Smartare Elektroniksystem
ELECTRONIC COMPONENTS & SYSTEMS
INTERNET OF THINGS SVERIGE
SVENSK ELEKTRONIK

Handbook for Development of Cybersecure IoT Products

Revision management
This is the first version of the handbook (published 2023) and it 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 companies 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

T2Data AB

Uppsala universitet

Weop AB

Xertified AB

Copyright and other rights

Disclaimer

This handbook is authored based on the working group’s collective knowledge and experience gained from many years within the business. Although the working group has iteratively scrutinized the handbook’s contents, the working group cannot guarantee that there are no errors. The expectation is that the contents of the handbook will be useful, however the working group does not take any responsibility for errors or damage which may arise within the areas or other content that this handbook addresses.

Editing: Maria Bergenheim, IoT Sweden

Design: Oh My

ISBN: 978-91-985741-5-9

Foreword

Smarter Electronic Systems is a strategic innovation program within the frame of Vinnova's, Formas' and The Swedish Energy Agency's joint venture regarding strategic innovation areas. The program's objective is to support Swedish industry concerning world class sustainable development and competitiveness. During the crafting of the program agenda three main challenges were highlighted as the most important in order to achieve the requirements of the future. These three were: leading edge competencies, supply and management of competencies, and efficient value-chains. For each challenge, a council was appointed. In the scope for the council regarding efficient value-chains, the work on handbooks were initiated. 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*, has been written in cooperation between Smarter Electronic Systems and Internet of Things Sweden (IoT Sweden).

The different value-chains involved in the development of IoT Products are complex. There are many actors involved and they contribute in various ways to cybersecure IoT Products put into the market. Synergy between object owners, users, and customers is important. In addition, close cooperation within development, manufacturing, test, maintenance/service and support is also required. This is necessary 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 in between object owners and users at customers, development, research, manufacturing and maintenance/service, has been acknowledged as decisive for how successful the IoT product will become over its whole life-cycle. Efficient collaboration and cooperation results in lower manufacturing and maintenance costs over the life-cycle, faster time-to-market, higher quality and cybersecurity-levels.

The Handbook for Development of Cybersecure IoT Products has been crafted by a working group of representatives from companies and organizations providing contributions over a broad range of knowledge and experience. It targets managers involved in product design, development, maintenance, and other areas having an influence on product specifications. The handbook, in combination with the *"Smartare Elektronikhandboken 2.0"* (The Smarter Electronic Handbook 2.0), enables effective knowledge transfer between participants cooperating to develop IoT Products which are cybersecure over their entire life-cycle.

This is the first version of the handbook and 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 also 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.smartareelektroniksystem.se and
www.svenskelektronik.se

With Best Regards,
The working group behind the *Handbook for Development of Cybersecure IoT Products*

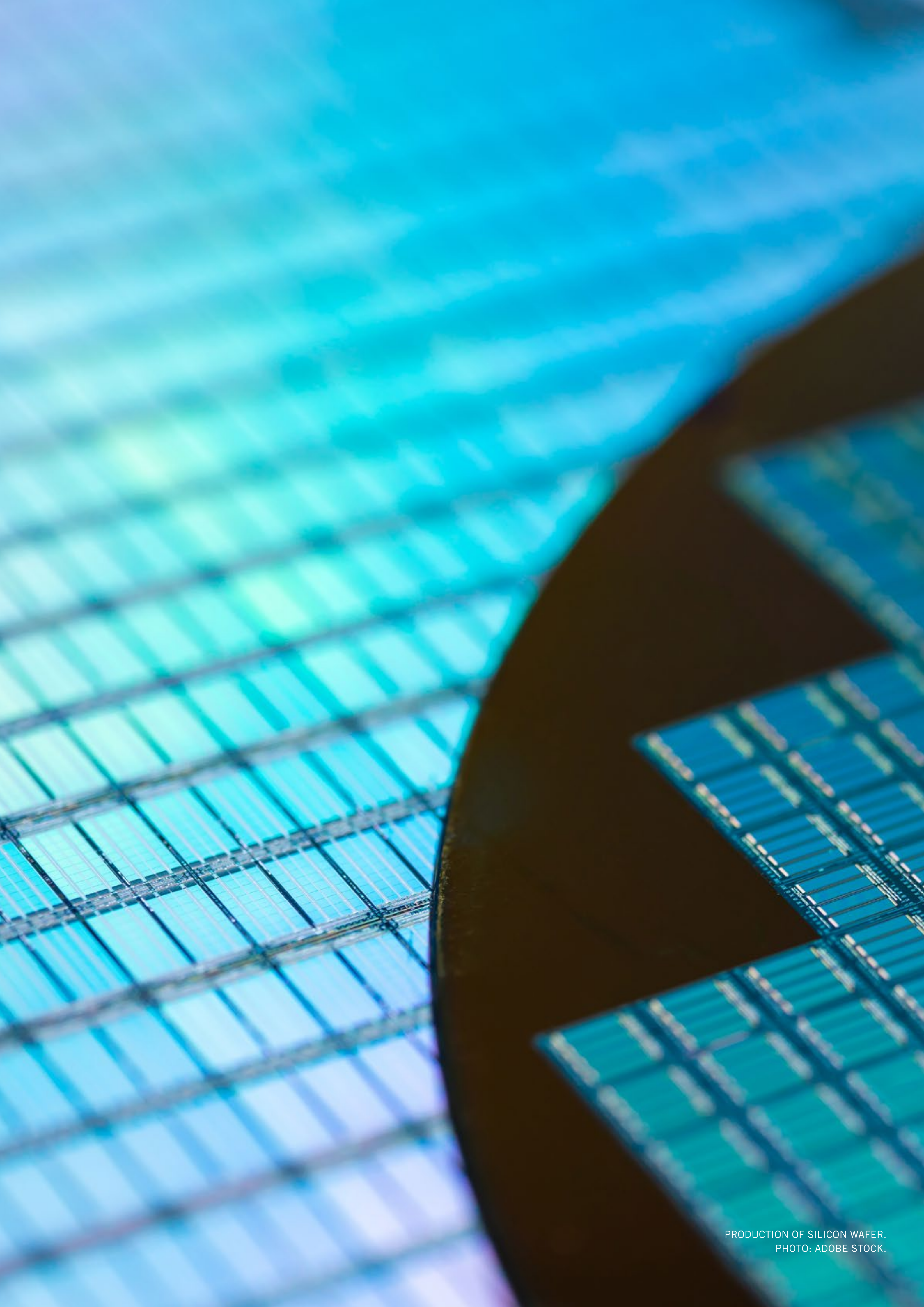
Summary

The *Handbook for Development of Cybersecure IoT Products* aims to support both primary and secondary stakeholders as the handbook spans the whole life-cycle and thus naturally involves the stakeholders and actors involved or part of the vale-chain from start to finish. To consider the whole life-cycle demands that requirement gathering/engineering and the design have a wide and deep set of knowledge about how users at customers will use the IoT product as well as about technology from the 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 posed by product manager and users. In addition, it is necessary to understand how data and information generated within 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 requires that extraction of data and information from the IoT product is enabled and that updating, upgrading, re-configuring and optimizing can be made both locally and remotely. To do this, deep knowledge about the contexts where the IoT products are to be used needs to be combined with the understanding of how cybersecurity and IT- and OT-infrastructures allow data to be sent out and in as well as how potential remote connections can be made from the outside. Thus, the management of suppliers and other stakeholders in an IoT products value-chain may need to find out and clear any obstacles to facilitate the above so that the IoT product can create and deliver a good value for all involved.

If IoT products create cybersecurity problems, or risks in the contexts where they are used, they will probably not be used for long regardless of how good they are. Further, if it also is not possible to raise a protection around them (as well as the IPR and data/information generated and stored) the expected life-cycle will be shorter. Simultaneously, to require that protection is raised around, due to non-adequate inherent protection and cybersecurity, will result in higher cost and complexity for users. To raise an extra protection around will likely also increase the complexity to send and receive data and how remote connections can be made. Thus, there are a lot of things and requirements to consider and also necessary is an understanding for the whole life-cycle together with object owner's IT- and OT environments. To note is that there is a large difference between IoT products aimed for domestic (home) use compared to use in professional contexts and critical infrastructures. IoT products aimed for domestic use, which often are cheaper than those for use in professional contexts or critical infrastructures, still need to have an adequate level of cybersecurity to not cause unnecessary risks. An additional difference is that in domestic contexts the expected knowledge level is lower in terms of being able to accomplish cybersecure installations and configurations.

The handbook encompasses the processes related to the development of the IoT product, focusing on hardware and embedded software. What is not addressed are the need for cybersecurity-related structures and processes, at manufactures and other stakeholders or actors within the value-chain, who help to manage the IoT product throughout its life-cycle. 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 the operations, availability or stored data and information. The more critical applications and high availability requirements, which are posed by object owners and customers, the more robust and resilient these structures and processes must be to withstand cyberattacks and operational problems.



PRODUCTION OF SILICON WAFER.
PHOTO: ADOBE STOCK.

Contents

1. Introduction

The idea for this handbook starting as the publication *"Smartare Elektronikhandboken 2.0"* was crafted as the surrounding world experienced an increased threat against IoT products. The two handbooks shall be seen as complimentary and thus it is a good idea to read them both prior to starting up new development projects concerning IoT products. IoT is an abbreviation for Internet of Things, and we will use the abbreviation IoT throughout this handbook.

The following definition of "IoT product" will be used in the handbook: in general, as IoT products we refer to intelligent and connected units who communicate and transmit data over Internet. These units are equipped with processors, sensors and software in a way that they can perceive their surroundings, communicate with it, and thus create a behavior adapted to various situations in order to be able to contribute and create attractive and helpful surroundings/environments, products and services[1].

Regarding the need for this handbook, we need increasingly cybersecure IoT products due to expanding malicious activity among hobby hackers, professional hackers as well as state-supported intelligence organizations whose purpose are to steal information, make money or disrupt operations/processes, for instance at critical infrastructures, municipalities or counties, within target countries. This fact can no longer be dismissed, and we must all adapt ourselves and our IoT products to these circumstances. Below are some scenarios for different contexts where IoT products may be used and what can be the consequences unless the IoT products are cybersecured:

Domestic (homes) – a cyberattack can cause for instance connected fridges, stoves, heating systems, TVs and home computers to stop working or get locked. In tenant buildings, common systems, such as, building automation (control systems for water/sewage, heating, electricity, ventilation, locks, etc.) can be affected and in worst case stop functioning. Further, cars and garden equipment are nowadays also often connected and need to be cybersecure in order to not cause physical damages or fires due to malicious overloading of components or systems.

At work in office spaces – besides that office computers, various IT-systems and networks can become non-functioning, also elevators, lock/alarm systems and building automation control can become affected partly or fully. The conference room equipment can be tampered with and conversations recorded or tapped using the microphones in computers, mobile phones or conference equipment.

At work in production/distribution environments – the IT environment (used by offices and administrative processes) is often connected to the OT[2] environment (used by production and distribution processes) and these often collaborate in a manner where what should be done is decided and administrated in the IT environment and subsequently sent to the OT environment where the ordered production/distribution is executed. An OT environment, which commonly comprises a lot of IoT products, may, like an IT environment, be affected by different types of cyberattacks affecting the operation's availability and integrity, quality of output, or completely stop/disrupt the operations. Unfortunately, the OT environment can negatively be affected in case the IT environment is under cyberattack as no new order data is transmitted and no feedback of production/distribution data are received back. Thus, the production can in worst case be stopped when the buffered order data has been executed/produced and there is no new data to

[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

continue with. There are examples of cyberattacks seriously affecting, destroying, or wiping all data within production equipment. Further, some production/distribution environments can get serious problems in case of longer unplanned stops due to material becoming stuck or stale inside of piping or other equipment, which then needs to be fixed or replaced. Examples of such material are pre-stages of pulp and paper, plastics or food. In addition, there are environments, similar to OT environments, within health care but are not there referred to OT but MT[3]. Further on 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 infrastructures[4] (production/distribution of energy, water production/wastewater management, tele communications, roads/railways/bridges/ports/airports, food production/distribution, etc.) – in a similar way to the above production/distribution environments it is necessary to have collaboration between IT and OT environments. The difference here is that a stop 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, although there is no functioning IT environment present, by using reserve routines (and historic data). For instance, if energy production/distribution is disrupted for more than 2-3 days, this will have a large impact as

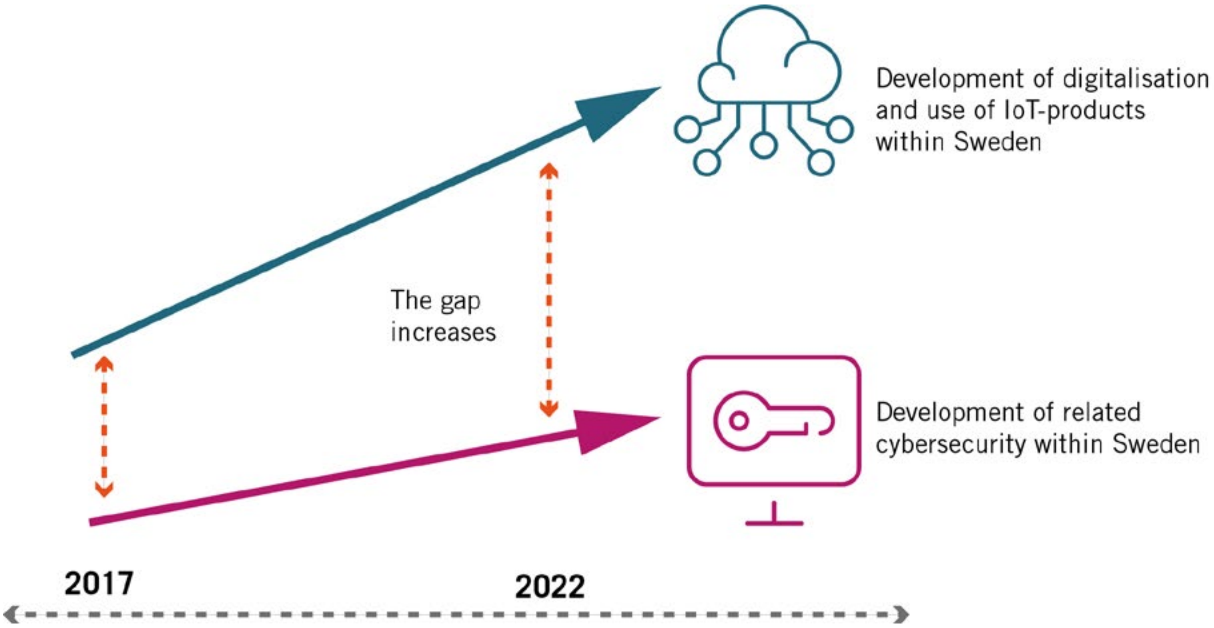

Development of digitalisation and use of IoT-products within Sweden
The gap increases
Development of related cybersecurity within Sweden
2017
2022

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

[3] MT – Medical Technology

[4] The Swedish Civil Contingencies 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/

the lack of electricity and electronic communications will affect almost everything in the long run. Further, some of these OT environments are very sensitive and thus not connected to the IT environment (or Internet) and use own networks or public ones with high grade security measures employed.

