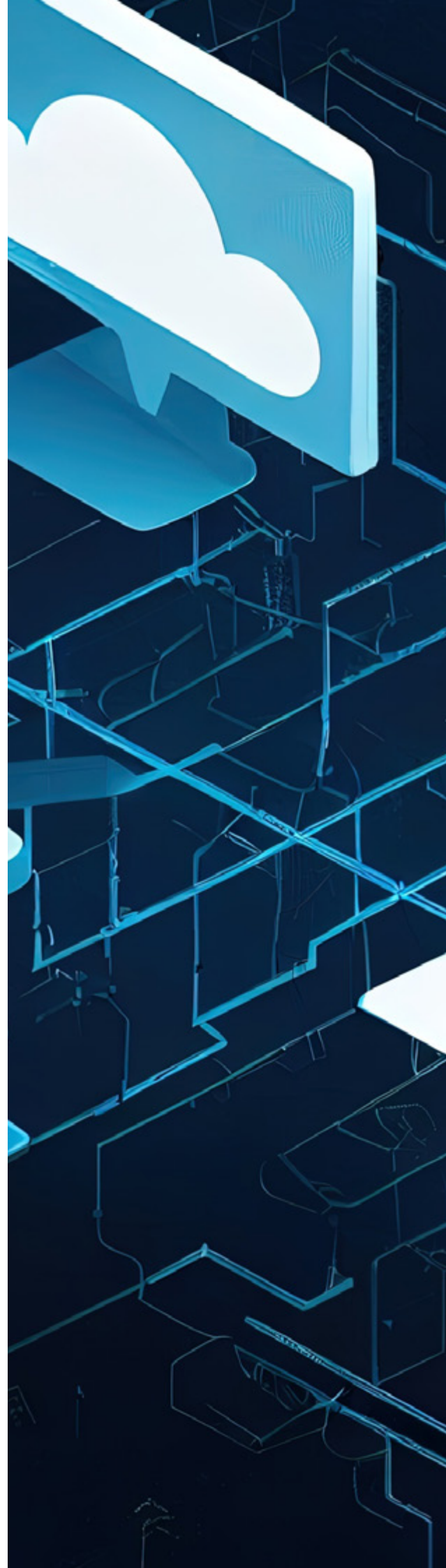
- Training the development teams in cybersecurity and cybersecure development – knowing how to protect their own IPR and develop cybersecure design, code, the ability to craft test cases for cybersecurity and automated test suites/test rigs including security tests (for such purposes OWASP's top-10 lists may be a good starting point along with similar material from major software or hardware providers).
- Ensuring control of the requirements or limitations in potential open-source code or open design that is used, and storing copies of such locally for future use if they disappear from Internet (as well as version control of the IoT product).
- Efficient testing of functional and holistic requirements (i.e., cybersecurity, digital preservation, quality/stability, availability, usefulness) as these are often connected as the holistic ones cut through. All this requires broad technological competence, and understanding of test requirements (see above in the handbook) and test scaling.
- What needs to be considered is the amount of much of testing that can be completed with few people involved through the use of smart test matrices and automated testing (test suites, test rigs, and test robots, etc., to cover all test cases, and performance/ load testing). Naturally, security test tools should be part of the automated testing, which will result in more security tests being executed throughout the development stage.

Some of the tests can be executed at night or in other time zones to shorten the total test time in calendar days, making the development process faster.

- Use cybersecure development tools and review open designs, frameworks, libraries or open-source code. Open designs and frameworks should be analyzed and tested before being inserted and used, and may further need to be monitored over time as the quality tends to decrease and the contents acquire additional contributors (which increases the risk of poor and dangerous code additions to the code base or unwelcome components/parts in hardware). This is not an easy task and grows over time. Thus, sufficient resources are needed. Always map out the background of open-source code and open designs in terms of history, how many updates were made and by whom. Are developments and improvements continual, or is it dead code?
- Have a cybersecure test environment that no external parties can change to falsify test results and reports.
- Use cybersecure collaboration tools for sharing documents, instant communications and online meetings.

All this requires work, time and cost compared with disregarding cybersecurity. However, the positive effects are increased efficiency in testing and improved test coverage as well as fewer problems and unnecessary costs later in the lifecycle. Further, such a set up and structure can be re-used for other development projects related to IoT products.

If flaws, errors or dangerous code strings are found in open-source code, procured software components, or open designs for hardware, it should be reported so that it can be corrected. Many suppliers of components, open-source code and open designs are happy to be apprised of faults, errors and bugs and may, in some cases, offer monetary rewards to the reporting party (e.g., bug hunters).





CLOUD-BASED CYBERSECURITY SOLUTIONS.
PHOTO: ADOBE STOCK.

6. Post development

– cybersecure support, service, maintenance and additional supporting processes and services

A cost driver and potential cybersecurity risk is when support, service, maintenance, additional supportive processes and services, such as hardware, software and operations optimization, are not well planned, and knowledge of the IoT products' target environments is limited. A supplier of IoT products may need a few options to manage the most common operational environments and use them to make special adaptations when using professional services (i.e., consultancy services). A few aspects should be considered. How will the process be managed? Do it onsite? Mix onsite and remote work? Do most of the work remotely hardware changes and mechanical maintenance? See section 3.7 for additional information on these requirements.

It is advisable to recommend object owners and users a cybersecure operational environment to emphasize its importance if their current knowledge in this area is poor and focused on operational processes. Further, cybersecurity is now a legal/regulatory requirement for many organizations due to EU NIS2 etc. This should be introduced during the business development/sales phase and will normally not be an issue. On the contrary, it signals responsibility and professionalism. If this is not brought up, or hidden from object owners and users, it will create problems later on for those involved after the development phase of the lifecycle. Preferably, the documentation of the IoT product (see section 3.5 for requirements) should comprise cybersecurity in the body copy or be brought together in an appendix. Besides installation and setup, it should describe how to verify cybersecurity levels using instructions, procedures or small utility applications that can be distributed along with the IoT product. Helpful figures that comply with accepted cybersecurity standards and guidelines should be part of the documentation as they help all involved.

Please note that if an IoT product has its own network or network segment and is connected to a larger network at the customer site, then the larger network should have the same (or higher) level of protection required by the IoT product. If not, additional cybersecurity protection (i.e., controls) may need to be added. It is also necessary to outline the communication channels and protection levels for those that are needed/recommended, what and who can access the IoT product, and what those with access are authorized to do (see example in section 3.2.3). Such controls include firewalls, advanced routers/switches/gateways, and data diodes.

The EU Cyber Resilience Act requires continuous monitoring of whether the IoT product (or offers where such are involved) is, or becomes, vulnerable. A consequence of this is that, during the lifecycle, there is a need to provide updates to mitigate vulnerabilities. These updates can be distributed and installed in a cybersecure manner.

Monitoring an IoT product, or a whole fleet of IoT products installed at customers, is becoming more common to collate requirements (and learn what does and does not work) and/or as an add-on service for predictive or condition-based maintenance and optimizations. It is advisable to separate/segregate the data pertaining to how an IoT product is used as well as further data about processes and quality. Such data, which can be used in fleet management functions, and provide an overview of weaknesses in the design, in specific components, in the entire concept, or in recurring problems (such as manufacturing flaws from a certain production site or rough handling), is an important part of cybersecurity. It is also important to gain a specific understanding of stability/robustness, availability, and what is worn/torn at different use levels in various contexts.

The level of wear/tear for an IoT product may require different maintenance if used in a damp and dusty mining environment than if it is used outdoors near a road or railway where the weather can vary. Thus, the data set should be considered, and users should assess whether different groups of data are generated that can create value for customers, their users as well as stakeholders and actors in the value chain. Based on the data situation, an information model can be crafted. Further, there needs to be a suitable agreement or contract with the object owners at customer sites and along the rest of the value chain concerning who owns what data or groups of data, where the data can be stored and processed, who can use what data for what purpose, etc. (cf. EU Data Act). It is difficult to achieve this after installation, so it should be discussed with customers at an early stage. The next step is to be able to extract data from an IoT product in an efficient and cybersecure manner, and transfer it to storage and processing for various purposes.

If data changes, configurations or optimizations shall be retrieved by the IoT product from a cloud service/server using a communication channel opened up by the IoT product as it transmits data (enabling appropriate and easy cybersecurity with fewer connections initiated externally). The data from an IoT product, depending on needs and cybersecurity requirements, and what is acceptable to the customer's object owner, can be stored in the IoT product (requires RAM memory and disk or memory card), on the object owner's local server, on a central server at the supplier or other part of the value chain, or in a cloud service. If an external cloud service is desired, from Microsoft or Amazon for example, cybersecurity needs to be set up and configured correctly, and verified regularly. Verification should always be conducted before using a new cloud service, or instance of such, and then on a regular basis so that laws, regulations, and recommendations are followed and aligned with what is required.