Unfortunately, there is an increasing need to cybersecure IoT products to keep all functioning over time within domestic-, professional- and critical infrastructure scenarios and contexts. Figure 1 outlines that the increasing pace of digitalization, combined with increased use of IoT products, outruns the development of related cybersecurity. Thus, the gap continues to grow bigger. However, the handbook will bring up a number of positive factors which can close the gap over time.

For many years, Smarter Electronic Systems has together with a number of actors created and issued advice to the electronics industry regarding how electronics can be developed and manufactured by multiple actors working together in value-chains. The latest piece of advice is available as the *Smartare Elektronikhandboken 2.0*, which focuses on the interface between development and manufacturing for to reach efficient collaboration within the value-chain. The objective is better products with higher quality-level, lower manufacturing costs and faster time-to-market. Currently, we see a need to expand the advice with a *Handbook for Development of Cybersecure IoT Products*, 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 surrounding context1. Through this handbook, which complements the contents of the *Smartare Elektronikhandboken 2.0*, the whole IoT industry will be able to improve the level of cybersecurity in its products already from the very start. Further, the cybersecurity-level shall be possible to continuously be improved and augmented throughout the whole life-cycle. This requires a good and well-considered initial design and planning for further development and maintenance process so that updates, upgrades, and improvements can be issued and deployed over time. As the cybersecurity-level is improved also the quality of IoT products will get improved due to new requirements and increased testing.

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

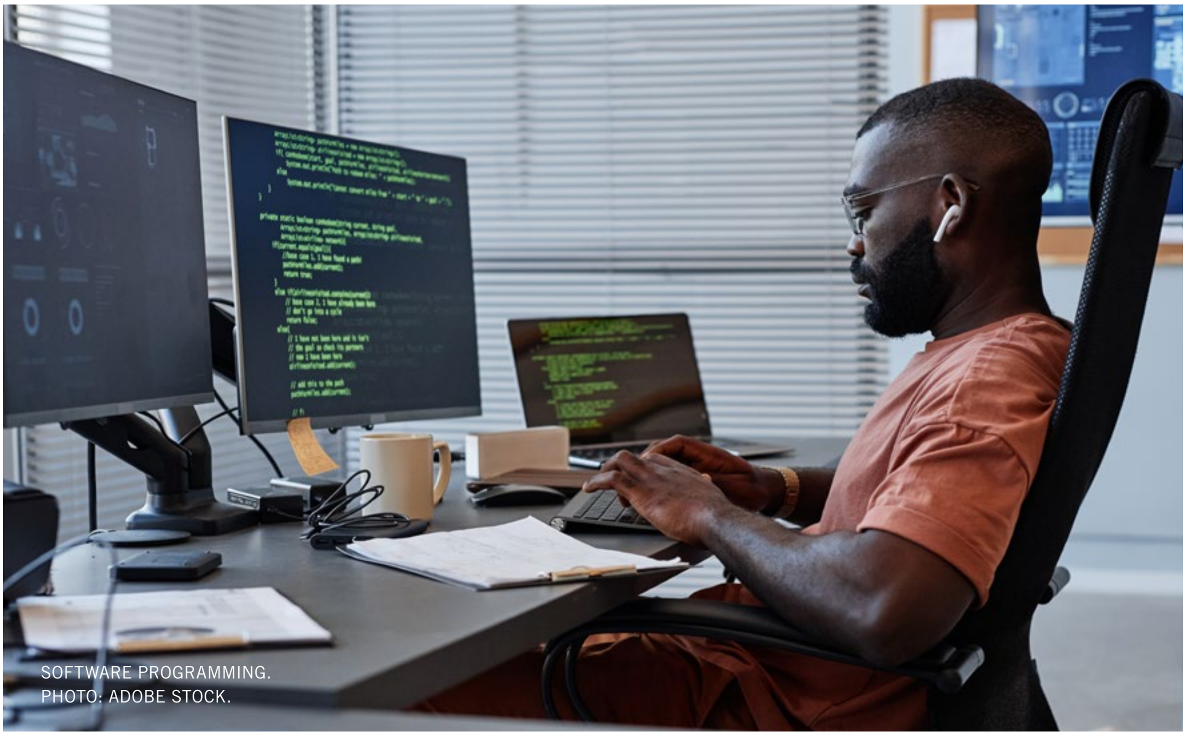
- Designers and developers (hardware and software), project leaders, testers, documenters and consultants
- Buyers
- Product owners
- Produkt managers
- Object owners

The secondary stakeholders for the handbook are:

- Manufacturers
- Installers
- Crews doing maintenance, service and support as well as services for optimizations
- Recyclers
- Authorities – who themselves are users and potentially also have a regulatory review/inspection responsibility

Collaboration and communication in between groups of stakeholders are essential for IoT products to be developed as well as cybersecure. All participants involved need to understand that in addition to cybersecurity concerns, if any requirements that affect the management of IoT product life-cycles are missing or deficient then the long term effects will be: higher costs, hard problems related to cybersecurity, and unnecessary friction between object owners at customers and suppliers. As it is of interest for all involved stakeholder groups that this should not be the case, they all need to collaborate regarding the set of requirements to enable a rational life-cycle

MANUFACTURING OF ELECTRONIC EQUIPMENT.
PHOTO: ADOBE STOCK.



SOFTWARE PROGRAMMING.
PHOTO: ADOBE STOCK.

management for each involved stakeholder and any additional parties involved as well. Some of the stakeholders need to understand which laws and regulations that apply as well as which industry standards and best practices that are suitable (or required) to use. The groups of secondary stakeholders need to be involved rather early as well. These need to be informed and trained in order for them to be able to, during their part of the life-cycle, be able to manage IoT products adequately 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 will be:

- The handbook will address the whole life-cycle of IoT products and cybersecurity requirements for development of a new IoT product to enable the life-cycle to be long with high availability.
- To provide advice/check lists/standards/methods/best practices which can be used by hardware and software designers and developers (as well as their managers) who are not experts on cybersecurity. The emphasis will be on the T in the IoT products.
- The scope will extend to a moderate level of practical and structural advice concerning cybersecurity for development of IoT products. The advice shall be easy to read and digest.
- IoT products vary regarding extent and other limits, from locally connected with limited local functionality to globally connected transmitting data to cloud services, where the data is used for optimization of the IoT product's function as well as the process it is part of. The handbook will address this as well as how continuous maintenance of hardware, local software, and configurations/settings can be made in a rational and cybersecure manner.

Chapter 10 comprises explanations to technical terms and abbreviations used concerning IoT products.

1.1 Stakeholders

There are many stakeholders participating within the value-chains wherein IoT products are developed and later used in. Below, a number of the stakeholders, who can have significant impact on the set of development and operational requirements used for the design of IoT products, are outlined. The focus is on the stakeholders (or other actors) who participate from the very start until the IoT product's life-cycle ends and is decommissioned and recycled. 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 leaders, testers, documenters and consultants

As the development of an IoT product has progressed so far that a set of requirements has materialized, a suitable group of people is needed to develop the IoT product. 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 that there is enough competence to further develop and assess if the potential open-source code or open design is safe, cybersecure and applicable for actual use. The stakeholder groups and sub-groups are briefly outlined below:

Designers and developers of hardware and software – design and development of hardware and code, as well as using hardware and code developed by others, ensure that the right functionality (based on the requirement specification) is realized in a way that it all is cybersecure. This is not easy to accomplish and requires continuous training and intelligence gathering related to cyberattack progression and cybersecurity in general. Failing to do this can result in IoT products that may become dangerous or non-acceptable among customers as this is revealed. In cases where open design or open-source code is used, this commonly entails that the development team needs to review this manually and using tools to verify that nothing unwelcome has been planted. This needs to be verified at each new version, and may be a large undertaking if a lot of open design or open-source code are used. Further, hardware components, various chips or semiconductors, and ready-to-use circuit boards which are 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 the development/manufacturing is outside of EU/USA and made in low salary countries or non-democratic countries). Thus, designers and developers need to improve their testing and verification skills, both for what they do themselves but also for external hardware or software, add additional cybersecurity test cases, as well as try to automate as much as possible. Automation enables fast testing, coverage, and repeatability. Thus, automation of development testing and increased usage of test suites and/or test rigs simplifies testing/verification of own development as well as development made by externals.

Developers of services, processes, and other necessary supporting structures – the extent of an IoT product may vary from just a product with warranty up through 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, the development of services and processes differs somewhat from the development of hardware and software, and thus other competences may be needed along with an understanding of the whole life-cycle, value-chain, and how these need to be improved within the years to come. As a basis for services and processes within the supporting structures, a mix of existing tools and services can be used together with ones locally developed. Some examples of services and processes, which can be conducted on-site or remotely, are: support, service, maintenance, training/education (for own staff, customers or others in the value-chain), fleet management functionality with monitoring and additional value creation and efficient functions or services (see chapter 7 for more on this). A good and supportive self-help for problem solving, having an FAQ, instructions, videos, virtual/augmented reality, which can be consumed via the web or an app could be valuable in order to save time for both developers and users.

Project leaders – a project leader is commonly assigned to have responsibility for the development of an IoT product based on a requirement specification and the expected outcome should have a certain level of cybersecurity and quality. To do this, a set of resources are assigned together with a deadline. To support the project leader, there are roles such as product managers and other relevant parts of the value-chain.

Testers – testers are needed not only for the crafting of test cases pertaining to the basic functionality, which naturally shall be tested (preferably) as a combination of automatized test and manual tests, requiring the knowledge and ability to craft test cases also for advanced cybersecurity. The testers should conduct various forms of penetration tests, tests of availability/performance and which information that can be extracted/exfiltrated by different measures such as faulty logins. The hackers, who can attack an IoT product, use a plethora of tools, ranging from very simplistic to very advanced, which the tester must be aware of. Potentially, a shielded lab may be needed for such testing using hacking tools. Doing this provides a good understanding of reality and for how test cases should be designed as well as how common cyberattacks are designed, planned and executed.

Documenters – also documenters need to be able to understand recent and relevant cybersecurity for IoT products. Unless cybersecurity is not integrated into the description of the basic functionality, an option is to add an extra chapter or appendix to the manuals to outline how the architecture is set up and how to apply cybersecurity within and around the IoT product (if it normally is connected where many other things and systems operate). It can be a good idea to describe which is the inherent cybersecurity functionality, how to install/commission and configure it adequately, how to update/upgrade as well as how to verify that the cybersecurity functionality is correctly configured and working. For the last mentioned, specific procedures or scripts may need to be developed and described.

Consultants – consultants are often added to development teams to strengthen the team within design, development of hardware or software, testing, documentation or project management, etc. Commonly, consultants split their time between different customers (and development teams), who can be suppliers of IoT products or similar and be competitors, which requires that some things need to be addressed. The protection of intellectual property rights, patent ideas, and patterns/copy right (i.e., IPR) must be performed such that the cybersecurity-level is not negatively affected if consultants are team members or part of maintenance later on. Thus, secrecy and confidentiality agreements need to be set up and how to implement cybersecurity and instructions/awareness related to that. To consider is also if consultants should be on premise together with the rest of the team or can work remotely. In any consultancy agreement there should be requirements that consultants have a good knowledge regarding cybersecurity and when developing IoT products.

Others – development teams may comprise many different roles and categories of staff, ranging from CEO, CTO, development managers, program management, project management to sales representatives who can bring in requirements from customers to cleaners and janitors who moves around in the development team's proximity.

CIRCULARITY IS IMPORTANT WHEN DESIGNING IOT.
PHOTO: ADOBE STOCK.

For all these, cyber security and protection of IPR and secrecy must also be set up properly alike for any consultants involved.

1.1.1.2 Buyers

Initially, it is never easy to foresee the actual use of an IoT product although a certain use is expected and prescribed. The possibilities to solve new problems, and also old ones, which were not part of the framing of the initial thought process will always appear and spur the continuous development of an IoT product. To listen to and talk to customers and users on a regular basis is always a good idea in order to keep updated on the needs, how the IoT product is used, what can be improved and what might be missing. With respect to buyers, there may be a number of part stakeholders involved who are not up-to-date and understand how an IoT product should be used as well as what requirements are posed from the surrounding context. In such cases it may be a good idea to offer help and actively ask questions which reveal answers to what is needed concerning the IoT product and its future usage. Potential part stakeholders at a buyer may be:

Procurement – procurers do not always have the necessary special knowledge required and follow a simple or limited procurement process. In this context, support may be needed to ensure that also cybersecurity is part of the set of requirements from the very start as it is usually hard and expensive to add these later on. Unfortunately, to add cybersecurity requirements later will not render as good of a result as if these were part already from the start. A potential development of procurement processes is to from the very start ensure that all competencies needed within IT, OT and cybersecurity are part of the process (in order to avoid the mentioned later difficult problems to solve as well as high costs for that).

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 can be part of monitoring such functions/processes to ensure that all work and quality is above the expected level. Examples of such are controls for a function/process and regarding monitoring sensors and cameras may be used.

Technology-/development department – customers often have a department managing technology/development matters, who can build up production- and distribution lines adapting technology for these. The ones working in such departments often have a good knowledge for both functions/processes and technology, which makes them an important part stakeholder to discuss and interview.

Operations and maintenance/service – those who work in operations and maintenance/service are the ones who are in contact most with the IoT products. The operations/usage phase is also the longest phase of the life-cycle for an IoT product. Thus, among these workers there is a good understanding for how an IoT product can be efficiently installed, commissioned, configured, updated/upgraded, changed, decommissioned and in general maintained. This should be made easy to execute efficiently, for instance by having a set of well-working fleet management functions, to lower the life-cycle cost of an IoT product. A low life-cycle cost makes an IoT product interesting compared to competing IoT products and, in particular, if these miss fleet management functions.

Thus, it may be a prosperous idea to talk to various part stakeholders at buyers as they all may have small pieces of information to the complete the bigger picture. These are also a good source for ideas how to lower the total life-cycle cost for customers.

1.1.1.3 Product owners

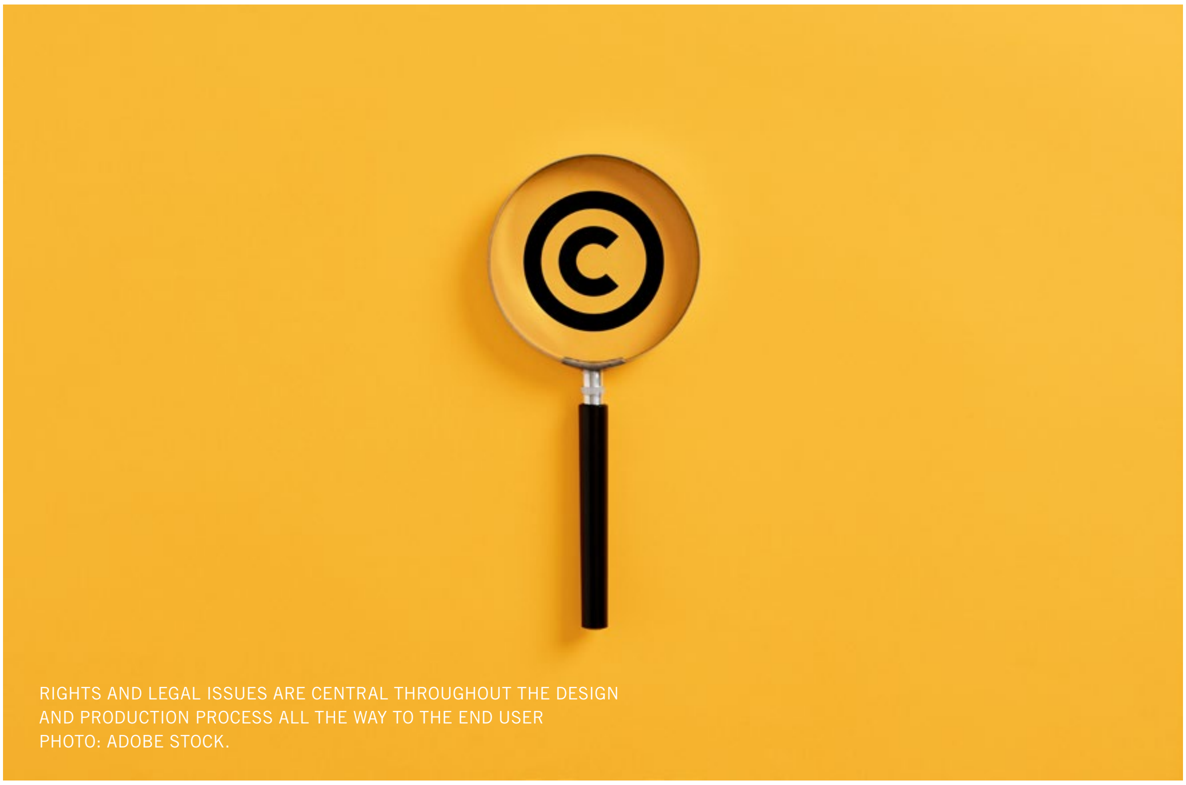
The product owner, i.e., the company which owns the IoT product and puts it on the market, has responsibility for, e.g., that the CE mark is fulfilled and that all legal/regulatory requirements are met.

1.1.1.4 Product manager

On the supplier side of an IoT product, it is a good idea to have a role who is responsible for the product's requirement engineering (and perhaps also for similar products in a family) throughout their life-cycles and thus is the prolonged arm of the product owner. Having a clear responsibility and authorization to manage the IoT product makes it a lot easier to, already from the start, get the right requirements into development and then later add new requirements until the end of the life-cycle. Commonly, a product manager manages the requirement engineering and continuous requirement collection as well as strategic planning of the development (e.g., in the form of a roadmap) as well as acts as the glue between customers, development, sales representatives and other stakeholders. Further, it is usual that the requirement specification is managed and compiled by a product manager.

1.1.1.5 Object owner

At the buyer side there may be object owners, who are responsible for IoT products or have budget responsibility to maintain them as well as other assets residing in production- or distribution environments. The object owners have after installation and commissioning the responsibility to maintain and keep the IoT products up-to-date until they are decommissioned and end-of-lived or are transferred to another object owner. These object owners often work closely with function-/process owners, who have larger responsibility, to ensure that what is to be accomplished is executed with right quality, availability and on time. Object owners may not always consider cybersecurity, but they are increasingly forced



RIGHTS AND LEGAL ISSUES ARE CENTRAL THROUGHOUT THE DESIGN AND PRODUCTION PROCESS ALL THE WAY TO THE END USER
PHOTO: ADOBE STOCK.

to do that due to necessary planning for access from within, external/remote access, redundancy, backup/restore, and logging, etc.

1.1.2 Secondary stakeholders

No chain is stronger than its weakest link. If there are many secondary stakeholders involved within the value-chains, these will need both physical security and cybersecurity. This should be part of the value-chain agreements and the implementations reviewed on a regular basis as otherwise these can contribute to an increasing risk exposure. Below, there are a number of potential secondary stakeholders described, whereof some are integrated into the supplier (developing the IoT product) in case the supplier has integrated the whole vertical and horizontal value-chain to the customer. However, it is common that there are a number of external parties acting as secondary stakeholders.

1.1.2.1 Manufacturers

If having the manufacturing internally and in own factories, it is easier to keep an adequate level of cybersecurity around and within the production environment as well as protect the information necessary to produce the whole, or parts of, IoT product. An IoT product may be very simplistic or have an advanced architecture. Further, the borderline between when it is an IoT product and a cyber-physical system is a bit unclear. Anyways, the production environment must be protected to enable that all in it is kept confidential, it is not possible to make unauthorized changes in the manufacturing process or process parameters, and that the processes run without disruptions and stops as such can negatively affect the output quality as well as lowering the output volume. Further, physical security within and at the perimeters of production facilities and factories need also to be adequate to prevent burglars, theft, as well as sabotage of electric supply, ventilation systems or water pipelines.

If using outsourced manufacturing, these production facilities and factories need to have the same levels of physical security and cybersecurity as any own factories. There is a difference if standard components are outsourced compared to if there is IPR, such as hardware designs, software or knowledge about the production process, which must be protected and kept confidential. Thus, sometimes it is not applicable to outsource outside of trusted production facilities and factories or to countries outside the EU/USA, where political pressure or involvement may endanger confidentiality of IPR.

Thus, an assessment of physical security and cybersecurity is recommended at least annually in order to ensure that the outsourcing is executed in a desired manner and that the physical security and cybersecurity-levels are adequate. The 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

Post manufacturing, an IoT product can be stored and distributed fully or partly by own means, or by using an external distributor or distribution solution. Regarding simplistic IoT products, this is not that complicated whereas for IoT products, which may also carry spare parts/components or software and manuals requiring regular updates, it can be a good idea to consider this in order to be able to keep all this physically protected and ensure that no unauthorized persons can access the IoT products, spare parts/components, software or manuals. If adding a virus or malware to software updates or manuals (if these are executable or readable files), it can cause significant problems for object owners at customers and the supplier (no matter if the distribution is manual via service/support staff or are downloaded from a portal or cloud service). Concerning the distribution of hardware, software, and manuals, etc., the processes are required to check/verify that no unwelcome or extra unauthorized are added.

Further, IoT products can have services possible to add, such as maintenance, service, support and optimizations. Some of these services are executed on premise and some remotely using data which may be transmitted to a cloud service. If these services engage own staff, external distributors/executers, and if any cloud services used are hosted at an external cloud service provider, it is required here to apply the requirements for physical security and cybersecurity. See more on this further below.

1.1.2.3 Installers

If the customer or supplier do not conduct the installation and commissioning, it is common to use external installers. Alike any distributors, these need to have adequate physical security and cybersecurity in case they have a supply in stock and use this to install as well as keep any needed software in an own portal or cloud service. Installers need continuous education and training on the IoT product and its installation, configuration and commissioning, as well as build and maintain a general awareness about cybersecurity (which includes both physical- and cybersecurity). If the IoT products will be installed in sensitive operations or processes, which require very high availability, the installers must see to that no one else can assess the IoT products or its various components. Further, installers need to know what to do when they decommission and replaces old IoT products with new ones or other solutions. Then any potential sensitive data, configurations, control data, etc., must be wiped or removed so that no one else can figure out what the IoT product has been used for or provide data about the old operation environment (i.e., networks, IP-addresses, connections). Some IoT products may need to be destroyed/destructed completely if it is not possible to verify that all sensitive data and configurations are completely wiped or removed. A product manager or object owner should preferably interview the installers about potential improvements of installation, configuration and (de)commissioning.

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

Common value-adding add-on services for IoT products, within value-chains, are to provide support, service, maintenance and optimization of hardware or software as well as the processes where IoT products contribute. Further, add-on services, such as, re-engineering of processes and integrations with other solutions are common. Among the part stakeholders participating within this scope, here can often valuable ideas be found for improvements of IoT products as these are the ones who manages the IoT products during the longest phase of the life-cycle and can clearly see any flaws and potential improvement areas in combination with the possibility to compare with the competitors' IoT products and solutions. At the time of service and support, when some IoT products may get replaced, it is important to ensure that sensitive or IPR-related data or information is wiped or erased. This situation is very similar to the one for installers. A product manager or object owner can have a great exchange of ideas and learn about flaws and potential improvement opportunities regarding how IoT products behave while in operation.

Add-on services can be provided on-site or partly from distance (using remote access and tools). If on-site, it must be ensured that no viruses or malware are brought in, and the providers need to together with the customer's users agree on how to keep the processes cybersecure. In many instances, external lap-tops, USB-sticks/disks or mobile phones are not allowed to bring in any files or other items from the outside and other secure procedures are needed. The staff at customers need also to monitor that the service providers only do what they are allowed to do and not collect data or information from the competitors' equipment and solutions surrounding or about processes and process parameters they should not have access to. It is a trend to increasingly do more from distance (i.e., remotely) through using external connections, such as low- or high-level VPN, which save time and costs as the distances to travel may be long at the same time as the time to provide the service relatively short. Thus, customers need to maintain strong control of whom are allowed to get access from distance and have a standardized way to provide such access. Such a standard may encompass time limitations, access only during normal business hours, and removal of inactive user accounts. At acute problems, there can be a fast activation process for external connections with a short life span. Further, it is common that suppliers collect data in a central cloud service in order to be able to help part stakeholders at customers with analyses of processes' outcomes or the processes' operational details, optimization of processes and process parameters, to find signs of wear and tear as well as maintenance needs or replacement of equipment. In addition, maintenance, updates or upgrades of software, and re-configurations are often carried out this way too. Some customers want to have their own local servers in own data centres (on-premises) 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, which all should be part of the agreement set up. In the future, ownership of and access to data will become increasingly important and central to data-driven business models. Thus, the locations where the data and information are stored must have adequate physical security and cybersecurity. This goes for whether storage is local, within a cloud service or at the suppliers' servers.

CLOUD TECHNOLOGIES AND SERVER DATA PROCESSING
PHOTO: ADOBE STOCK.

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 as well as marked on any initial packaging. As IoT products are to be recycled, they firstly need to be wiped or emptied of any data and information and some parts even destructed or destroyed physically. This is due to that there are different types of memories and disks that can be hard to wipe/erase completely. Further, no IPR of high sensitivity or value should end up at competitors or those who wants to hack their way in. In such cases, memories or disks need to be shredded or crushed. If doing so, remember to facilitate for the next step with recycling. Thus, it can be a good idea to have a clear instruction and also refer to any similar rules, instructions or policies of the object owner or users' organizations regarding management of data or information at the end of the life-cycle. See also section 3.5 and chapter 8 for more on this matter. Commonly, object owners and users have a process for recycling and if there are any deviations from a normal process or instructions – it needs to be brought up with management. To remember is that if an IoT product is left in a general bin at a recycling facility, the control of it ends. If necessary, additionally cybersecure and protected storage may be required prior to the recycling starts.

1.1.2.6 Authorities – who themselves 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 for instance various forms of critical infrastructures as well as that they can be the regulatory reviewer who visit and review actors where IoT products are used in processes. Thus, they need to have a good knowledge in cybersecurity both regarding the IoT products as well as the contexts wherein these are used. Examples of such authorities within Sweden are The Swedish Food Agency (water production), The Swedish Post and Telecom Authority, The National Electrical Safety Board and Swedish Civil Contingencies Agency whereas examples of those who use IoT products are 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).

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

A question that often arises is if there is any reason to certify an IoT product? There are obvious reasons such as legal or regulatory requirements, e.g., GDPR and CE-marking within the EU (as well as the upcoming EU Cyber Resilience and Cybersecurity Acts), or industry requirements which are expected in order to be able to market the product. Further, the UK, which is a large market within Europe but outside of the EU, there will be a requirement for UKCA-marking for products from the 31st of December 2024 alike the EU's CE-marking. There are more on these industry requirements in the bulleted list further below. Further, certain customer segments may have specific requirements or more or less have to buy certified products in order to be able to show that they fulfill the requirements posed in the next step of a value-chain (from authorities or customers). In addition, boards of directors and owners of businesses or organizations has started wake up and sometimes initiates various cybersecurity-related certifications, e.g., ISO 27001 or IEC 62443, for the own business or organization. Subsequently, they need to review which equipment, IoT products, software, etc., that they use themselves as well as market/provide and which certifications that may be required pertaining to these. Thus, a certain measure of proactivity has been sparked with the intention to provide advantages within business development and marketing, and that later on their offering is not to be early filtered out in the sales process (or disqualified as offer) due to a too low level of verified cybersecurity.

To certify an IoT product costs both time, work effort, and money. Thus, this needs to be thought through for to provide more output value than what is input to this process. A good practice is, prior to starting any certification efforts, to query colleagues and friends within the same business as well as the certification auditors (for the standard of interest) how much a certification may cost as well as how much calendar time that can be expected.

The certification of an IoT product may provide advantages as some tasks or processes can be minimized or eliminated. Examples of such are sets of queries from customers, as part of qualification steps or pre-procurement information collection, as the procurers can themselves easily read or get simple information about which certifications the IoT product has. Just this step can minimize a work effort of commonly 10-100 hours each time as the sets of queries are not identical. Further, if having certificates of standard certifications to show customers and other stakeholders, well-selected and appropriate standards provide a clear view of the cybersecurity status.

Below are some examples of standards for cybersecurity that are applicable for IoT products within 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, Informationsäkerhet inom fastighetsområdet & IoT, Arkitekturgemenskapens Referensarkitektur för IoT (till smart stad och digitala tvillingar)
- **Industry** – IEC 62443 3-3, 4–1 and 4–2
- **Marine applications with class actions required** – DNV-RU-SHIP Pt.6 Ch.5 and Lloyd's Register Cyber Safe for marine (these are both based upon the IEC 62443 3-3)
- **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
- **Municipalities, counties, and government agencies** – Swedish Association of Local Authorities and Regions/RISE, (KLASSA för IoT), SSNF Robust och säker IoT (stadsnät i Sverige), Traficon (Finish 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
    - EU Cybersecurity Act, which is a framework comprising cybersecurity requirements for certification
    - EU Cyber Resilience Act, which poses requirements of the inherent cybersecurity of a product during its whole life-cycle
    - EU Radio Equipment Directive (RED), which will apply for 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 keep some standards, which are adequate and provide support during an IoT product's life-cycle, close and use these for support in for instance chapter 3 and its requirement analysis.