PEOPLE PROTECTING PRIVATE INFORMATION WITH ANTI-VIRUS SOFTWARE.
PHOTO: ADOBE STOCK.



CODE DATA ON A MONITOR.
PHOTO: ADOBE STOCK.

Many cloud services have flaws in their cybersecurity due to poor configuration and set-up in combination with failing to regularly verify the cybersecurity.

Further, during the design phase it is necessary to consider and investigate how support, service, maintenance and reconfigurations, as well as fleet management functions, can be conducted in a cybersecure manner. In addition, assess what has to be done onsite, onsite and remotely, or whether most of the work (except what must be done physically, such as maintenance and repairs) can be done remotely. It is helpful to draw up and visualize the processes to discover where collaboration and data sharing are required. If the process for distributing, retrieving and installing software updates can be executed smoothly and automatically (without virus or malware infections), it will be of great benefit. Some customers have a test environment where updates and upgrades are tested before being installed in the operational environment. These tests often run from a week to up to six months. Some customers allow operating systems and firmware to be updated without testing if the supplier is trusted and has a solid track record without mishaps.

However, a thorough fact check is recommended and that the required processes should be drawn up. According to the EU NIS2 and CRA, processes are required for incident management and related communications with customers and authorities.

Further, the EU EcoDesign Regulation will require bills-of-material for hardware and software. If possible, these should be created automatically. If a customer's policies do not allow external connections, the situation becomes more complicated, but one option is to use the same communications channel as data is transferred from for data retrieval, configuration changes, software updates/upgrades, etc. If this is not possible, more of the work must be done onsite. This requires routines to ensure that no viruses or malware have infected software and equipment physically brought in to object owners at customer sites. The object owner decides how data can be exfiltrated. It is advisable to have several options for how this is done in case the object owner rejects some options. It is usually unacceptable to have a continuously open connection for exfiltration of data unless required for rapid reactions or changes. Further, some operational environments cannot have continuously open connections except at regular intervals. Thus, various stages and buffering of data (for instance using a buffering gateway with firewall functionality above the IoT product or buffering built into the IoT product itself) combined with different data transmission mechanisms (such as FTP, secure email, IoT hub, local or global data ponds that export data after filtering and approval, mobile) and secure transfer (for example SFTP/FTPS, SMIME/PGP, HTTPS (XML/JSON), secure MQTT/AMQP, secure OPC-UA, mobile text messages, or other protected transmissions)

crossing various types of networks and topologies may be needed to be robust and not lose any data while in transit. Commonly used industrial protocols⁹ for collating data and/or automation/control functionality are Profinet, Profibus, Modbus, OPC/OPC-UA, etc. OPC-UA is being developed for cybersecurity and has an information model which can standardize processes for developers and object owners at customer site. The smaller the number of intermediary stages and buffering, the better and easier it is to maintain availability and cybersecurity. All intermediary stages buffering need to be monitored to detect stops or problems. Further, in sensitive operations environments, customers often do not want mobile communications with SIM cards as this can open up for cyberattacks.

All this should be found in the customer's policies and internal standards. For mobile communications, this needs to be managed by keeping it in a separated "island" in the network or having equipment (such as a data diode) that ensures only outgoing network traffic.

In case it is permissible to use controlled connections initiated from outside the network, these need to fulfill customer policies and standards regarding cybersecurity (this probably applies to IT and OT as a connection will likely traverse both the IT and OT environments). Preferably, the best option is to be flexible and use the customer's standard external connection options and not limit this to a specific home-grown solution.

Then, if it is possible to access/reach the IoT product after using the customer's solution for external connections or if there is an additional gateway or firewall with an extra VPN connection, it is usually possible to make it work. Customers often limit external connections. It is necessary to limit access for external connections, in particular those initiated from outside, and it should be possible to swiftly to shut down/terminate an external connection for a specific user, or for a group of users. Suppliers of IoT products to be aware of the common configuration parameters for external connections initiated from outside:

- Requirement for fulfilled process for identifying users and setting up user accounts (i.e., enrolment) as well as having successfully completed training in cybersecurity (i.e., with approved test result) to allow the use of an external connection from outside the network.
- Time-based access (what times during the day and what weekdays is access enabled).
- Authentication level (password, certificate, two-factor or multi-factor authentication).
- Authorization (what the user is allowed to do and with what tools etc.).
- Should access be low-level or high-level – what is required to be able to do what is needed? It is harder to limit low-level access (e.g., IPSEC VPN) than high-level access (e.g., SSL VPN). Many solutions for external connections often comprise low-level and high-level options; having only low-level options is not recommended. Thus, suppliers of IoT products need to be aware of this and not depend on a low-level access solution alone but also be able to offer high-level access.
- The cybersecurity of the device that is used to connect (e.g., end-point security).
- Time limitations for access. Access time should be limited and require a renewal in 1–12 months. If not renewed, users shall be automatically inactivated and removed (to clean out old access set-ups).
- If the above is in order, should it be possible to establish an external connection or does it first need approval and be opened up every time (e.g., by a customer user who checks a box in an interface and approves it) and is it possible to terminate at any point an active connection from outside,?
- Time limitations for sessions – it is common to maximize session times for external connections to 30–60 minutes unless otherwise required. Unlimited session times entail risk and are not recommended.

⁹ Some examples of relevant book summaries: <https://www.sciencedirect.com/topics/computer-science/industrial-protocol>

7. Monitoring the IoT product throughout its lifecycle

Monitoring an IoT product's general status and maintenance requirements is important enough to merit its own chapter. As a supplier, or other stakeholder or actor in the value chain that assumes this responsibility, it is an advantage to be able to follow up on an IoT product over time. However, this requires certain pre-conditions to be met. One is to agree with object owners at customer sites to be able to retrieve the necessary data, be able to exfiltrate it, and be able, and permitted, to use it for this purpose. One way to start is to generate an information model to map out the processes in which the data will be used before proposing an agreement with the object owner. Being prepared, it is easier to explain which data is required for which purpose. This helps object owners to see the value and may prevent an objection to "our data" being exfiltrated and used by others. Process and quality-related data is something else, although add-on services such as monitoring of processes (i.e., process parameters) and quality (e.g., tolerances for input materials, measurements during and after process stages, and output tolerances) as well as optimization can be offered based on whether there is access to such data. Figure 5 is an example of different groups of data that have been separated. The supplier owns what is related to monitoring and the status of the IoT product, the object owner or another suitable stakeholder at the customer owns what is related to processes and quality, and the final part is personal data, which needs to be handled in line with the GDPR in EU and corresponding privacy laws in the USA, India, China, Australia, etc.

Different types of data in the IoT product should be clearly separated before being transferred/exfiltrated further on using different tables in the database or even different databases.

It is easiest to use different tables in the IoT product as it may not have the processing capacity to run too many processes in parallel. Other impacting factors are license costs, whether it is feasible, and whether any such requirements are made by object owners at customers. Who owns the data, who can do what with the data, and what the data may be used for, are questions that need to be managed in an agreement or contract between the sales representative and object owner or other appropriate role at the customer. In addition, the EU Data Act requires that the customer get access to the data. Further, separation also enables different cybersecurity levels (e.g., encryption algorithms and key lengths) for groups of data and the capability to improve access rights and authorization for what can be done with the data.

The cloud service or server side (e.g., a local server operated at the customer site or a central server operated by the supplier) also raises certain considerations. Is it reasonable to mix customer data in the same database and tables (often referred to as "one-tier" or "multi-tenant") or do all, or certain, customers have their own instance in the cloud service or servers (if it resides at the supplier's)? The latter is often referred to as "multi-tier" or "single-tenant" solutions, and increases the complexity and cost of operations and licenses. However, if it is required by the object owners and they pay for it, it may be necessary to provide the service.