1.3 Regulatory frameworks and legal requirements

The EU NIS Directive, i.e., Directive on Security of Network and Information Systems, became Swedish law during 2018 and will get updated to "NIS2" at the latest in 2024. The foundation for the directive is requirements put on organizations, delivering services that are of importance for society, to have systematic risk- and cybersecurity efforts where any security-related incidents are to be reported and managed adequately. The current version of the directive poses requirements on obviously critical operations within for instance health care, clean water production and distribution, digital infrastructure, etc. The new version will increase the scope considerably and also includes district heating, sewage and wastewater management, food, chemical production, as well as a number of branches of manufacturing and production industries. In coordination with NIS2, there are a number of other new and updated regulations and directives from EU (see example in Figure 2). Many of these has direct connections in between. Thus, it is needed to make a thorough analysis of all these frameworks, directives, and acts, in order to create a unified set of requirements to move on with.

Some examples of such complimentary to the NIS2 are:

- **CER** – *Critical Entities Resiliency Directive.* Requirements on organizations involved in operations that are critical for society. Overlaps with the NIS2.
- **DORA** – *Digital Operational Resilience Act.* Requirements for resilience within the financial industry.
- **CRA** – *Cyber Resilience Act.* Requirements on technical equipment and there are many overlaps/connections with NIS. Further, it is relevant for IoT products in general.
- **RED** – *Radio Equipment Directive.* Concerns primarily requirements on equipment with any kind of radio communications technology.
- **MDR/IVDR** – EU regulation concerning medical technology products and medical technology products for in vitro diagnostics.
- **Machine Directive** – Requirements for ensuring that machines in any form not are dangerous to use. This directive will also in the future address cybersecurity, usage of AI and other technical challenges within the area.

Among these, it is most likely that the NIS2, CRA and RED are applicable for IoT-technologies within many areas. In cases where IoT is used as part of a machine, also the Machine directive will likely be applicable. Medical technology products are highly restricted having strict cybersecurity requirements. NIS2 and the others put a lot of focus on creating cybersecurity within the supply-chains and putting requirements on one's suppliers. In practice, this entails that all parties who expect to provide products and services to NIS2-organizations need to adapt to the requirements although the own organization is out of scope for NIS2 requirements. Additional requirements highlighted by NIS2 are incident response management, resilience to issues/disruptions, coordination with authorities who have regulatory review responsibilities, vulnerability management, ability to measure the efficiency of cybersecurity efforts, management responsibility, and the need for competence at management level.

The NIS2 has a scope for sanctions towards operations who does not comply with up to 2% of global turnover or 10 M Euro.

2. Threats towards IoT products, risks and principles

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

IoT products can be used in a lot more contexts and applications not foreseen. The handbook mainly addresses IoT products used in the following contexts although there are many others 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.

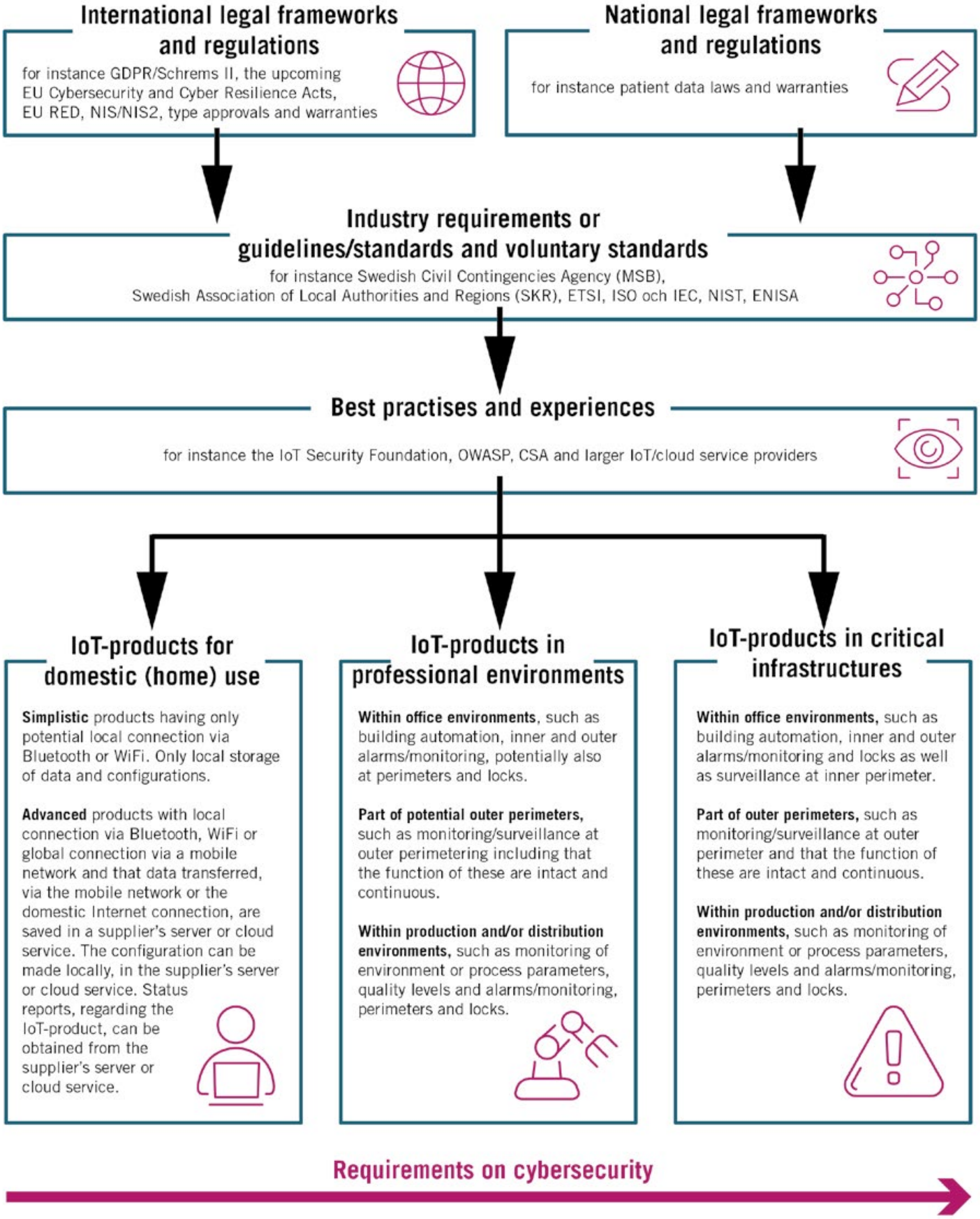
Professional environments – building automation systems and lock/alarm systems, industrial production/distribution, maritime environments with function of vessels or platforms, health care ranging from acute care to elderly care, food and beverage production/distribution, remotely by humans driven or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

Critical infrastructure – functions or services critical for society[5].

Within professional environments and critical infrastructures, IoT products are by many professionals seen as one of the largest threats to their operations. Thus, it is of great importance that IoT products further on get an inherent good, or very good, level of cybersecurity so that this labeling can be removed.

Figure 2 indicates how overarching legal requirements to voluntary good ideas and experiences can affect an IoT product except the requirements posed by object owners at customers and the supplier itself or other stakeholders in the value-chain. The IoT products shown are put into the different categories of domestic (homes), professional environments and critical infrastructures. There are of course many more, but these are not brought up here. The point is not that there are more, but to understand that there are requirements not only originating from the object owners at customers as well as different groups or types of IoT products from very simple ones to extremely advanced, which may be connected or not to networks. In addition, the cybersecurity and availability/resilience requirements may differ significantly between IoT products targeting domestic use compared to use in professional or critical infrastructure contexts. Thus, a customer must be prepared to pay more for IoT products targeting professional or critical infrastructure environments compared to those targeting domestic use. Further, to install IoT products aimed for domestic use, because they are "cheap" and "solve the problem", into the other mentioned environments is not a good idea and will likely not either be particularly cheap or value-creating in the long run.

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



International legal frameworks and regulations

for instance GDPR/Schrems II, the upcoming EU Cybersecurity and Cyber Resilience Acts, EU RED, NIS/NIS2, type approvals and warranties

National legal frameworks and regulations

for instance patient data laws and warranties

Industry requirements or guidelines/standards and voluntary standards

for instance Swedish Civil Contingencies Agency (MSB), Swedish Association of Local Authorities and Regions (SKR), ETSI, ISO och IEC, NIST, ENISA

Best practises and experiences

for instance the IoT Security Foundation, OWASP, CSA and larger IoT/cloud service providers

IoT-products for domestic (home) use

Simplistic products having only potential local connection via Bluetooth or WiFi. Only local storage of data and configurations.

Advanced products with local connection via Bluetooth, WiFi or global connection via a mobile network and that data transferred, via the mobile network or the domestic Internet connection, are saved in a supplier's server or cloud service. The configuration can be made locally, in the supplier's server or cloud service. Status reports, regarding the IoT-product, can be obtained from the supplier's server or cloud service.

IoT-products in professional environments

Within office environments, such as building automation, inner and outer alarms/monitoring, potentially also at perimeters and locks.

Part of potential outer perimeters, such as monitoring/surveillance at outer perimetering including that the function of these are intact and continuous.

Within production and/or distribution environments, such as monitoring of environment or process parameters, quality levels and alarms/monitoring, perimeters and locks.

IoT-products in critical infrastructures

Within office environments, such as building automation, inner and outer alarms/monitoring and locks as well as surveillance at inner perimeter.

Part of outer perimeters, such as monitoring/surveillance at outer perimeter and that the function of these are intact and continuous.

Within production and/or distribution environments, such as monitoring of environment or process parameters, quality levels and alarms/monitoring, perimeters and locks.

FIGURE 2 – IMPACT FROM 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 PROTECTION.
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 of these, but the ones mentioned are enough to start with. All of these are good to keep in mind while considering and mapping out which assets, who are within the IoT products or in their proximity, and needs to be protected in order to avoid probable consequences. Below, there are several such assets described in brief.

Domestic assets

Which domestic assets are worth protecting? Besides destroying the building, by causing fires or floodings, there are data about the residents which can be accessed via microphones/speakers and cameras and that data is wanted to be kept confidential with the integrity ensured. During the cold part of the year, electricity and heating systems need to function so that water piping does not freeze and cause water damages. Further, during the whole year, water and sewage, ventilation as well as the electric system and internet connection etc. should also function well. Poorly protected equipment used for internet connection may provide access to various systems and potential sensors, information about the home network's set up, and further information about more or less everything that is connected to the home network. If a fridge and freezer, which are not protected from water leakage, are unnoticedly turned off it may cause water damage. Further, a low-quality connected toaster, which is kept going continuously, may cause a fire. In addition, based on the data collected about the residents it can be analyzed if 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. In worst case, this may lead to unwanted visitors when the residents are out of the house. If there is an unsecured alarm system, it can be tested if it is activated, used to reveal what answering times various sensor readings or a triggered alarm have, if sensors function and are activated, and if sensors can be shut down when wanted. There are many examples of why IoT products or solutions, often referred to as smart products, used in domestic environments must be both physically secure as well as cybersecure

Professional environments

Professional environments comprise many assets needing protection, such as data about: various 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 which equipment that are installed in the network. Further, there may be a lot of details about an operation's processes, what is produced and distributed as well as how this is executed. The last mentioned can be open IPR or IPR which needs to be kept secret. In addition, for most operations it is vital to run production and distribution processes without disruption in order for what is produced to keep the wanted 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 can affect markets and thus must be protected. IoT products which are faulty installed, or erroneously configured, are a great concern for many cybersecurity professionals in professional environments, and such IoT products without adequate cybersecurity-level will get highly dependent on that the cybersecurity-level in the surrounding network is kept up continuously over time. The function of an operation's IoT products and processes can be related to the trust of object owners at customers in the supplier's ability to deliver and the supplier brand. This trust is in some cases extended to authorities who have regulatory review/inspection responsibilities. The trust can probably take a hit or two, but in the short term some sales may be missed. A larger hit to the trust can be harder to cope with in the long term.

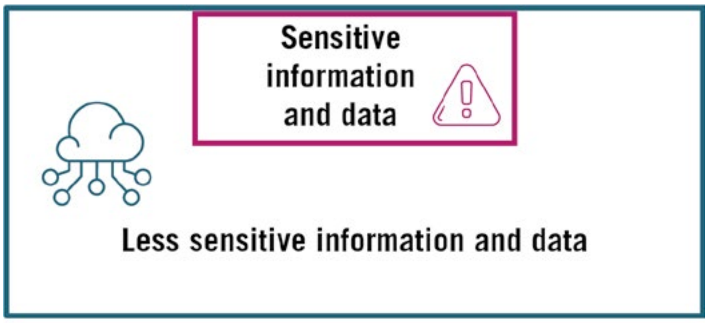

Sensitive information and data
Less sensitive information and data

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

Critical infrastructures

Critical infrastructures comprise a lot of assets needing protection and these assets are subject to national laws and regulations and must have an adequate physical protection and cybersecurity-level. The assets may hold highly interesting data and information about the processes, facilities and networks they are used in. Commonly, these processes must operate at very high availability, 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 although availability and integrity are paramount.

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

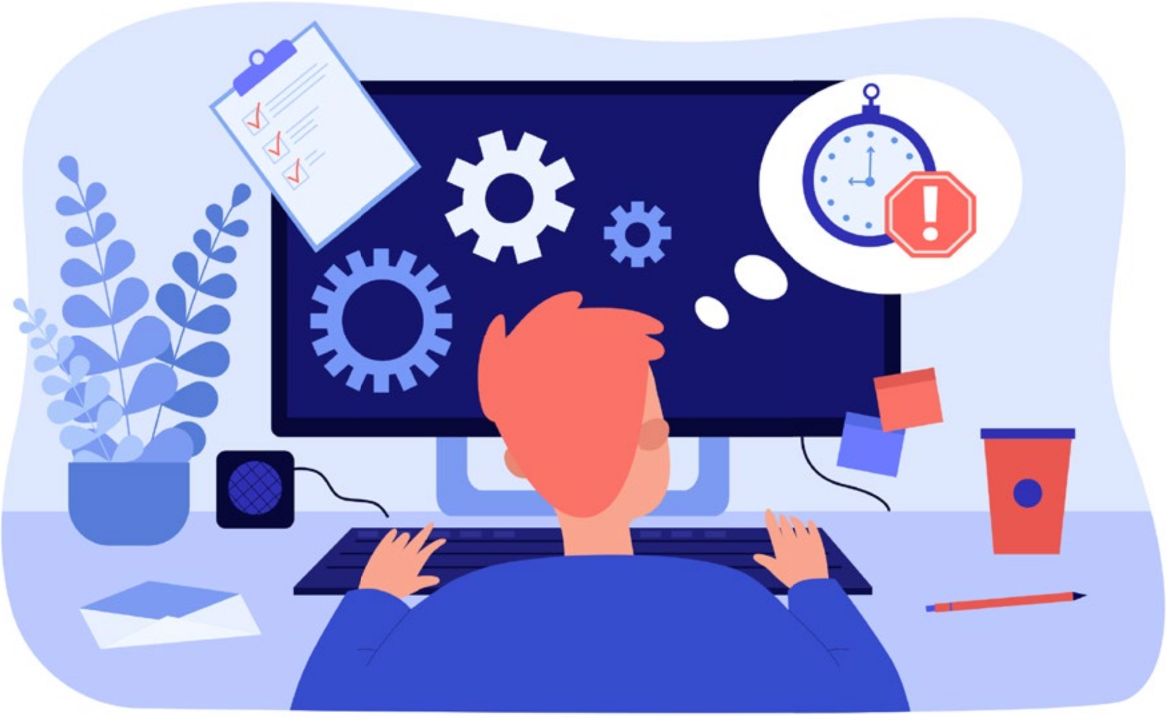
To sum up, all mentioned contexts, ranging from domestic to critical infrastructures, must consider which are their assets to protect. The common answers are: data and information, availability and integrity of various equipment and processes, the trust of object owners and partners, brands, etc. Thus, a supplier of IoT products needs to understand its customers' contexts and develop an adequate protection through instructions and processes in combination with functionality in order to achieve the wanted level of protection and cybersecurity. It is a must to understand which are the legal and regulatory requirements which directly or indirectly have impact now and in the future. Further, what to protect and secure must be understood and turned into development requirements. Additional structures and processes may be required to develop in order to reach the adequate protection and cybersecurity-level.

2.2 Weaknesses and vulnerabilities

Assets may have inherent weaknesses and vulnerabilities already from the very start, or these can arise later on due to poorly developed updates or upgrades or that combinations of issues are discovered. The weaknesses and vulnerabilities may reside within the hardware, or its potential firmware, operating system, and the code or applications which 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 – which is an encrypted tunnel from one point to another), or that updates or on-site maintenance bring in non-controlled software and equipment causing a virus or malware to get in. It is usually easier, at a later stage, to fix security weaknesses and vulnerabilities in software than hardware.

In domestic contexts, unfortunately it is common to have almost no, or poor, protection of equipment connected to Internet as well as poor segregation of networks (i.e., separation and segmentation) used for building automation, children, work, alarms, etc. A segregation of the network(s) makes it harder for virus and malware and can also, besides provide improved security, enhance the bandwidth needed if there are high load on the network.

IoT products aimed for domestic contexts are often able to update themselves, in terms of firmware and software, if this is configured at the installation. Else, there is a need to manually update firmware and software on a regular basis. Further, it is unfortunately common that IoT products for domestic use have poor design of cybersecurity or initially lack it within hardware, firmware or the software run on top of this. An area where improvements are made, but still is not adequate, is to force the change of standard configurations and passwords during installation and commissioning. Unless these are changed it is unfortunately rather straight forward, if the IoT product can be accessed by unauthorized persons, to take over the IoT product and potentially use if for unwanted activities. Such activities may include: creating disorder; extortion by encrypting the data, information and systems; cause systems and IoT products to be inaccessible; use IoT products as parts of bot-nets for DDOS-attacks targeting Internet-based services such as banks or payment systems (SWISH and BankID) or web sites for booking of train tickets. If there are unprotected IoT products for domestic use that comprise microphones, speakers, or cameras, it may be good practice to ensure these do not comprise weaknesses or vulnerabilities and that these cannot be used to collect data/information about the residents and whether they are at home or not.



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

There are many commonalities between IoT products for domestic use and these aimed for professional environments or critical infrastructures. In the latter ones, it is however much more important to not open up weaknesses or vulnerabilities through poorly designed functionality and too low level of cybersecurity. The level of cybersecurity also goes for the networks, external connections needed, and the processes related to installation, configuration, commissioning and later support, service and maintenance until the decommissioning and deinstall. It is essential that in professional environments and critical infrastructures to also ensure that information about the networks and network equipment, wherein the IoT products are used, is not revealed through poor design or cybersecurity. Such information is often used as part of cyberattacks.

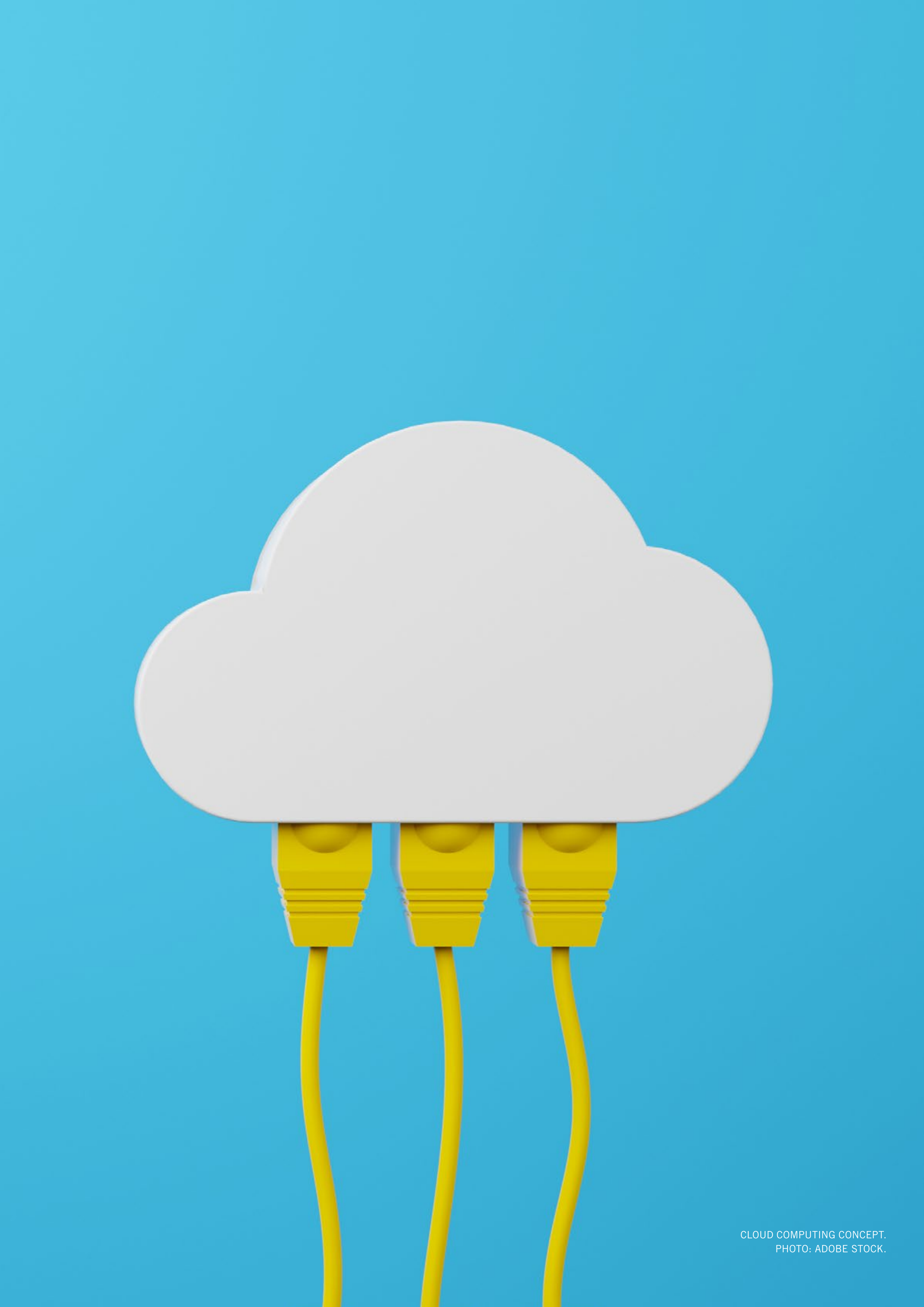
TO NOTE! If there is an interest to learn more about weaknesses, vulnerabilities and what is actually exposed to the outside (i.e., the Internet), a possibility is to use the web browser TOR in combination with the search tool Shodan (this should not be made from a computer within a secure network). Then it is easy to view, within different geographic areas, equipment that are obviously exposed and potentially unsecured and thus possible to connect to. If doing this, a large amount of web cameras, sensors, and building automation systems, etc., can be listed. Unfortunately, there are many good and cheap tools available for various types of hackers both on the Internet as well as on Darknet. See 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 as well as how to install, configure or commission the IoT product in a cybersecure manner. Further, also missing is often how to maintain an IoT product's cybersecurity-level during the whole life-cycle. Thus, it can be good to add this either integrated into the user manual or make an extra appendix at the end of it. A rule of thumb is that the lower the inherent level of cybersecurity is the higher protection level around it is required.

2.3 Common threats

Commonly, different threats are categorized as *less malicious*, e.g., hobby hackers, and malicious ones such as professional hackers and actors 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 last five years with the projection to increase furthermore. Cyberattacks or attempts to intrude are launched around the clock and are largely automated in order to the malicious actors to find out where they can get in and what they can do there. Following, these actors make a (business) plan, and depending of purpose/intent, they craft a schedule for what to attack or what to infiltrate for collection of information over time. Professional hackers and national state supported actors have very good knowledge and is in many cases well ahead of many IoT product suppliers as well as their suppliers of firmware and operating systems etc.

Another threat, mainly posed by professional hackers or national state actors, is to hack into an IoT product's development environment or somewhere in its distribution chain with intent to plant a hostile piece of code or hardware component and thus provide a way in (i.e., back-door) later on as the code is distributed to the target environments at the users. This is often denoted as a "supply-chain attack". Another way to plant hostile code is through the use of open-source code (there are various frameworks), which have not been adequately reviewed prior to addition to the code base. There should be responsible lead developers who review the open-source code, its continuous updates, and accepts these prior to addition and use. The origin of the ones behind the open-source code should also be reviewed



CLOUD COMPUTING CONCEPT.
PHOTO: ADOBE STOCK.

and no open-source of unclear origin should be used. Later, it is very hard for developers, who use the open-source code adopted, to find any hidden back-doors or code that send out selected data about the users, process and environment/ networks. If the open-source code, or code packages procured from vendors, are signed and all look good, it is quite a demanding task to review all (and do it continuously) also with the help of review tools. This is very hard for the ones that install and use IoT products to detect, in particular if the update or upgrade packages distributed are signed and all look OK in testing pre-installation. One problem is that sometimes the hostile code can be time activated and dormant or just opens up a window to the outside and enables hostile actors to decide what, how and when to do hostilities. The usage of open design concerning hardware has the same type of problem and open designs need to be reviewed and any assembled components/circuits should be carefully reviewed and tested as well prior to usage.

Further, an additional threat is the own staff (or inhouse consultants) and the ones involved in the whole value-chain around an IoT product until it is decommissioned and deinstalled. Commonly, it is mistakes or a too low level of competence that may open up weaknesses or vulnerabilities and allow these to remain surrounding the IoT product. Rarely, it is disgruntled staff who consciously disrupt processes, do sabotage or steal data, information or IPR and sell it to hostile actors. Unfortunately, the latter occurs although the first mentioned, with mistakes from own staff (or inhouse consultants), are more frequent.

In addition, there are multiple threats, and these 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 intended for hacking or disrupting organizations and their processes. To buy hacker tools cost from a few dollars to thousands of dollars, all depending on what can be accomplished with the tool. Such tools can be purchased on Internet, Darknet or from firms specialized in providing such tools to actors like police, intelligence services and others who can pay. Thus, the relation between what it costs to raise a cyberattack to what the impact may be, is that with a small amount a large impact/ loss/cost can be caused. Further, owners of IoT products or owners of organizations where IoT products are used, need to ensure that their IoT products are not part of bot nets or other hostile campaigns.

There are IoT products which are connected in different networks but do not communicate outbound, these which communicate outbound, as well as these that are installed in isolated islands and disconnected from the network where they are used. The ones, residing in isolated islands, may sometimes have a mobile connection outward to be able to transmit data, get updates or upgrades, get remote support or maintenance. In such cases, it should be considered whether to have a process for opening up remote access and not keep such open continuously. It is rather common to put “problematic” equipment in islands if they are old, non-updated and have a too low level of cybersecurity to be allowed in the organization’s network. A vulnerability which can be used by various actors is the support, service and maintenance of IoT products and find ways to get hostile code, malware or viruses planted. Thus, the processes for support, service and maintenance must be reviewed in order to ensure that these do not open up such weaknesses and always ensure that any new updates, upgrades, components or spare parts brought in are verified to be “clean” prior to installation. Examples of where verification can be needed are downloaded software packages, external lap-tops, USB-sticks or disks. Thus, there must be cybersecured support, service and maintenance processes at the supplier of the IoT product and at other involved parts of the value-chain.