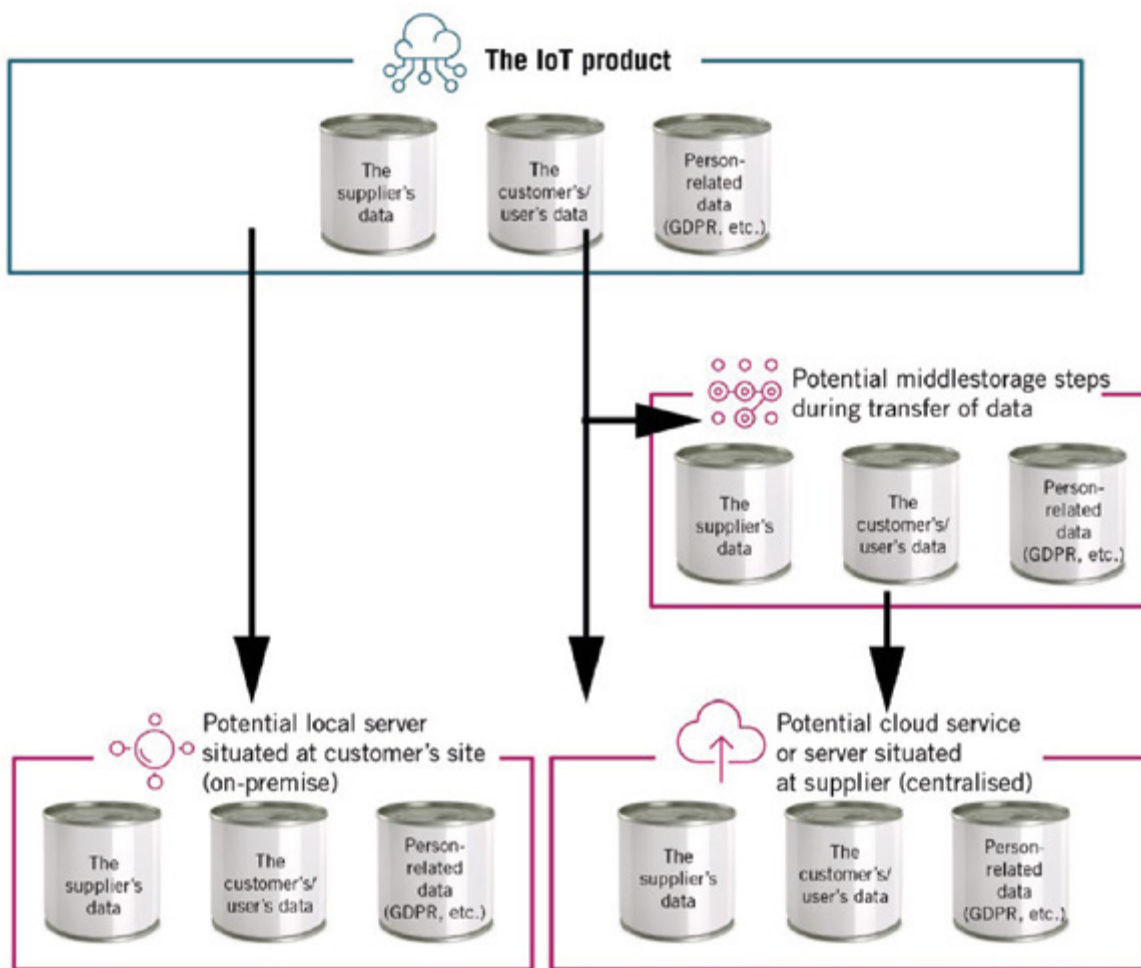


FIGURE 5 – EXAMPLE OF SEPARATION OF DATA IN THE IOT PRODUCT, LOCAL SERVER OR INTERMEDIARY STORAGE STEPS DURING DATA TRANSFER; AND CLOUD SERVICE/CENTRAL SERVER, WHERE THE SUPPLIER OWNS THE MONITORING DATA, CUSTOMERS OBJECT OWNER OWNS PROCESS AND QUALITY DATA, AND PERSONAL DATA IS KEPT APART FROM THE OTHER TYPES OF DATA.

By focusing on monitoring and the data relating to general status and maintenance needs, excellent opportunities are available to capture new requirements to develop new versions or generations of IoT products. However, agreements and preconditions need to be in place. Progress can be made by uncovering what works and does not, whether common problems arise, and whether the problems are related to the same root causes for an IoT product. If the same root causes are identified, the product manager and object owner, together with the development team and other suitable stakeholders, can analyze what needs to be done to make a sustainable IoT product that adds value.

In some cases, instructions or training needs to be made available for installers and users rather than design changes if these damage the IoT product through rough handling or being installed in the wrong places. Another aspect is to limit use so that an IoT product cannot break itself by executing certain operations or movements. Thus, monitoring needs to be structured so that data can be analyzed efficiently. Further, the data from those who conduct support, service, maintenance and repairs should also be collected to complement the data derived from the IoT product. To simplify data management and analysis of the human-generated data, it might be useful to use an application that groups data

into standardized groups and areas, which can then be complemented with free text when the data is entered. Free-text reports alone will hamper analysis and data management. It will require considerable effort as the data will need to be categorized and harmonized using a common measure or scale (i.e., normalization) to usefully analyze results and make comparisons.

The monitoring and follow-up of IoT products can be extended further. Only the imagination and ability of the development team will limit what can be achieved. For example, self-tests and self-diagnostics can be used, which are run regularly to check all components, parts, mechanics, that all functions are working, and tolerances are in the desired ranges. As a complement to the physical and functional tests, use of automated and built-in test suites can be used to verify the level of cybersecurity of the IoT product. Manual procedures can be used for this, but it is better to automate as much as possible. The data and results generated by self-tests, self-diagnoses, test suites, and procedures should be collated, stored and used for further analytics and follow-ups.

The next step might be to check whether availability requirements are extreme and make it hard for humans to physically access an IoT product. For such situations, the concepts of self-healing or self-repairing IoT products or parts can be useful, in combination with redundancy. Examples of such situations are when the IoT product is built into structures, is situated below water (or far under surface level), or is in the air or space. In such cases, check whether robots or drones (unmanned aerial vehicle - UAV) can be used carry out or assist in repairs, service, or maintenance, if humans cannot be present or if it is too dangerous for humans. In the future, non-human interactions with IoT products will likely be commonplace.

Fleet management is being further developed further. Additionally advanced business models will increasingly rely on fleet management functionality, where the supplier side can monitor and control what happens with the

installed products used by customers. It may not be an isolated IoT product, but rather an integrated product with services, a product-service system, or a function that has been sold under an agreement on contractual parameters such as: subscription, promised level of availability, promised level of improved productivity, risk and revenue sharing from the added value derived from the IoT product above a certain threshold. This requires the ability to monitor and follow-up, as well as the capacity to add to what can be done remotely, except what needs to be done onsite such as physical service and maintenance (often referred to as MRO – maintenance, repair, and overhaul). Further considerations are later re-use and reinstating, through remanufacturing or refurbishment, of parts of or the entire IoT product. This improve profitability and sustainability while lowering the environment impact. Fleet management functions usually grow organically with time as needs and possibilities are discovered. Below are examples of fleet management functions for monitoring, follow-up, administration, and configuration remotely:

- Prepare, at the supplier's or other suitable stakeholder, the installation and initial configuration, either for an individual IoT product or a group of such with plug-and-play. For this, the IoT product needs to be aware of certain matters from the start as it arrives at the customer's operational environment. Installation/configuration should be prepared at the supplier's or other stakeholder's in the value chain. Further, the IoT product should be programmed to know where it can automatically retrieve/download the full installation and configuration in a cybersecure manner.
- Remote administration and configuration – to be able to change settings and configurations in one IoT product or group of IoT products and initiate the change. Further, updates and upgrades can be initiated this way and be synchronized with various asset management functions below.

- Emptying/removal/wiping of data and deinstallation – the ability, at the end of the use in the customer’s operational environment or end of the lifecycle, to remotely empty/remove/wipe IPR and data from all parts where such are, or have been, stored (i.e., applies to the IoT product, any intermediary stages and -storage, in cloud services or server parts). It should be possible to control whether this applies to only one IoT product instance, a group of IoT product instances, one/some/all at a certain customer or a group of customers that are part of the fleet. The latter functionality should require that more than one administrator do it, i.e., it should require the cooperation of 2–3 people with appropriate authorizations to minimize mistakes and sabotage. Further, there should be a verification notification (and logging) when such operations are completed. More on this in the following chapter.
- It should be possible to limit an IoT product’s functionality and operational level in case of problems (e.g., graceful degradation) to reduce the load or, at worst, automatically initiate a shutdown to avoid serious and costly damage or breakdowns. Depending on the context, such decisions may sometimes require a human decision, but a high level of automation of such decisions can save expenses or at worst to have to buy a new IoT product. If such problems are identified early using the fleet management functions, the users/operations at the customer site can then decide how to handle them if a temporary replacement is needed until the issue is resolved.
- Collection of feedback and complaints from customer users on the IoT product – if there is no other channel to the product manager, for instance via a web site, social media or user groups, the fleet management functions can be used to collect feedback and complaints. The feedback and complaints, which can generate new development requirements or ideas for improvements as well as the correct errors or unclaritys. The use of a standardized input for different areas and functions (using normalized measurement data and estimations) with space for free text input can be beneficial to enable this data to be matched with the data from support, service, and maintenance.
- Asset management – be able to monitor what IoT products the customers have and where they are installed and operating. An overarching asset management system should be connected to the below systems/functions relating to change/configuration/obsolescence management as the asset management system is hierarchically above these:
 - Change management – store data about planning, execution, and results of changes in operations (e.g., re-configurations and set-ups plus the context of the operation).
 - Configuration management – store configuration data to know what hardware and components each IoT product has, which software versions, and when updates/upgrades/patches are made to a version. This saves considerable time and facilitates planning of updates/upgrades/patches. It also enables searches of ongoing cyberattacks when there is a need to detect whether the software and version under attack. An example is the recent log4j issue.
 - Obsolescence management – this pertains to storage planning the number of spare parts/components and old versions of software that need to be available and for how long. It is expensive and ties up capital, which may not convert to revenue, and may also require considerable space (which may also cost). Obsolescence management can be a useful and profitable part of the business if managed properly and optimized.

A correct overview and basis for decision-making requires a status summary to know what is happening and whether any acute matters need to be taken care of. A fleet management system or function may have a cockpit or management view, from which it is possible to drill down to further detailed operator views for those who continuously monitor and manage problems in the fleet of IoT products.

8. At the end (or a new start) of the lifecycle

– cybersecure decommissioning and destruction of data/information in the IoT product and potential cloud services etc.

Before the operational phase of the lifecycle begins, it is hard for suppliers of IoT products to foresee how the products will be used and who will use them. Further, it is also hard to foresee new areas of use and potential extensions of requirements, etc., that materialize and can be capitalized on in terms of business, social, or ecological sustainability. In addition, object owners at customer sites often wish to extend their agreements/ contracts far longer than the supplier would like to. This is because the object owners discover that the IoT products work well and are still creating value in an environment where new investments are made mostly as assets break down, or cause too high risks or physical danger. Extending the lifecycle and offering support, service, and maintenance for an IoT product places an extra load on the supplier and value chain. To compensate for this, the license fee is often raised to reflect the extra load and cost, as well as the inability to focus on recent IoT products.

As the world's resources are being used up, new forms of thinking and concepts are being adopted among suppliers and value chains that manage some physical products or systems. To improve resource management and optimize use to increase sustainability, various ways of extending IoT product's lifecycle are being examined. This is often called the "circular economy". Recently the "elliptic economy"¹⁰ has emerged, where the use phase is extended further to reduce global resource consumption, and is being investigated by suppliers.

To reach such sustainability, a supplier should also consider which existing/improved/new business model to use, what the foundational and cybersecurity infrastructure should look like, and what sort of knowledge and training packages are needed. The following should be considered:

- **Application of plus-1 strategy**, which may entail that one or several functions are added, and other features are slightly improved so the IoT product can extend its lifecycle and be sold a few more years to create value for object owners at customer sites. This can make for satisfied object owners. Such a strategy has often been used by auto manufacturers, where some models have been sold for up to 20 years or more.
- **Remanufacturing or refurbishment** extend the lifecycle by changing worn parts or components. These can be combined with upgrades or parts or components that improve the IoT product's functionality further on.
- **A similar concept is reconditioning**, which encompasses cleaning up and restoring surface layers and testing that they are acceptable. Sometimes a few parts can be changed, but not usually as part of reconditioning. Reconditioning is offered by suppliers of used servers, network equipment, cars, and mobile phones that are in good condition.

¹⁰ <https://www.industrinyheter.se/20221118/35318/elliptisk-ekonomi-annu-mer-hallbar-cirkular>

- **Repurposing**, which may entail using the IoT product for applications that were not part of its original scope, and where an older version of an IoT product will be sufficient.
- **Down-cycling**, which means that an IoT product can be continued in markets or contexts that have lower requirements, or the capacity to pay is lower, than the primary market but the business volume is still of interest. Developing countries are an example of this.

To achieve the above at the end of the primary lifecycle, an IoT product needs to be emptied/wiped of IPR details and data/information returned to factory settings or dummy contents. The image below shows part of the recycling process of electronics and metals, where IoT products should have been emptied/wiped before being added this process.

At end-of-life, the documentation/user manual should comprise instructions for how to prepare the IoT product and its parts for end of life/scrapping/destruction/recycling without compromising IPR or data/ information (such as configurations, set-ups, recipes/programming, operational information such as IP addresses, etc.) to unauthorized persons. Thus, all products need to be emptied/wiped regarding IPR and data/information, all of which should be verifiable.

The measures above apply to all locations where IPR and data/ information are stored, which may include much more than just the IoT product. Cloud services, servers, AI/ML services, and intermediary storage used should be included too, and be verifiable. Thus, it is an advantage to add a function that empties/ wipes all IPR and data/information from all places for each IoT product, a group of such, a customer's IoT products, a group of customers' IoT products, or all customers' IoT products, at end of life.



RECYCLING OF ELECTRONIC COMPONENTS AND METALS. PHOTO: ADOBE STOCK.

9. Use cases

Early on, it is difficult to understanding and capture a complete set of requirements for an IoT product because when it is used new ideas and experiences are generated. To better enable capture, relevant use cases may provide a better initial overview of the set of requirements for everyone in the development process. Chapter 9 is a continuation of Chapter 4 and provides a few examples of use cases. Before starting up the development process, use cases should be complemented with additional information about the operation and use of the IoT product.

9.1 Use cases with concrete examples

Below are five use cases ranging from domestic (home) to professional environments. The purpose of the cases is to generate an understanding that the cybersecurity needs in various contexts are not identical. The more cybersecurity required, the more it will cost to develop, test, certify, etc., throughout the IoT product's life-cycle. Further, the more the functionality, the more the work that will be required later on for further development and maintenance.

To outline the use cases, a common structure has been used to make it easier to compare them:

- Organizational type – brief description.
- Operations/processes – introduction of the operations/processes to understand the set of requirements for the IoT product. The requirements may differ among: customers/users, laws/regulations, industry standards and other stakeholders.
- Type of IoT products and how they are used.
- Cybersecurity requirements for IoT products.
- Other – areas of interest not included in the above

9.1.1 Use case – domestic (home)

- In a domestic setting, the use case ranges from apartments in multi-tenant buildings to townhouses, houses and cabins. Home standards are increasingly improving, which also applies to the infrastructure in the form of Internet connections via fiber, cable TV, and mobile networks. Most households have a low level of cybersecurity awareness and related knowledge about how to cybersecure the household and achieve a hygiene level for cybersecurity.
- People spend a lot of time in their homes and use a variety of connected products, machines and systems that have requirements for sustainability/recyclability, energy efficiency and cybersecurity. Also required are mandatory standards for electrical safety and type approval with CE marking. Others recently added include personal data (GDPR), IoT security for consumers (ETSI TS 103 645/ TS 103 701) and the EU Resilience and Cybersecurity Acts, with their requirements for a hygiene level of cybersecurity in digital consumer and professional products.
- Domestic settings are going through the replacement of “unsmart” home electronics and appliances, machines and systems with increasingly smarter and connected IoT products such as: refrigerators, washing machines, toasters, baby monitors, TV and media equipment, smart watches with pulse meters and GPS, mobile phones, home computers/pads, game consoles, Alexa or Nest-like devices from Amazon/Google/Apple, heating/cooling systems, building automation systems, lock and alarm systems, cars and lighting fixtures. All these increasingly smarter IoT products are used to increase comfort, remotely monitor and control functions or control automatically (e.g., control by energy cost level), check the status of locks



MANY PEOPLE SPEND A SIGNIFICANT AMOUNT OF TIME AT HOME, WHERE A WIDE RANGE OF CONNECTED PRODUCTS, APPLIANCES, AND SYSTEMS ARE USED.
PHOTO: ADOBE STOCK.



and alarm system including water leakages. Their purpose is to improve and simplify daily life as much as possible. There may also be instances of e-health or home care, which use sensors and safety alarms. In such cases, personal data and its integrity as well as availability are of great importance.