2.4 Risk analysis and risk mitigation

Risk analysis, which involves to estimate/calculate the probability of and the potential impact from how an asset, by using its weaknesses/vulnerabilities, can be used within the scope of the threat. Thus, a risk analysis potentially needs to involve many actors in a value-chain. At an initial stage, it is likely that the IoT product supplier's development organization will be most involved in risk analysis efforts and at that stage also try 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 get involved as well as if there are any part stakeholders of interest at the customer (where the IoT product is used). At professional customers, object owners, maintenance leaders 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 both professional and domestic customers, user groups or similar can be a good source for new requirements to develop. To listen to customers is also a way to avoid discontent users or stakeholders, who may post their discontent on Internet if nothing happens

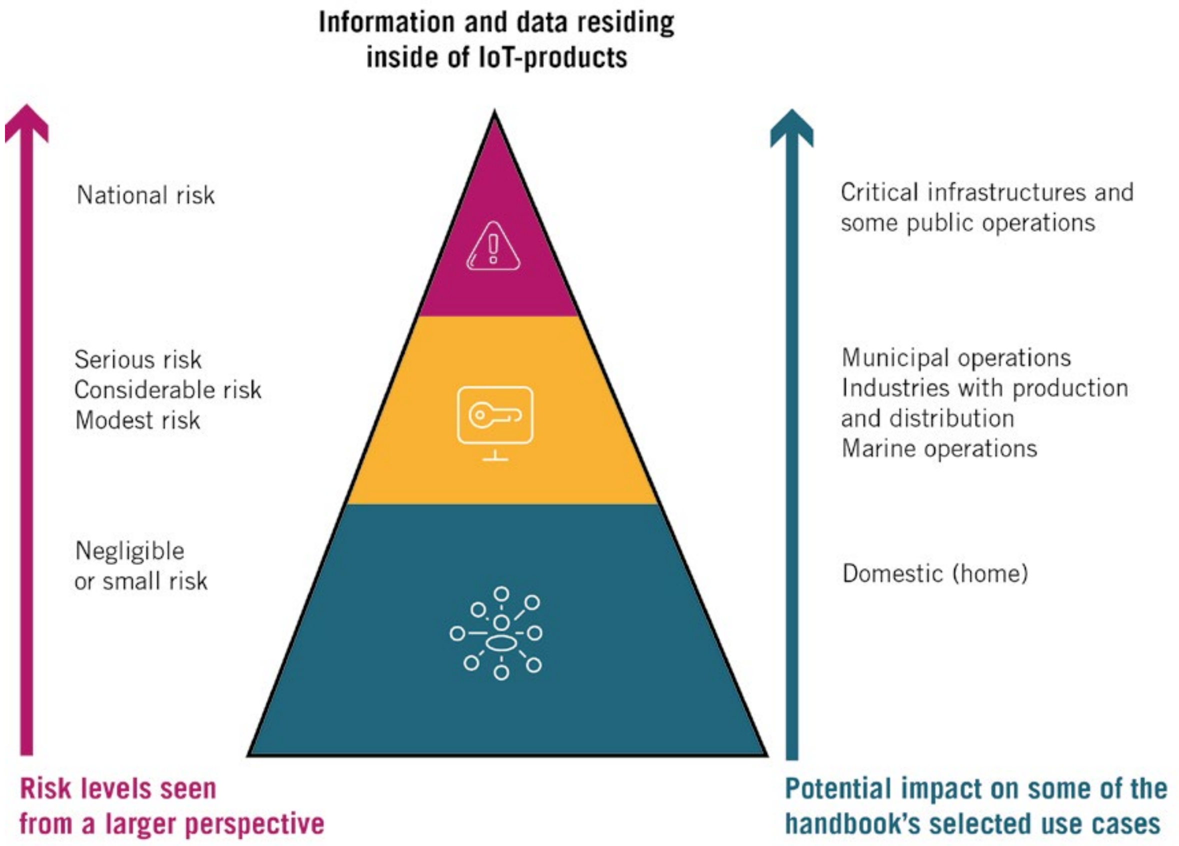

Information and data residing inside of IoT-products
National risk
Serious risk
Considerable risk
Modest risk
Negligible or small risk
Critical infrastructures and some public operations
Municipal operations
Industries with production and distribution
Marine operations
Domestic (home)
Risk levels seen from a larger perspective
Potential impact on some of the handbook's selected use cases

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

RISK ANALYSIS SHOULD BE MADE ON A REGULAR BASIS DUE TO CHANGES IN THE SURROUNDING ENVIRONMENT PHOTO: ADOBE STOCK.

in terms of development and improvements. Further, some suppliers pay those who finds weaknesses/vulnerabilities to prevent that these end up in hacker groups on Internet or Darknet to make money there instead.

Figure 4 provides an example for how different organizations' data and information can be seen in risk levels and roughly what impact a potential exposure of these can render in a larger perspective. The potential impact of the risks regarding for instance availability or integrity is not part of the Figure 4.

There are simplistic and complicated methods to use for a risk analysis. It is probably better to start up with using a simplistic method and make it further sophisticated later on as needed. 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. To remember, nevertheless which method is used, is to involve all parties, stakeholders and actors who need and can contribute. Unfortunately, it is common to bring in too few of these, which can result that the overall risk is not accurate. Further, risk analyses are to be executed on a continuing basis (at the start of all development projects at IoT product suppliers and at least annually at the customer) and more often if the surrounding world, i.e., the risk profile, drastically or fast changes to the worse.

2.5 Principles for cybersecure design of IoT products

There are supporting principles for many aspects of design and development of products. There is general as well as specific ones targeting IoT products. The design-for-x or x-by-design thinking has been around for a long time and, in particular, involving mechanical product development, and these principles have been developed as demanding business models have transformed mechanical products to become IoT-fied or transformed to further extensive cyber-physical systems or even larger systems (e.g., systems-of-systems). Examples of such business models are: products with loosely coupled services, products with integrated services, PSS (Product-Service Systems) and functions or functional products. These should all be of interest for suppliers of IoT products. Pertaining to cybersecurity, EU and ENISA have since a while launched the principles of security-by-design and privacy-by-design. The foundation for these is that cybersecurity requirements shall be part of the initial set of requirements, as otherwise the later added-on cybersecurity will become more expensive and likely not as good too. Further, personal information (which is processed, stored and/or communicated) shall be protected already from start to end of the personal information's life-cycle within that system. This concerns mainly general software and systems, but also IoT products. There are additional design principles of interest, such as Stallings and Brown[6] who prescribe to minimize the attach surfaces of networks, software, people and via physical access. Stallings and Brown outline 13 principles including for instance: least level of rights/authorization, separation of rights/authorization (i.e., that a single user can only do certain tasks alone where some tasks requires that two users are 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 encompasses that each part of a system shall have its own adequate level of cybersecurity and not be dependent on any other parties' level of cybersecurity. Thus, here goes the slogan "never trust, always verify" and that no one shall trust anyone else prior to a successful verification. An IoT product can, or should if needed, be divided into different trusted zones. Of course, this depends on which parts or components that the IoT product comprises. However, to be able to create a separation and keep up a high level of availability and protect data/information, such separation into zones can be necessary. Chapter 3 will bring up more on this aspect and if the requirement engineering during development of IoT products uses the contents from chapters 2 and 3 - both the above design principles will be considered. Chapter 3 brings up a number of standards, whereof most addresses at least the security-by-design[7].

Another, but not new, principle or paradigm is the micro-services paradigm, which has started to be used a lot 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 that causes the costs for maintenance and testing to be unnecessarily extensive and time consuming (as all code need to be tested even at small changes). To lessen this problem, "containers" or similar is used to put small and independent micro-services (which should be easy to replace and have well-defined service descriptions) which collaborates with other such micro-services using well-defined protocols and interfaces. The strategic thinkers have added common base functionality for cybersecurity, administration and fleet management in an underlying platform which 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 you change one or a few of them. If there are changes to the underlying platform, it needs to be tested as well as a number of selected micro-services depending on what the changes are related to. However, to keep developing IoT products and keep all software code in one or a few blobs is not efficient nor a profitable way forward. There is a risk that not doing this will impair the innovation speed and tie up resources for no good at all. There are many such underlying platforms for IoT and automation, and the hard thing to do is to select which is currently good as well as in the future. If the code is developed in an adequate way, it is of course possible to change the underlying platform and if having a common underlying platform within a development organization it can potentially render good scaling effects as knowledge and automated test suites can be re-used for new projects and IoT products.

Regarding the hardware, there are similar ways of thinking as for the software, as when it is possible and suitable to break down larger parts into exchangeable modules and components which have well defined interfaces and standardized functionality (i.e., compatibility).

[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

3. Prior to starting up a new project

This handbook aims to cover the whole life-cycle for an IoT product and this affects the requirement analysis and the potential infrastructure and processes as well as structures needed around an IoT product. There are quite a few aspects that need to be considered prior to starting up a new project as well as already from the very start of the life-cycle. Unless these aspects are well-considered, there is a risk that the initial development/project cost looks fine whereas the whole life-cycle cost and profitability will not look good.

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 necessary 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 optimizations and training packages. Commonly, this phase is the longest in a life-cycle
- Monitoring of IoT products during its life-cycle. Usually, this phase is also long
- At the end of a life-cycle

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

At an early stage, it is necessary to keep sensitive planning and decision-making concerning an IoT product's business protected and confidential. This does not directly impact on an IoT product's final level of cybersecurity but the start to get there. Thus, needed to protect are: information and sketches/drawings as well as notes which are 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 within as a small group as possible in order to maintain confidentiality prior to the next steps to take.

Therefore, cybersecurity is needed in an organizations IT-environment and development environment 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 to continue with
- Concept development – protection of ideas, sketches, and drawings as well as business modelling/planning
- Prototypes and/or demonstrators

- Protect the early requirement analysis' results, which may be generated out of prototypes or demonstrators as well as the experiences made out of these

Further, it is needed, for all involved, to not talk or discuss the early stage's contents or results but act responsibly and handle such information with adequate protection at visits at customers, in the car from work to home when stopping to shop groceries, while travelling in the line of duty, or commuting to and from work using public transport. Thus, all this may require that such information is encrypted and protected by additional means both within the organization's environments as well as when it is outside the premises carried around inside of lap-tops, mobile phones, and USB-disks or are e-mailed.

3.2 Requirement analysis – collection and analysis of functional and holistic requirements from stakeholders, laws/regulations, industry standards, etc.

There are a number of general and governing requirements for cybersecurity, i.e., the CIA+TP which are further described below, that may impact the whole IoT product's design and adaptation to various circumstances during the life-cycle. Specifically, the developer of an IoT product needs to understand the surrounding contexts, processes and data/information that will be present during the usage. It is advisable to ask users at the customers which level of availability (e.g., potential availability classification) is wanted and what data/information that will reside within the IoT product. Examples of data/information security categories are: open, internal, confidential, strictly confidential as well as if personal data or data about critical infrastructures/state security will be part of the scope.

- **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 requirements for availability, robustness and resilience (i.e., be able to continue to operate in case of serious problems or issues)?
- **T (Trustworthiness)** – what is required to uphold the trust, concerning the IoT product, from customers, the surrounding world, and the own organization?
- **P (Provenance)** – traceability (i.e., provenance) regarding the data/information which reside in the IoT product and potentially later is transferred to other systems for storage and analysis? The IoT product's configurations and settings may be affected here as well. Any changes made to the IoT product's hardware and software need to be traceable in the development environments by for instance using "tag" in software code and version numbering or similar arrangements.

Within IT environments, the order of importance for the starting triad is commonly CIA whereas within OT environments and critical infrastructures the order of importance is often AIC and the TP attached at the end. Thus, it is of importance to know/learn if the IoT product will be used in IT or OT environments alternatively within critical infrastructures.

Regarding the data/information, which will be generated within or around an IoT product, and that have a potential value for analytics or add-on services and extra functionality pertaining to maintenance/monitoring/optimizations, it is advisable to firstly analyze business-related, legal and contractual matters such as:

- Who will own the data that will reside within 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?

THE CYBER SECURITY THOUGHT PROCESS MUST START ALREADY WHEN YOU START PLANNING A NEW PRODUCT AND IS NOT SOMETHING YOU SOLVE ONLY IN THE END-USER PHASE. PHOTO: ADOBE STOCK.

Depending on the outcome of above questions, it is anyways a good idea to separate different types of data in order to facilitate so that the above questions can be answered clearly and also prepare for future business development (which may take off as everyone understands the possibilities of using data for different purposes). An example of such a separation is:

- **Data related to persons** (due to for instance GDPR within the EU). If this data are kept separate, it is much simpler to develop functionality needed to follow up compliance to various laws and regulations.
- **Process and quality data** which concerns the activities or processes where IoT products are used. These data can for instance be used for optimizations of functions and quality-level within processes (by measurements on the processes' input and output – broken down to sub-processes and/or whole processes).
- **Maintenance-related data**, which pertain to wear and tear and need for maintenance of IoT products and its surroundings, and are collected via sensors, cameras, counters, etc. This is something that IoT product suppliers commonly provide as add-on services as well as collect data about their fleets in order to find if there are any general problems or weaknesses that need to be designed out or corrected through improved maintenance processes, etc. Additional related functionality may be to enable reduced load (graceful degradation) or emergency shutdown capability to prevent a complete breakdown.

3.2.1 Industry standards and standards which can be usable and provide guidance to cybersecurity requirements

Laws and regulations can pose obligatory requirements whereas other requirements may be voluntary or posed by the industry an organization is active within. All this can be the base for general and physical security requirements as well as cybersecurity requirements. Some physical security requirements may be related, or linked to, cybersecurity requirements by that an IoT product may need an outer physical security protection/perimeter or that it is locked into for instance a cabinet/room preventing physical tampering without authorized access and authorization level. Further, there are a number of best practices which can, in an efficient manner, provide others' past experiences and not having to repeat these spending unnecessary efforts and costs. Such best practices can be a source for cybersecurity requirements pertaining to the own IoT product. Below, there is a summary which may provide a high-level guidance into these. However, all product development groups need to do their homework and find out what is required and applicable for their IoT product within the contexts and industries of interest.

- **Product rules/regulations and laws** – CE-marking including for instance RED and other type approvals as well as extended warranty. This is often a requirement within EU, USA, Australia and Asia
- **Laws about safety/security/cybersecurity**
  - GDPR (and Schrems II) or similar laws/ regulations in other parts of the world
  - The nearing EU Cyber Resilience Act (cybersecurity requirements posed on products throughout the whole life-cycle)
  - The nearing EU Cybersecurity Act (framework for cybersecurity certification)
  - Patient data laws
  - National safety/security protection laws
  - The EU NIS/NIS2 directives which concern critical digital services related to (an extended) society
  - UN Resolution MSC.428(98) concerning marine/shipping sector
  - Swedish law 2018:1174 concerning information security for digital services critical for society
- **Industry standards** – some examples are as follows:
  - 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 (pertains to automation/ control systems in various industries)
  - 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's guidelines and are also based upon IEC 62443 3-3). See also IACS E26/27

  - Swedish Civil Contingencies Agency's recommendations for industrial control systems and IoT as well as cyber-physical systems (critical infrastructure). The Swedish Food Agency's recommendations, which are based on the ones from Swedish Civil Contingencies Agency, are used at regulatory audit/review of production and distribution of for instance clean water
  - ENISA's recommendation regarding IoT/cloud/critical infrastructures and development and used of these (industry and critical infrastructures)
  - Swedish Association of Local Authorities and Regions'/RISE's KLASSA för 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
  - ioXt Alliance (certification program for secure IoT products)
  - SSNF's Robust och säker IoT (stadsnät)
  - Traficon (Finnish transport and communications networks)
- **Best practices and more** – examples are as follows:
  - GOV.UK (Consumer IoT Security)
  - IoT Security Foundation – search their global web site under the "publications" part
  - OWASP IoT Verification Standard (advise 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 the "research" section
  - IBM (cloud and IoT) – search their global web site for best practices and advise
  - 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-related requirements do not have any relation to other matters, and can be considered as stand alone, they are easier to manage. However, there are many such requirements which have relations to other matter alike cybersecurity. To manage the latter ones, the design principles and modularization can be used as well as standardized components/parts and micro-services as the requirements are broken down into smaller pieces.