- The domestic context requires cybersecurity considerations for what the habitants want to protect. Usually, large amounts of personal data are available, which should only be accessible by those concerned, which implies that mobile phone security must also be part of this. Apps exist that collate and transmit data or information as well as what various sensors, microphones and cameras pick up. A hygiene level, or baseline, for cybersecurity is needed to protect homes from cyber-attacks and intrusions. Ideally, protection should be layered, starting from the Internet connection and inwards to prevent malicious actors from: destroying IoT products, learning whether people are at home, accessing alarm/surveillance system cameras, opening locks or disabling alarm systems, planting encryption viruses, or using the IoT product as part of botnets. A hygiene level entails having a firewall/router at the Internet connection and to segregating/segmenting the network(s).
- If individual IoT products need a higher level of protection due to their sensitivity, such as alarms, cars, mobile phones, computers, building automation, these should be especially well protected. Besides the network, anti-virus or anti-malware solutions, local firewalls, etc. should be in place. However, some current IoT products may not have this capacity and will therefore be vulnerable. For advanced availability requirements, for instance in e-health or home care situations, and alarm and monitoring systems, extra measures may be needed for cybersecurity in addition to having a redundant Internet connection via fiber, cable TV or mobile networks.
- Further, hardening the network and IoT products will also improve cybersecurity. Hardening means that non-essential services are removed or inactivated, communication is limited to only authorized and essential communications (i.e., non-essential communication ports should be closed and, if possible, only required protocols allowed on the open ports and between network segments). It would be ideal if the supplier hardened the IoT product from the start, to be opened up on commissioning (i.e., secure-by-design) if required. The main issue for households is the cost of installing an appropriate level of cybersecurity.

Therefore, many households spend too little and end up with a poor hygiene level, which is not maintained over time. Another major issue arises if the supplier has not developed the appropriate level of cybersecurity, as it seldom improves over time. Further, it is good practice to enable automatic updating/upgrading to install cybersecurity updates as they are released (i.e., fast). Moreover, a warning should be issued if there is, or appears to be, a security breach.

- In addition, a common sense of cybersecurity hygiene and basic knowledge of what to do and what not to do are necessary. This should include: not clicking on unknown links or files sent by unknown people; not opening attached files which have not been checked by an anti-virus solution; not being conned/defrauded by strangers on the phone, or by text messages/emails with links. This is referred to as cybersecurity awareness. Further, all new procurements or re-installations of an IoT product's basic configuration should require mandatory changes of: device name, user account names, passwords, network addresses and IP masks. It is often possible to apply a high level of cybersecurity, but this may require that the basic configuration be walked through, reading the instructions, and being elevated using stronger encryption algorithms and authentication levels.

9.1.2 Use case – industrial organizations or corporations with production and distribution processes

- Manufacturing and process industries often have an administrative environment (IT) and the manufacturing/production environment (OT). Further, distribution processes are sometimes connected to the OT environment but are usually partly or wholly separated. Previously, in many cases only the IT environment was connected to the Internet. However, now OT environments are usually connected, and can be connected, to the outside.
- Some OT environments are not connected, or only poorly so, to the Internet. Cybersecurity awareness and maturity have always been satisfactory in parts of industries. However, awareness and maturity need to be strengthened among almost all employees today, and industries must organize their cybersecurity for IT and OT environments as these are usually interconnected.
- Many industrial corporations and organizations operate outside normal working hours, often run multiple shifts or 24/7, with planned downtime only one or a few weeks per year. The more continuous the operations are, the harder it is to make changes in the production processes. Detailed planning is required for changes or new installations to be able to complete them in the planned stoppage. It is also important to be able to restart and be operational as soon as possible after stoppage, preferably without issues or disruptions. For efficiency reasons, it is increasingly common for suppliers and consultants to be able to connect from the outside to provide their services. Further, many IoT products need to share data with internal and external recipients. A number of sustainability requirements for IoT products need also be considered, such as those related to the surrounding environment, the need for robust and stable functions, as well as being recyclable, energy efficient and cybersecure. In addition to work environment requirements, electrical safety requirements and type approval with CE marking, the EU GDPR, NIS2, and the EU Cyber Resilience and Cybersecurity Acts require a hygiene level of cybersecurity for digital consumers and professional products.
- The manufacturing/production environment contains a wide variety of IoT products with sensor solutions for monitoring and controlling processes and production equipment. Further, also common are alarm/lock systems, building automation with ventilation, heating, and cooling, maintenance systems that monitor the condition of production equipment

and assets, measurement systems for piles of production input materials (i.e., raw materials), warehouse systems providing barcodes for production output, etc.

Distribution processes also use IoT products to keep track of where output is and that the output quality is kept at a required level (e.g., moisture, cooling or maintaining the right temperature) until delivered. In distribution environments, physical security is often lower than in the manufacturing/production environment, which must be considered properly. Manufacturing/production and distribution environments can be tough on IoT products in terms of physical protection (i.e., environmental protection for water/dirt/dust/cold/heat, impacts and physical intrusion attempts to connect to internal networks via the IoT product) and cybersecurity.

- In industrial corporations and organizations protectable information resides in the IT and OT environments. As most of the value is created in the manufacturing/production environment, it needs to function and operate well. Thus, aspects such as availability, robustness and stability in the manufacturing/production processes are often the most important. Further, the integrity of the processes must be maintained, and variations, stops or disruptions need to be avoided to ensure that the resulting output has an stable and required level of quality. Large amounts of information reside in such processes, some of which can be confidential concerning knowledge of processes and implementations, methods, recipes/patterns, programming, etc. Knowing whether a manufacturing/production process is operational or not can be valuable. Thus, IoT products, such as sensors, measurement, monitoring and maintenance systems need to have proper physical protection combined with a required least level of cybersecurity hygiene. Weak areas, if they exist, are where problems mostly occur. Regarding hygiene levels, the first step is to segregate the networks into IT and OT segments and then divide/segment the OT environment into

smaller sections to keep the processes apart. This protects them from problems and allow authorized communication only in and out of the segment (as well as between segments). Besides the above, users should only be allowed to do what they need to (and no more). External connections should be controlled and data shared only with the right recipients

Moreover, network monitoring, patch routines, incident management, backup and restore processes, etc., are necessary as well. Many IoT products have poor inherent cybersecurity and cannot be reasonably upgraded or replaced. Thus, some should not be connected to the OT networks, but be in islands.

Another issue in OT environments is to manage third parties (i.e., suppliers/vendors and consultants) that move around in the environment, and to ensure that these do not bring in viruses/ malware or connects “objects” without having proper authorization from those responsible for OT security to do so. Distribution environments often comprise IoT products that are exposed and can be used as entry points to access networks and spread viruses/malware. Thus, these IoT products need physical protection, and communication with them needs to be controlled. Cybersecurity must be considered and maintained over time, as well as on decommissioning, to prevent IoT products being discarded in public recycling containers with their packaging.

In addition, IoT products should be hardened. This entails removing or inactivating unnecessary services, and limiting communication on specific ports, applications and protocols to only what is needed. The supplier offer hardening as part of their basic configuration, and that if desired or required some objects can be opened during installation. General basic configurations for hardening should be applied as general practice. The main problem for industrial organizations and corporations is often lack of competence and clear rules, which may result in cybersecurity issues in the OT environment.

Another problem is that the cybersecurity in OT environments is more underfunded than the IT environment, which is somewhat strange as most value is generated in the OT environment. An additional, but smaller issue, is that supplier warranties require that upgrades and patches must be approved/authorized before installation, which causes delays that open up vulnerabilities.

- In general, good cyber hygiene and knowledge of what to do and what not to do are needed. For instance, mobile phones must not be charged via USB ports on equipment, uncontrolled (USB disks) should not be used, nor should unauthorized or uncontrolled software be installed. Moreover, users should not click on unknown web links, open attached files from unknown senders, which have not been checked for virus/malware, nor become a victim of social engineering initiated via the phone to get access to login information. Further, all new procurements or re-installations of an IoT product should entail that factory/basic configurations be changed with respect to device name, user accounts, passwords, network addresses and IP masks.

The cybersecurity level should be set at the same level as, or higher than, the hygiene level decided. This may be an issue as AI-based threats have dramatically reduced the time to address and remedy vulnerabilities.

9.1.3 Use case - maritime industry

- Maritime industries, spanning vessels, platforms and harbors, usually have an administrative environment (IT) and another for production (OT). This differs somewhat from land-based settings as the maritime industries, including parts of their distribution processes, are most often situated in ecologically sensitive areas. The distribution processes are sometimes connected to the production OT environment, such as pipelines from oil/gas platforms, but usually they are separated by using vessels for transport, which their own IT/OT environments (which may be connected to the Internet to share data or retrieve updates etc.). Previously, only the IT environment has been connected to the Internet but an increasing number of OT environments are being connected (which requires high-level



cybersecurity depending on the type of operation, criticality and risks perceived). The cybersecurity awareness and maturity in parts of the maritime industries has been good for a long time, but now it needs to be strengthened for almost all employees. These corporations need to organize their cybersecurity for both the IT and OT environments.

- Many maritime industries have round-the-clock operations and only stop production for one or a few weeks a year. The more continuous the operations are, the harder it is to make changes and, in such cases, changes or new installations must be planned to ensure that they are all completed during the downtime and can be smoothly moved back into operation again without disruption. AI-based threats require rethinking here. For reasons of efficiency, it is becoming increasingly common that suppliers and consultants need to exfiltrate data from IoT products to be able to plan for activities and optimizations (and create external connections to provide services remotely). Thus, there is an increasing need to be able to exfiltrate and share data from maritime IoT products for both internal and external use.

However, this requires an Internet connection, which is not always available, and the bandwidth may be low and expensive (if satellite communications are used). Mobile network coverage is improving, but still does not cover many remote places on earth. IoT products for maritime use have a number of requirements pertaining to sustainability. These include the environment they are used in; a robust and stable function; and being recyclable, energy efficient and cybersecure. Besides common workplace safety regulation, electrical safety requirements and type approval, the UN/ IMO/IACS requirements for cybersecurity (if class action and based on IEC 62443 3-3/4-1/4-2), GDPR in the EU, NIS2, and the EU Cybersecurity and Cyber Resilience Acts concerning cybersecurity for digital consumer and professional products all need to be considered. Vessels that travel the world are subject to a number of additional legal frameworks as well as physical security and cybersecurity in harbors, to prevent unwelcome objects coming onboard.



CYBER SECURITY RISK ANALYSIS TEAM REDUCES RISK.
PHOTO: ADOBE STOCK.

- In production processes on board, a number of IoT products for monitoring and control of processes, production equipment and propulsion are commonly used. Further, IoT products are often used in steering/navigation and communication systems, physical security (warnings, evacuation, fire extinction systems, etc.), alarm/lock systems, automation for ventilation/heating/cooling, clean water production, measurement systems for cargo and tanks, etc. In addition, distribution processes use IoT products in similar ways as production processes, but also to keep track of where output/products are and ensure that their quality remains intact (e.g., pressure, moisture, cooling, keeping in the right temperature range). In distribution environments, physical security often depends on the age of the vessel and may require improvements so that unauthorized persons cannot gain access to IT and OT. Production and distribution environments can be tough on maritime IoT products in terms of physical endurance/protection (environmental protection from water/dirt/dust/cold/ heat, resisting impacts, sabotage and physical intrusion, attempts to connect to the networks via the IoT product) and cybersecurity.
- In the maritime industry, a great deal of information resides in the IT and OT environments that needs to be protected as most value is created in the production and distribution environments. Thus, value creation requires a high level of availability, robustness, and stability in the processes. Further, the integrity of the processes needs to be remain high and level, with stoppages and disruptions avoided, to achieve output with a stable and required level of quality. Significant variations in production processes may cause danger. Among the large amounts of information in a production process, some may be secret, such as process and implementation knowhow, methods, recipes/patterns, programming, etc. Further, knowing whether a production/distribution process functions or not may be valuable if it affects stock market prices,

for instance. IoT products, e.g., sensors, measurement equipment and systems, monitoring systems, operation systems, control/navigation/planning systems, communications systems, and maintenance systems, need adequate physical protection in combination with an approved level of cybersecurity. The level required depends on the operations and context as well as the class of a vessel or platform. The level is often considerably higher than for land-based industries. The basic level usually requires that the IT and OT networks be segregated, and that the OT environment be divided into smaller segments so that different processes are isolated and protected from others, with only authorized communications inside the segment and between segments. Besides that, there is need to ensure that users can only do what they are supposed to do (and not more); control external connections and how data can be shared with the right recipients/partners in a secure manner; monitor networks; ensure patch routines; update incident management; and ensure that backup and restore works. Many older IoT products have a poor inherent level of cybersecurity, which cannot be reasonably upgraded or replaced. This means that they are not permitted to be connected to the OT network, but reside in isolated islands. Since the introduction in January 2024 of tougher requirements, certain older IoT products may need to be replaced and may not be allowed to be installed in new builds. Another issue is how to handle third parties, vendors and consultants who are in the OT environment to ensure that they do not introduce viruses/malware or connect “objects” without authorization from those responsible for OT security. Maritime distribution environments often house IoT products that are exposed and can be used as a stepping stone to access networks and spread viruses/malware. Thus, there is a need for physical protection, to control who can communicate with them, to consider how to maintain, cybersecurity over time and determine what happens at end-of-life.

Further, maritime IoT products need to be hardened, which entails removing or inactivating unnecessary services, strictly limiting the communications only to ports, applications, and protocols where authorized traffic should pass. The supplier should offer hardening as part of basic or factory settings, which can be opened during the installation if required. It is advised to use basic configurations for hardening to minimize human error. A major issue for the maritime industry is often the lack of sufficient competencies and organization as well as locally implemented rules, which may result in issues related to cybersecurity in the OT environment. A lesser issue is the suppliers' function warranty, which usually needs supplier approval before upgrades and patches can be installed. Suppliers often take time to do the testing required, which leaves a time gap in which the IoT product is vulnerable.

Generally, a level of cybersecurity and knowledge should be in place about what not to do, e.g., not charge mobile phones in USB ports on devices or equipment; not use uncontrolled media (e.g., USB sticks); not install uncontrolled software; not click on unknown links or open any files/attachments that have not been scanned for viruses/ malware, etc. Further, each new procurement or re-installation of a maritime IoT product's basic configuration should require mandatory changes of device name, user accounts, passwords and network addresses and IP mask. Cybersecurity should be set to the required baseline, or above, (which can be determined by class action).

9.1.4 Use case – municipalities (which are governed by public procurement legislation)

- Swedish municipalities operate widely and to a varying extent. Certain parts are similar to critical infrastructures, industrial organizations and corporations, and healthcare, whereas other parts are oriented toward administration. There are only a few very large municipalities,

some are medium-sized, and most are small, with a population of a few thousand to ten thousand. The small populations in most municipalities, and if they are rural, has a negative effect on the availability of adequate competence in IT, OT, IoT products and cybersecurity in general. Some parts of the operations are more challenging than others, e.g., primary and secondary schools where almost all pupils are connected, as well as public locations such as libraries, sport arenas, buses and squares all provide public municipal Wi-Fi-connectivity.

- A municipality is usually divided into administrative districts/areas, such as: public service, primary and secondary school, social care, recreational activities, culture, environment and construction/building, digitalization, rescue services, harbors, etc. In addition, election and guardian districts/ areas may exist. For urban construction/building, a technical office deals with real estate, traffic control and lights, sewage and clean water production, as well as IT (unless that has its own function in the municipality). Some municipalities have their own energy corporations with energy production and distribution. Other districts/ areas have responsibility for schools, libraries, sport arenas and facilities, elderly care and shelters, local public traffic (buses and trams etc.), which all may have their own IT, OT, or MT (medical technology) infrastructure, IoT products in multiple locations. In a municipality, the boundary and definitions for what is classified as critical infrastructure may be somewhat unclear and should be given more attention. The critical context concerns areas such as sewage management and clean water production, energy production/distribution, traffic, rescue services, and elderly care. Further, larger roads, public transportation, airports, and harbors with major logistical impact should be part of the critical context. Depending on the population of the municipality and the operational impact on society at large, the critical districts/areas mentioned may be subject to national security protection laws and secondary laws from the Swedish



JUSTICE. JUDGES CLUB. PHOTO: SHUTTERSTOCK.

NCSC, Swedish Civil Defence and Resilience Agency and Swedish Food Agency, and other authorities. Sensitive personal data/information is kept by many districts/areas, and requires a high level of cybersecurity. Thus, legal and regulatory frameworks, such as GDPR and NIS2 and the EU Cyber Resilience Act need to be considered.

- Due to the wide array of municipal operations, numerous IoT products are installed at many locations (depending on the level of digitalization). Many IoT products are used in a similar manner to those in industrial organizations and corporations, critical infrastructure for monitoring and control. Areas of applications include building automation (ventilation, heating, and cooling), surveillance/locks/alarm systems, etc. In health and elderly care, IoT products are used to monitor patients, in equipment for remote care (likely to increase substantially), safety alarms, and other applications that enable health and elderly care in clients' own homes at increasingly higher ages. Thus, many IoT products are installed and used by municipalities, and the numbers will increase as far as cybersecurity allows.
- Common problems in municipalities related to cybersecurity and the use of IoT products, are lack of competence, budget constraints, and the fact that public procurement legislation discourages certain suppliers. In addition,

the breadth of the operations increases the burden. For small and medium-sized municipalities, the main issue often is to recruit the right competence. Using consultants is a short-term solution. As a result of the COVID pandemic and subsequent digitalization measures, it is easier nowadays to get remote support or help. Small municipalities usually have small budgets and an IT department of 2–3 employees who have to manage 100+ systems and cybersecurity as well as everything else. This equation simply does not add up. To find solutions for the future, neighboring municipalities have started to collaborate and share systems and competences.