Functional requirements concern what the IoT product is to be able to do and preferably these shall be practical and well designed to facilitate an efficient management throughout the life-cycle and to optimize the life-cycle cost as much as possible. To develop functional requirements into functionality, that is complicated and expensive later on, such as poor service and maintenance functions will discourage many customers and their users from buying additional ones or replace IoT products whose life-cycles end. Thus, this is important to consider for suppliers of IoT products. An example of this is recent cars where it is very hard to, by one-self, replace a front lamp.

Practical functional and environmental requirements are for example as follows:

Operations environment – the environment where an IoT product operates impacts on the design regarding both outer protections combined with cybersecurity. A tough/rough industrial environment poses its requirements as well as if an IoT product will reside in a more or less unmonitored and unprotected environment outside, indoors or at domestic environments. Thus, both physical attacks as well as cyberattacks may lead to unavailability or destruction in exposed environments. Physical access may also lead to risk for cyberattacks by connecting through unsecure/unprotected interfaces or just being able to remove a hatch and be able to access electric contact points or memory cards in the interior of the IoT product.

Hardware requirements – there are often, also in what appears to be a secure environment, a need to protect the IoT product from physical access and destruction and to not be possible to open up easily. The least that is needed is for instance to use a seal or sticker on any openable hatch above memory cards and/or interior with electric contact points. An alternative is to recommend that the IoT products should be installed in a fully controlled environment with physical locks (i.e., within a locked room or cage/cabinet). To just have a simple plastic cover, which is simple to bypass, may cause that a break-in is not detected within soon. To prevent this, there can be a built-in function that sends an alarm and potentially also deactivates the IoT product at a physical attack or destruction attempt (in particular, if the IoT product can be used to launch a larger cyberattack into a network). IoT product 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 environment – the possibilities to be able to exchange/replace old worn or torn hardware components or freshen them up again in order to be able to continue to use (i.e., re-furbishing or re-manufacturing) should be considered for the IoT product's life-cycle. When the primary life-cycle for an IoT product reaches the end, it is often possible to find a new life-cycle in other contexts, where the requirements may be lower, and it is possible to avoid scrapping or destruction (i.e., re-purposing or down-cycling). However, the IoT product needs to be emptied and all data, information or configurations, etc., properly wiped prior to that the IoT product continues with a new life-cycle elsewhere.

Information flows – it is likely that data and information will flow through the IoT product during its life-cycle and considerations are necessary regarding where the flows shall be stored or buffered on its way to any potential processing. This needs to be made in a cybersecure way. Previously, there is an example for how to segregate the data and information in an IoT product regarding personal data, process- and quality-related data, as well as maintenance- and fleet management-related data, in order to facilitate transparency pertaining to: who owns the data, who can do what with the data when and how. If cloud services or the suppliers' own central servers are used for storage of data and information, it becomes a bit more complicated compared to if the storage is at the customer's site in a data warehouse or local server. Anyways, there are a lot of interesting business development to do now and in the future based on data and information. Thus, this should be considered well.

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

Knowledge in the operations environment – if the IoT product is simplistic, the knowledge required to operate it should be acquired via some training. In case of that the IoT product and its function is complex, there may be a need for extra knowledge provided from the supplier or some other actor within the value-chain. Potentially, depending on context, support and service can be provided from distance through a cybersecurity connection or on-site. Further, training and education packages can be provided. In addition, externals can participate through a cybersecure video link, and a virtual/augmented reality (VR/AR) can be used for training and trials prior to doing the real activities.

Cybersecurity in the distribution chain – how should an IoT product and its components/parts simply and effectively be distributed to customers initially and then later during the life-cycle 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, a lot of time and travelling can be saved. Such a process, which commonly have several steps, need to cybersecure. Consider if it is possible to automated parts or whole steps by using fleet management functions with plug-and-play, autoconfiguration of local settings and network connections, through already prepared central settings which are fetched combined with automatic or manual commissioning. There are a lot that can be achieved here and if able to cut costs for customers and users, having many IoT products, using a high degree of automated process steps - the IoT product becomes very attractive. Some of the advantages using central management, or fleet management, are less errors and it is easier to change a lot of IoT products fast if or when needed.

SYSTEM ADMINISTRATION IS PERFORMED BY A SPECIALIST..
PHOTO: ADOBE STOCK.

Cybersecurity during the potential operation and maintenance phase – an IoT product needs to be designed to be able to be operated and maintained in a cybersecure manner until the end of the life-cycle. Usually, data and information about the process, quality outcomes and maintenance need are needed to do this somewhat optimized, but the IoT product also need to be designed so that this can be executed effectively either on-site or from distance (i.e., what is possible to do or prepare remotely) combined with what can be automated.

Cybersecurity at the end of the life-cycle – at some point in time, an IoT product and its parts/ components need to be de-commissioned, potentially destructed and re-cycled 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 de-commissioning and at the same time also securely remove any IPR, data and information. Further, if physical destruction is necessary, it needs to be according to the customers' policies and their users. However, as a supplier, it is a good idea to have an instruction for how to best do this unless there is a producer responsibility to do the destruction and re-cycling. In case of such a responsibility, there should be an internal supplier instruction in order to properly ensure adequate destruction and re-cycling.

3.2.3 General cybersecurity requirement for IoT products

Each IoT product and the contexts where such are used pose specific cybersecurity requirements. This needs to be discussed and analyzed, in terms of impact, together with customers and users combined with understanding the surrounding world in terms of threat environment, wars and war conditions, laws and regulations. To provide an insight into what can be categorized as general cybersecurity requirements, we will look at the structure provided by the standard IEC 62443 part 3-3 and the security level 1 (out of 4 where 4 is the highest). An industry can have enforceable requirements for components and systems which are critical and can have impact on the environment. Such an example is the maritime industry with class action, which goes for new contracted vessels and installations from 1-Jan 2024[8]. 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.

In IEC 62443 part 3-3 and its lowest security level 1, which in general applies to cybersecurity of components, 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. Within Sweden, different industries have various industry specific guidelines and sets of requirements (see for instance Swedish Civil Contingencies Agency 's 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). Furter, administration from an unsecure or external network may require 2- or multifactor authentication.
  - Identification and authentication of software processes and devices.

[8] Look on the web about IACS UR E26/E27 - https://iacs.org.uk/news/iacs-adopts-new-requirements-on-cyber-safety/

  - User management.
  - User groups/roles.
  - Ability to change and manage authentication method.
  - Management of wireless access.
  - Requirements for ability to be able to change strength/length of passwords and whether passwords shall be visible or not at login.
  - Ability to manage how non-successful login attempts are to be handled (how many are allowed, temporary lock, only administrative accounts are locked and need to be enabled again, mange length of time-outs prior to new login attempts can be made or a number of attempts have been made during a certain period of time).
  - Be able to manage and change system messages.
  - Be able to allow or disallow access from untrusted/unsecure networks.
- **Management and control of usage through:**
  - Requirement for authorization (who has rights to do what) regarding human users according to the principles of division of responsibility and least privileges.
  - Control/management of wireless usage and access.
  - Control/management of potential portable or mobile devices (in connection to the IoT product or its networks).
  - Ability to limit the usage 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 any 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 laws, standards, or object owners at customers).
  - Ensure there are 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 to take in case of audit logging failure – what to do and how to get attention to rectify it?
  - Time stamping of each log entry.
- **System integrity including:**
  - Integrity of communications in unprotected networks (in order to notice if any communications are altered).
  - Have protection against dangerous/malicious code (everywhere or at points with incoming or outgoing communications).
  - Ability to verify that the cybersecurity functionality work (i.e., to have a set of functions, procedures, scripts or similar that can be executed to show/verify that all work as it should work).
  - Validation of input.
  - Have ”fail-to-safe”-functionality if normal operations is not possible due to a cyberattack (and ability to return to a failsafe state).
  - Have integrity protection of sessions (e.g., use of unique sessionIDs for each session).
- **Data confidentiality including:**
  - Protection of the communications and storage confidentiality (through encryption).
  - Apply authorization for access/read.
  - Have requirements for updated and adequate encryption algorithms, key lengths, certificates, processes for management of keys and certificates.

  - Ability to upgrade algorithms and keys with additions if/when there will be tougher requirements.

- **To limit data flows through:**
  - Have segmented networks (logical/physical or both) where the IoT product is operated.
  - Have zone protections with ability to monitor and control the communications at the border of the segment (i.e., compartmentalization) and have "deny-by-default and allow-by-exception" as well as that it should be possible to manually stop the communications in between zones. Further, possibility to operate in island mode.
  - Ability to hinder "peer-to-peer" communications or similar solutions (i.e., only have approved communications within the solution and in/out of segments).
  - Partitioning of application/services/data (in order to achieve independence and protected zones).

- **Response times at events through:**
  - Having audit logs that are readable (read only) for authorized users (humans or tools).

- **Ensure availability of resources through:**
  - Have protection towards DOS-attacks or similar problems – the IoT product shall be able to operate in degraded mode also during such attacks.
  - Have resource management – the IoT product shall reserve adequate system resources for security-related functions in order to prevent that all system resources are occupied (i.e., at maximum load) by the other functions.
  - Have backup functionality – backups of critical data and audit logs shall be made without affecting the normal operations (and be stored at a location that is available but not on-line, i.e., de-linked).
  - Have functionality for restore and recovery/restart – the IoT product shall be possible to restore and recover/restart at a known and safe state after a disruption or error.

CYBER SECURITY CONCEPT, CYBER CRIME ON THE INTERNET.
PHOTO: ADOBE STOCK.

- At high requirements for availability provide extra power source inlet (i.e., possibility to have two or more different power sources plugged in) and a change from primary to secondary power source shall not affect the IoT product's cybersecurity functionality.
- Ability to configure and change settings or configurations of networks and security level – the IoT product shall be possible to configure (via an interface) so that its network and security parameters are aligned with recommendations from the supplier (may be executed locally or centrally via a cloud service).
- Apply the principle of least functionality – unnecessary functions/services, ports, protocols, etc., shall be disabled, forbidden or removed from the IoT product.

If an IoT product has an own, or connects to one external, cloud service or server at another location for to store data, fleet management functionality, updates, report function, optimization functionality, etc., there will be additional requirements 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, there can be a need to be able to manage which software that may be executed on the IoT product (i.e., device) via secure or trusted boot and "chain of trust" from hardware, via operating system to apps. In such cases, additional hardening, such as ”secure boot", can be needed. This is a method designed to ensure that a device only executes trusted software. The method verifies the integrity of software which is loaded during the boot up phase. Commonly, secure boot is implemented as part of an IoT product's boot up software and is based on using cryptographic keys to verify the integrity/origin of software before loaded. Preferably, cryptographic keys are 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. 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 prior to loading and execution, and ensures that only trusted software can be executed. This can help to protect against malicious software, boot kits and other types of threats which depend on being able to execute its code on a device (i.e., the IoT product).

Thus, there are quite a lot that already exist to bring in and consider, and then use that to decide what is relevant for the IoT product to be developed (or for the improvement of existing ones). It is not necessary to come with up all by oneself and one can get far by reading and considering all that already exist in written form.

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 and take on responsibility for and also ensure that the other actors or stakeholders in the value-chain are onboard as well regarding these matters. This may include customers and their users as well. One matter to address is for instance what makes the IoT product function well, both short- and long-term, with an adequate level of cybersecurity. It is hard for a development team to collaborate with many actors and stakeholders, in a value-chain, about requirements crossing organizational borders. Thus, management needs to step up and address these matters to avoid expensive and insecure surprises at a later stage.

Some requirements affect all involved and are often referred to as holistic requirements that cross all borders, and that certain infrastructure needs to be available or that existing such must become interoperable or compatible, and finally that certain processes and set ups of assets/equipment need to be made in a standardized manner. Examples of such assets/equipment are: the IoT product, cloud service(s), certificate infrastructure with a root certificate and revocation lists, federation of identities (provide ability for an authorized identity to log in to multiple services as the organizations behind trust each other and adds that user identity to their list of authorized users), and access, etc.

The management should also start to think in terms of total life-cycle cost instead of initial development cost. This affects the requirement collection/analysis/engineering, decision-making and design and may result in a higher initial development cost which should later on in the life-cycle provide improved profitability. Such long-term savings may originate in that the IoT product is initially prepared and that the management has considered future development plans and architectural decisions. The use of design principles in the requirement collection/analysis/engineering may provide better future results too.

3.4 Cybersecure development environment and development 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 alternatively designs that later will destroy all?

If the above two questions are relevant, some additional questions need to be raised about what the development environment comprises (i.e., development, test and documentation) and who can access what and do what with:

- Who shall be authorized to access parts of the development environment (on-site or remotely)?
  - Who shall be authorized to access the development environment and which tools are they allowed to use there?
  - Is it needed that all can access the software code, hardware designs or service designs, and in particular if one is outside of the organization’s internal network and outside of normal work hours (e.g., weekdays between 08.00-19.00 o’clock)?
  - Is it needed that there is access to the development environment from other countries than Sweden (and if it is possible to open up specific temporary access in case there is a need for such remote work)?
  - Who are authorized to check out all code and can check in code to the main branch or make changes to drawings or blueprints etc.?
  - Is there a requirement to have a code review or design review prior to that any code, drawings/blueprints, service- or process descriptions are checked in to the main branch?
- Is there a need for specific protection of 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 as confidential or strictly confidential)?
- Are there any cybersecurity requirements for collaboration tools, i.e., secure communications and sharing of documents, protection level for documents, requirements for authentication levels, etc.?
- At some point in time, a decision or selection of development process/methodology suitable for the problem to solve need to be made. Here, it is important to consider cybersecurity from the start. It is a good idea to use a development process that ensures that the

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

initial set of requirements is adequate prior to starting up the development in order to avoid costly mistakes. The set of requirements will likely change a bit during the course, as in most projects, and evolve through a structured change management process. To use the same development process/methodology to all problems may not results in an optimal outcome and having knowledge and experience from using several such development processes/methodologies can be beneficial. This is due to the complexity of developing IoT products, which potentially comprise hardware, software, services, processes, cloud services, data/oral communications, and data analytics.

- What requirements should be posed on the development process/methodology? It needs to be able to run a number of parallel sub-processes but still be able to coordinate these so that they progress timely and 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), services and processes (ranging from service, support, maintenance to optimization functionality based on data), management of operation (need to build up the structures and infrastructure needed by the IoT product to operate in a long term and to make incremental improvements of performance and availability). It is an advantage if as much as possible of what is relevant is in the initial set of requirements and avoid poorly designed (or impossible) additions later on.

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

TESTING AN IOT PRODUCT IS IMPORTANT BOTH FOR THE SAKE OF FUNCTIONALITYAS WELL AS TESTING THAT THE LEVEL OF CYBER SECURITY IS GOOD.
PHOTO: ADOBE STOCK.