Larger municipalities usually have access to a wider range of competences and consultants. Unfortunately, public procurement legislation discourages IoT suppliers to do business with larger municipalities, too.

- In general, municipalities need to adhere to the increasing requirements for improved cybersecurity and AI-based threats as they store and process sensitive information and have critical operations and infrastructures. Thus, a general improvement of cybersecurity is needed, which also applies to the IoT products used in the wide range of operations in the districts/areas. Cybersecurity requirements vary depending on the type of operation and whether the IoT products are connected in the IT or OT environments, or operate in smaller

isolated networks. Paramount for municipalities is to recruit and ensure access to cybersecurity competence and the additional competences needed for IoT products. The use of IoT products is likely to increase considerably in the next 20–30 years as older infrastructure is gradually replaced and additional monitoring with different types of sensor solutions applied. Small and medium-sized municipalities ought to cooperate and share systems, staff and competences. If such cooperation and collaboration is initiated, municipalities need to agree and coordinate the selection of IoT products to be used and the cybersecurity levels to be applied so that the appropriate competences can be acquired.

9.1.5 Use case – critical infrastructures

- Whereas industrial organizations and corporations, and maritime industries have much in common (see earlier use cases), critical infrastructures are of further importance to society; hence the classification “critical”. Parts of industrial organizations and corporations and maritime industries can have a significant impact on society and cause major disruptions, in particular if value chains involved with production of components and
- merchandise, food production, and logistics, are impaired. Operations in the EU, which are classified by the NIS2 Directive as critical infrastructures/sectors and comprise: energy, transport, banking, infrastructure for financial markets, healthcare/hospitals, distribution of clean water and waste water management, digital infrastructure, ICT services (business-to-business), public administration, space, postal and delivery services, waste management, distribution of chemicals, production/treatment/distribution of food, manufacturing/production, digital supplies, and research.
- Most critical infrastructures with production and distribution operate their processes round the clock and may only be able to make brief stoppages in production and distribution. Some may have shorter stops, such as clean water production when the water towers are full until they need to be refilled, whereas sewage management and electricity distribution need to operate continuously. The more continual the operations are, the harder it is to change production and distribution processes. In such cases, all changes and new installations must be carefully planned and coordinated so that during down-time, they can be executed, and operations resume smoothly again afterward. For reasons of efficiency, employees may need to connect



from the outside, perform tasks and check that everything is progressing well. Third parties should not be allowed to connect from the outside unless there are strong reasons for doing so. Further, the need to share data from IoT products internally and externally is increasing. Multiple requirements relate to environmental sustainability, robust and stable functions, recyclability and energy efficiency, as well as appropriate cybersecurity. Besides legislations related to national security and safety, requirements exist for occupational safety and the environment, electrical safety and type approval with CE marking. In addition, guidelines are in place from the ENISA, Swedish NCSC, Swedish Civil Defence and Resilience Agency, and Swedish Food Agency, as well as legislation/regulations concerning EU's GDPR, NIS2 and the forthcoming Resilience and Cybersecurity Acts (with requirements for a hygiene level of cybersecurity for digital consumer and professional products).

- IoT products operated in critical infra-structures are often very similar to the ones used in industrial organizations/corporations and maritime industries, but may have further challenges in the distribution processes due to their exposure and their being difficult to physically protect because they range over vast geographical areas.
 - Sabotage needs to be factored into risk analyses nowadays. Thus, physical and cybersecurity requirements are higher than in industrial and maritime settings. This requires a high physical security level in production environments, strict access management, clearer separation of environments, and hardening of networks and equipment/devices (including the IoT products). For distribution processes, monitoring and intrusion detection are usually required in terms for physical access and cybersecurity. Distribution processes and network function need to be monitored to ensure that they are functional (i.e., are available and operate as expected).
- If these processes fail, issues need to be swiftly identified to satisfactorily fix the issue.
- In critical infrastructure, the cybersecurity requirements for IoT products and their surroundings are higher or considerably higher than for industrial settings. The baseline level for cybersecurity must be appropriate and without weaknesses. The major issues for critical infrastructures are lack of staff with the right competences and security clearance combined with sometimes unclear local rules, which may cause cybersecurity issues in OT environments because of their extent and the need for continuous improvement. New AI-based threats are another pressing factor, as are inadequate budgets. A lesser problem are the suppliers' warranties, which often require that upgrades and patches are pre-approved by the supplier before they can be installed. This may result in a time window with open vulnerabilities. Due to the continuity of operations, a certain level of redundancy is needed, which further enables some updates to be installed in a controlled manner without disruptions (unless installed in planned downtime). In general, IoT products need to be upgraded or changed swiftly and easily.
 - Finally, a high level of knowledge concerning cybersecurity and what not to do is necessary. Users should know not to charge mobile phones in USB ports, not to use uncontrolled media (USB sticks), not to install unchecked software, not to click on unknown links or open attached files that have not been checked for viruses/malware, etc. Further, all new procurements or re-installations of an IoT product's basic settings shall require a mandatory change of device name, user accounts, passwords and network addresses and IP masks. Unless the IoT products can live up to these expectations, they will not be used in critical infrastructures, which are many and extensive.

10. Suggested reading

– frameworks/standards, references and explanation of technical terms

Below is suggested reading on: frameworks and standards, upcoming EU regulations and directives, and reference literature for those who require deeper knowledge and greater detail for various areas and contexts.

Frameworks and other relevant tests that might be of interest to understand how an IoT product may fit in into the larger context of cybersecurity:

- Consumer/domestic security
 - ETSI TS 103 645/TS 103 701 (www.etsi.org)
 - For connected building automation systems – see below
 - NIST Cybersecurity for IoT concerning Consumer IoT Products (<https://www.nist.gov/itl/applied-cyber-security/nist-cybersecurity-iot-program/consumer-iot-cybersecurity>)
- In general, and mainly for IT environments
 - CIS controls framework (<https://www.cisecurity.org/>)
 - ISO/IEC 27001/2/5/17/18/19/32 and more (www.iso.org)
- In general, for OT environments
 - Recommendations from the Swedish NCSC and Swedish Civil Defence and Resilience Agency pertaining to industrial control systems, cyber physical systems and IoT (a number of such publications are available at www.mcf.se)
 - Swedish Civil Defence and Resilience Agency – guidelines on cybersecurity for connected building automation, 2015. <https://www.mcf.se/sv/amnesomraden/beredskap-for-kris-och-krig/beredskap-for-aktorer/beredskap-for-kommuner-och-regioner/handbok-i-civilt-forsvar-och-krisberedskap-for-kommuner/kommunala-verksamheter/krisberedskap-for-fastigheter-och-byggnader/fastigheter-och-byggnader-risker-och-sarbarheter/>
- NIST standards (mainly aimed at public organizations in the USA but offers good practices also for others) – Cybersecurity Framework, SP 800-213, NISTIR 8228, NISTIR 8259, SP 800-30/53/73/82/171 and a number of publications in the 800 series (can be found at www.nist.gov and more at <https://www.nist.gov/itl/applied-cybersecurity/nist-cybersecurity-iot-program>)
- ENISA – EU's center for cybersecurity has many cloud and IoT-related cybersecurity publications available on its web site (www.enisa.europa.eu)
- ISO/IEC 27019 for information security for process control in energy production and distribution (can be found at <https://www.iso.org/standard/185056.html>)
- IEC 62443 (where parts 3–3/4-1/4-2 are probably of the most interest – <https://www.en-standard.eu/>)
- ISA95/98 with the automation pyramid as well as the Purdue model (<https://www.isa.org/>)
- Handbook on OT and its security (<https://ltu.diva-portal.org/smash/record.jsf?pid=diva2%3A2010974&dsid=-3695>)
- Maritime environments
 - IMO guidelines for maritime environments MSC-FAL.1/Circ.3 and Resolution MSC.428(98) –with comprehensive frameworks from, for instance, DNV (DNV-RU-SHIP Pt.6 Ch.5), Lloyd's Register (Cyber Safe for marine) and American Bureau

of Shipping (Cybersafety program). See also IACS E22/26/27 (<https://iacs.org.uk/resolutions/unified-requirements>) General IoT-security (and if the data resides in a cloud service)

- IoXt Alliance standard for IoT Security – <https://www.ioxtalliance.org/>
- ISO/IEC 27018 (protection of personal information in cloud services – www.iso.org)
- PCI-DSS (protection of financial information/credit card information <https://www.pcisecuritystandards.org/>)
- Municipalities, counties, and countries – IoT in various environments in Sweden
 - Robust & Säker IoT: Vägledning för Robust och Säker IoT vers. 2.0, Svenska Stadsnätsföreningen (SSNF), 2025, <https://stadsnatsforeningen.se/branschstod/robust-infrastruktur/> Stödmaterial till Klassa. There is a number of publications from Swedish Association of Local Authorities and Regions, and others, <https://klassa.skr.se/sidor/stodmaterial>
 - Klassa för IoT, Swedish Association of Local Authorities and Regions and RISE, 2020, <https://webbutik.skr.se/skr/tjanster/rapporterochskrifter/publikationer/klassafo-riot.65074.html>
 - Informationssäkerhet inom fastighetsom-rådet & IoT, Swedish Association of Local Authorities and Regions, 2022, <https://webbutik.skr.se/skr/tjanster/rapporterochskrifter/publikationer/informationssakerhetinomfastighetsomradetiot.65014.html>
 - NIS2 Directive, <https://digital-strategy.ec.europa.eu/en/policies/nis2-directive>
- Health care
 - MDCG 2019-16 - Guidance on Cybersecurity for medical devices
 - IEC 81001-5-1 - Health software and health IT systems safety, effectiveness and security — Part 5-1: Security — Activities in the product life cycle

- Car/vehicle safety
 - ISO 21434 (www.iso.org)

Regulations and directives at EU level:

- EU Cybersecurity Act, <https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act>
- EU Cyber Resilience Act, <https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act>
- EU Radio Equipment Directive (RED), https://single-market-economy.ec.europa.eu/sectors/electrical-and-electronic-engineering-industries-eei/radio-equipment-directive-red_en
- EU AI Act, <https://www.digg.se/kunskap-och-stod/eu-rattsakter/ai-forordningen>
- EU Data Act, <https://www.digg.se/kunskap-och-stod/eu-rattsakter/oppna-datadirektivet>
- EU Ecodesign Regulation, <https://eur-lex.europa.eu/EN/legal-content/summary/ecodesign-requirements-for-sustainable-products.html>

Reference literature:

- Securing IoT and Big Data Next Generation Intelligence, 1st Ed., Edited by Vijayalakshmi Saravanan, Alagan Anpalagan, T. Poongodi, Firoz Khan, ISBN 9780367432881, CRC Press, USA, 2021
- IoT Security and Privacy Paradigm, 1st Ed., Edited by Souvik Pal, Vicente García Díaz, Dac-Nhuong Le, ISBN9780429289057, CRC Press, USA, 2020
- IoT Automation: Arrowhead Framework, Edited by Jerker Delsing, CRC Press, Boca Raton, USA, 2017
- Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and other Industrial Control Systems, 2nd Ed., Eric D. Knapp, Joel Thomas Langill, Syngress/Elsevier, MA, USA, 2014

Explanation of technical terms:

- **IT** – information technology, used more or less everywhere and often in homes and offices for administration purposes.
- **OT** – operational technology, used in production and distribution environments in industry and critical infrastructures. Sometimes, OT equipment is similar to the equipment used in IT environments

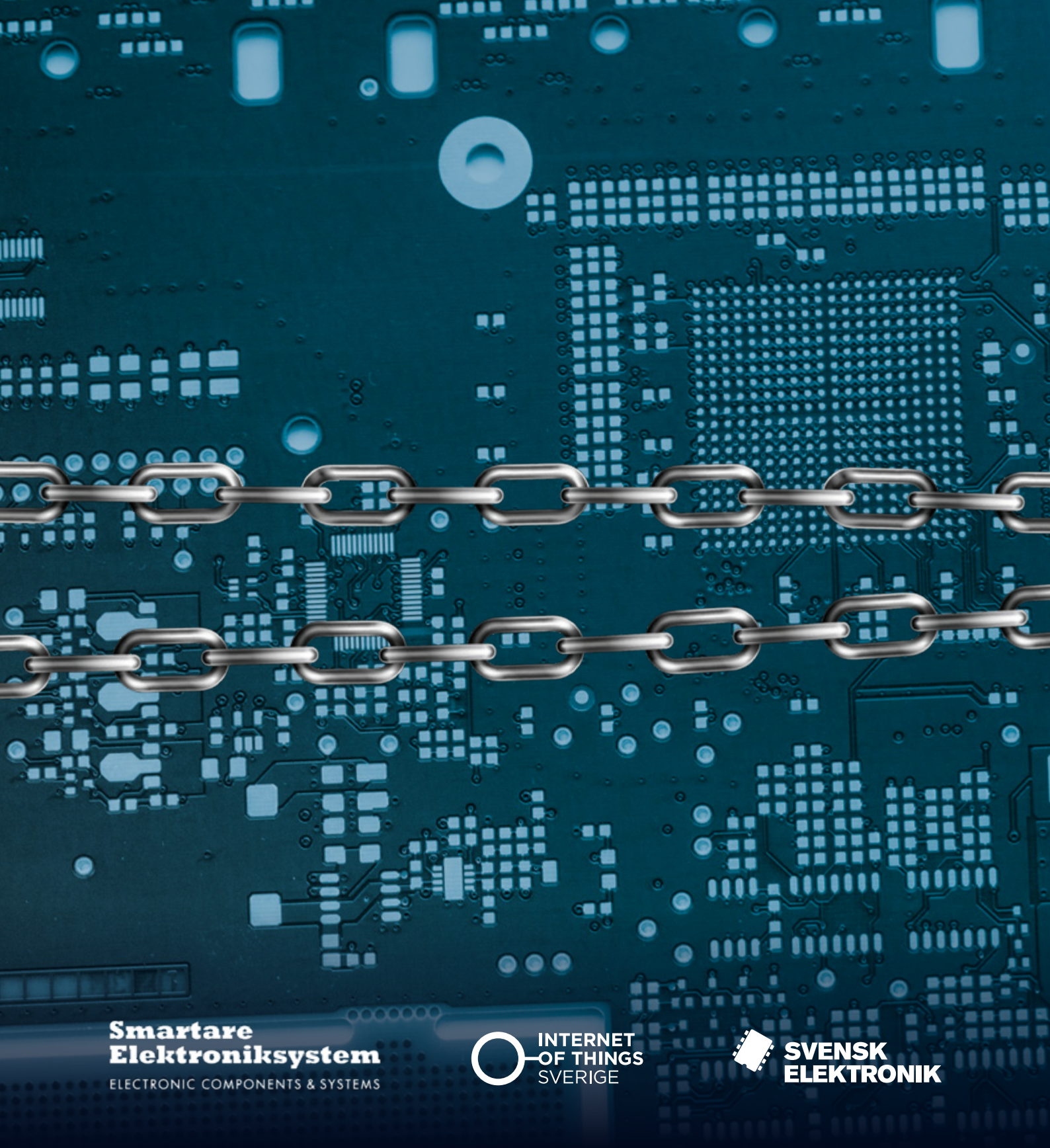
In the future, much IT and OT will likely converge from a technology standpoint although their functionality differs. In OT there may be requirements for speed, i.e., real time, as well as availability-level mixed with other requirements that are not time- critical.

- **MT** – medical technology, used in health care, is similar to OT but often has even higher requirements pertaining to time- criticality, performance and availability.
- **Fleet management** – if many IoT products are installed and running at different customer sites, these are often called a fleet. A fleet management system, or functions, can be used to track, monitor, remotely maintain or support a fleet of IoT products from a distance. Such a system or functions improves efficiency and accelerates the time before necessary actions are taken. An alternative, if remote maintenance or support is not possible, is to ask the customer's users/ operations to lower their load/speed or stop operations before a breakdown occur if there are signs of serious problems.





THERE ARE MANY FRAMEWORKS AND STANDARDS, AS WELL AS NEW LAWS AND REGULATIONS, TO KEEP TRACK OF REGARDING CYBERSECURITY AND IOT PRODUCTS.
PHOTO: ADOBE STOCK



**Smartare
Elektroniksystem**
ELECTRONIC COMPONENTS & SYSTEMS

 **INTERNET
OF THINGS
SVERIGE**

 **SVENSK
ELEKTRONIK**

With support from:

VINNOVA
Sweden's Innovation Agency



Swedish Energy Agency

FORMAS 

svenskelektronik.se

ISBN: 978-91-989591-9-2

PRICE: SEK 374 EXCL. VAT