It is always advisable to manage and control both physical security and cybersecurity around development environments. To develop something, putting in a lot of effort and funding, and then learn that someone else launches something very similar is not joyful and, in particular, knowing that it was we that developed and funded it all.

Those who develop services, processes and other structures needed, may take advantage of the same development environment as where the hardware and software is developed. If doing so, these developers can benefit from the existing model for set up of access rights, authorizations, who can make changes, version management backup, etc.

3.5 Requirements on documentation

– various user guides and manuals

It is necessary to include the cybersecurity-related matters of IoT products in the documentation. However, this is often not the case. Further, this is also necessary in case the IoT product is to be certified, but if not anyways a good idea for all target contexts from domestic to critical infrastructures. A balanced documentation including cybersecurity may comprise:

- The IoT product's function outlined. Provide a comprehensive view of the whole "system" and how the cybersecurity (plus any needed physical security surrounding) should be set up in a schematic way. Which roles will log in, to where, and what will they do?
- Recommend that customers and their users cybersecure their operations environments – how can that look like? Is an own physical and logical network segment needed as relevant protection (e.g., firewall/gateway having buffering of data) or is it just a part component of another system?
- What goes if the IoT product is operated in a non-recommended environment – who is responsible for this?
- How to complete a cybersecure installation, configuration, and commissioning?
- How to transmit any data outwards?
- Do the customers and users need to make firewall openings (i.e., which ports, protocols, etc. are needed for the operation) and what are the requirements for authentication and secure communications posed by the IoT product? All this needs to be explained in the documentation. If 2-factor authentication or other types of multi-factor authentication is required, for instance pertaining to administrators, this may require that such solutions are installed and possibly acquired if there is no such available.
- How to verify that an IoT product's cybersecurity is correctly set up and configured? Is there a specific function, procedure, script, or other way to verify this? This is a common requirement part of certifications.
- Will support and maintenance be provided from distance via Internet or other networks? Is it possible to build in maintenance/update functionality within the IoT product, which is initiated for instance as the IoT product connects to a cloud service to transmit out data and fetch any configuration changes made centrally? Another option is to have an external VPN-connection, which must be authorized and set up according to the customer's policies.
- Is local cybersecure support and maintenance needed on-site? If so, it must be ensured that cybersecurity is not compromised by bringing in any malware/viruses at updates of software or via the use of an external lap-top, mobile phone or USB-disks, etc. For such purposes, there is a need to have a cybersecure process, ensuring that no malware or viruses get into the target environment, complemented with trainings of the service engineers carrying out the on-site service and maintenance.

Thus, there is a need to have appropriate documentation, including cybersecurity, to provide the necessary guidance at installation, configuration, commissioning, and updating, etc., during the whole life-cycle. A further benefit is that the support technicians will get less questions and can focus on what requires a support technician's full attention instead.

At the end of the life-cycle, or the cease of use by a customer's object owner, required are instructions for how to delete and wipe IPR and data/information, and how for instance replace this with factory settings or other void contents. To have a function in the IoT product that does this, including providing a verification note at the end that all data and information etc. is deleted/wiped and/or replaced is appreciated by all involved. Further, an instruction for how to recycle the IoT product is needed in case some parts may need to be destructed or separated from each other. Observe that this all goes for all locations where IPR and data or information etc. are stored. This may include not only the IoT product itself, but any cloud services or servers and any intermediary steps used for transmitting data from the IoT product. Users at customers commonly have IT- and OT-policies with rules and an information security life-cycle management scheme which together stipulate how to decommission and end of life various assets within the IT- and OT environments. In some cases, full physical destruction may be required of memory cards, disks or other parts in order to ensure that nothing valuable in terms of IPR, data or information, are exfiltrated to competitors or other parties.

3.6 Test requirements

The testing of an IoT product is important for the functionality and 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 tend to that some matters are built into the development and test environments (which may require some development efforts and time). Thus, various forms of automated test suites, and test rigs, etc., should be requirements part of the initial requirement specification. Further, the test suites and rigs need to be continuously improved during the IoT product's life-cycle. Finally, all functional requirements as well as cybersecurity requirements shall be testable.

Various types of tests need to be compiled together to achieve a solid and stable IoT product as the outcome. Below, there are a number of potential groups for test requirements, which may be considered while drafting a test specification and test plan, to reach as a good test coverage as possible:

- Planning and overview of test coverage – will the IoT product comprise different configurations of hardware, software, and potential cloud services/servers or other additional services?
    - How large test matrix is required to achieve an adequate coverage?
    - Porting to various platforms – are the target platforms similar or different?
- Functional testing
- Testing and review/walk-through of potential additional services, processes, and structures
- Tests to ensure that all functionality (and services, processes as well as structures) are cybersecure
- Performance and scalability
- Test of documentation – are the set of documentation complete and correct?
- Test automation – test suites for cybersecurity, functional requirements, and performance/scalability/overloads
- Test rigs – what is needed to efficiently execute the tests? Can the test rigs have prepared configurations which automatically can be set?
- Penetration tests – for this an external party can be advisable – penetration tests are needed on a regular basis 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 automating, using test suites and test rigs, this will be faster and more efficient

If penetration tests and vulnerability scans discovers issues, this should generate a requirement for development or be managed through maintenance or upgrades. Well-considered test automation enables to test fast and that it is possible to repeat tests many times and that manual testing can focus on test cases which are hard to automate. The result of that is a good test coverage and that there is time to do a lot of testing during a development cycle. If an organization uses a platform to build IoT products upon, a sub-group of the testers can focus on testing the platforms base functionalities allowing the testers of the IoT product to focus on that and not the underlying platform. There are a number of publications regarding development of cybersecure interfaces and API's, and large cloud service providers and OWASP, with its Top-10 lists, share a lot of relevant readings and publications on their web sites. These can provide relevant input for developers and testers to craft test cases and test suites through the provided descriptions of common cybersecurity problems, weaknesses and cyberattack patterns.

3.7 Maintainability over time

– planning for updates, upgrades and migrations

Commonly, the longest phase of an IoT product's life-cycle is when it has been installed and commissioned at the customers' users until it is de-installed and potentially recycled or continues its life in some context elsewhere. It is a competitive edge to have an IoT product, which can be supported, serviced, maintained, and updated in an efficient and cybersecure manner, not only in terms of self-preservation but also to enable the whole value-chain to be profitable and keep the IoT product's total life-cycle cost interesting for all involved. In order to do all this, a training and education package may need to be developed for both internal and external use. Further, training and education for users at customers can be considered as an add-on service. In case there is a high attrition rate of employees, the training and education package becomes even more important.

To maintain an IoT product is not always straight forward to do and may require to be well considered to be both efficient and cybersecure for the target contexts. If an IoT product comprises 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 which are executed as a mix on-site and remotely – all this together provide a complexity and requirements for maintainability.

For an IoT product to operate and function well during the life-cycle, it will need either already from start to have adequate capacity hardware-wise in terms of processor, memory and storage, so that it is possible to later on add and upgrade firmware, operating system, platform, any software packages used, and open-source software which grows and application code. New extended demands on cybersecurity, which occur with regular intervals, will likely require that the hardware need to be able to endure significant more load compared to the initial situation. An alternative is to have the hardware as exchangeable modules, but then this will require that there are enough such modules later as they are needed. Many manufacturers stop production a few years after the initial model is introduced on the market and move on with new products and modules. Thus, this must be planned for and to start with a hardware configuration which barely meets the current capacity requirements will probably cause more problems and costs compared to if a hardware with better capacity had been selected from start.

As an inspiration, in particular from mechanic/electronic product development, there are concepts regarding “design for maintenance” together with a number of related “design for X”-concepts, such as “design for manufacturing”. In case it is hard and complex to plan for and execute maintenance and updates, etc., this will likely get unnecessarily costly and the IoT product will lose competitiveness. If maintenance and updates are fast and straight forward to do, any stop times in the operation environments will be shorter (unless there are redundancy to provide continuous operation).

Something that is often forgotten in early IoT product development is the data and information generated and stored for a long time. What data formats to use, and how can data be extracted and move to another supplier’s cloud service/server if the object owner at customers (i.e., the contractual party) own the data and information and in the future wish to move it elsewhere? To then require a hefty fee will not render any goodwill and nice comments as customers and users meet at industry meetings, conferences, or trade fairs. If an IoT product has good functions for migration from one data format to another and it is possible to extract and exfiltrate data and information (with help of meta data) to another context – then there will be good or excellent remarks.

3.8 Quality-level and what affects the level?

The quality-level of an IoT product is affected by many factors in relation to expectation from those of the users at customers and the price of the IoT product. In this handbook, the IoT product’s life-cycle is central and thus the quality-level needs to be kept at an adequate level, above the customers’ expectations, until the end of the life-cycle. Thus, it is not the quality-level after the installation and commissioning that is the big deal in case the quality-level deteriorates due to poor maintainability and inefficient or too late maintenance and updating. The cybersecurity, which is closely related to maintenance and sometimes also time-critical updates, is a part of the perceived quality-level. Thus, if the cybersecurity-level is or gets too low, the usage of the IoT product is disqualified in a number of contexts.

Further, a weak ownership of object owners or no budget for maintenance at customers affects the quality-level, directly and fast, of an IoT product (in case there is a need to maintenance and updates etc.). Unfortunately, there are many IoT products, and other production assets, which has a harsh life-cycle with no or little attention and care leading to fast deterioration that may cause disruptions within product- and distribution processes or other types of operations. In addition, a neglected IoT product may hold weaknesses for a long time, which in worst case can be used by any form of threat and cause disruptions, data leakage, malicious encryption of the IoT products data and information, etc.

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

3.9 Requirements from industrialization

To industrialize, or prepare an IoT product for more or less large-scale manufacturing, and further get the rest of the value-chain (needed to add value to customers) going is not easy. As a matter of fact, it is pretty hard to do all completely right from start and usually this requires a bit of trial and error to pave the way. During the industrialization, there are many steps and actors/stakeholders involved and this exposes an IoT product. Thus, physical security and cybersecurity is a must and having reliable technicians and production workers is a hard requirement too. In case there are many involved, this will be hard. A question to pose now is what to do by ourselves and what should the other actors in the value-chain do to achieve efficiency without risking the IPR developed as the IoT product is about to enter the market and meet the users. If too many have access to sensitive information or secrets, this is not likely to remain confidential for long. A further question to pose is if the value-chain can be outside of Sweden and EU from both physical security as well as cybersecurity reasons, and if there are dependencies to suppliers that may cause time-delays for manufacturing/production (i.e., supply-chain problems or transportation squeezes alike during the COVID years).

The requirement analysis should comprise some kind of design for manufacturing requirements to ensure that the IoT product is as easy as possible to manufacture, assemble, to quality test (post manufacturing/assembly) using for instance a test rig and/or test suite. To only manually test a few, such as 3 out of a 1000, is not a good strategy and it is better to automate the final testing and cover all. Then one knows that all IoT products that meet the customers and users are OK. If the volumes are small or mainly made by hand, the test automation is not as important as at large volumes, if the manufacturing/production is rational and simplistic and causing less defects and thus lower level of scrapping or time-consuming post operations to rectify defects. Unnecessary complexity in the manufacturing/production and testing of IoT products costs bot money and efforts. Thus, try to simplify and, if possible, automate as much as possible to achieve the potential benefits. Further, this is a must if the competitors do it.

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

4. Suppliers' process to pick up all requirements, achieve an adequate requirement specification and finally to verify all the requirements

To consider, if they can bring any value, are the numerous groups of requirements as well as specific potential requirements brought up in the previous chapter. To address requirement engineering with collection and analysis of requirements in an ad hoc manner increases the likeliness that important aspects and requirements are missed out. Thus, it is necessary to have a clear and structured process at IoT product suppliers (and perhaps also at the rest of the value-chain) which regularly brings back feedback on how the IoT product is performing and fulfilling the expectations of customers and users. To collect a complete set of requirements is not easy and this is outlined in the previous chapter as well. There are many aspects to consider and often there is a need for prioritizations if the initial set of requirements is larger than the capacity (and timeline) of the first development cycle. Therefore, a process for structured collection and analysis of requirements is necessary and that requirements which not are selected for a development cycle is kept in the process for the next cycle or minor upgrade/patch. In order to support a product manager and all involved in the development of an IoT product, a roadmap can be used to visualize, on a timeline, for instance the coming three year's development cycles and what major requirements/changes these will comprise. Such a roadmap should be dynamic and kept updated depending on what happens within: technology development, the own vision for the IoT product, customers' needs and expectations, and the surrounding world. The roadmap is a good tool to use when regularly communicating with important stakeholders in the value-chain so that they know about the main planning and what to expect. Further, use of a road map can facilitate allocation of budgets and procurement planning at customers' object owners.

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 the product managers and others involved in the requirement engineering have a homogenous group as customers and users, it may also be possible to get feedback and verifications of roadmaps at a regular basis. There are various methods 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 potential customers. Further, there are examples of handy frameworks in chapter 10 (for instance for municipalities, counties, and national states as well as marine users). It is likely that additional industries will do similar frameworks, etc., in order to craft common requirement processes and enhance the quality-level of such. Within Sweden, the Swedish Civil Contingencies Agency has crafted a high-level guide for critical infrastructures, which may be applicable for any IoT products targeting such contexts. EU and ENISA has also crafted a number of useful guides regarding cybersecurity for IoT and automation/control systems as well as critical infrastructures. These guides target both the private and public sectors.

The frameworks and all other publications are great reads. However, what is required is thorough and elaborated work by product managers and others involved for to pick up as a complete set of requirements as possible. Further, needed is also to prioritize and scope the set of requirements timewise on a timeline. There are no short cuts, but there is some help such as this handbook to grasp the picture and to work in a structured and systematic manner. Often, it is good for organizations to have a common process to enable structure and a systemic way of working as many of the involved can have different perspectives. This will improve the ability to capture the big picture and achieve as a good set of requirements as possible. Lone heroes, no matter if these use a process or not, will get a tough time and will not be able to meet all stakeholder and persons of interest to collect the requirement input needed.

Public procurement

Concerning public organizations and operations within EU, procurement of IoT products and potential add-on services requires that the laws regarding public procurement are applied (if the total amount exceeds a limit or the own decided limit). A procurement process made according to the public procurement laws will make it more difficult for IoT product suppliers as this hinders and slows down an often-needed frequent dialogue between procurement specialists and those who will install and later use IoT products. Thus, the necessary feedback and verification of requirements will initially be hard to execute in a rational and effective manner. As an IoT product is procured and is to be further developed, these initial barriers are not a significant problem anymore and it is possible to conduct a frequent dialogue between the parties. Preferably, this should 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 for to reach 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, lessen the own costs and efforts required to complete a public procurement process.

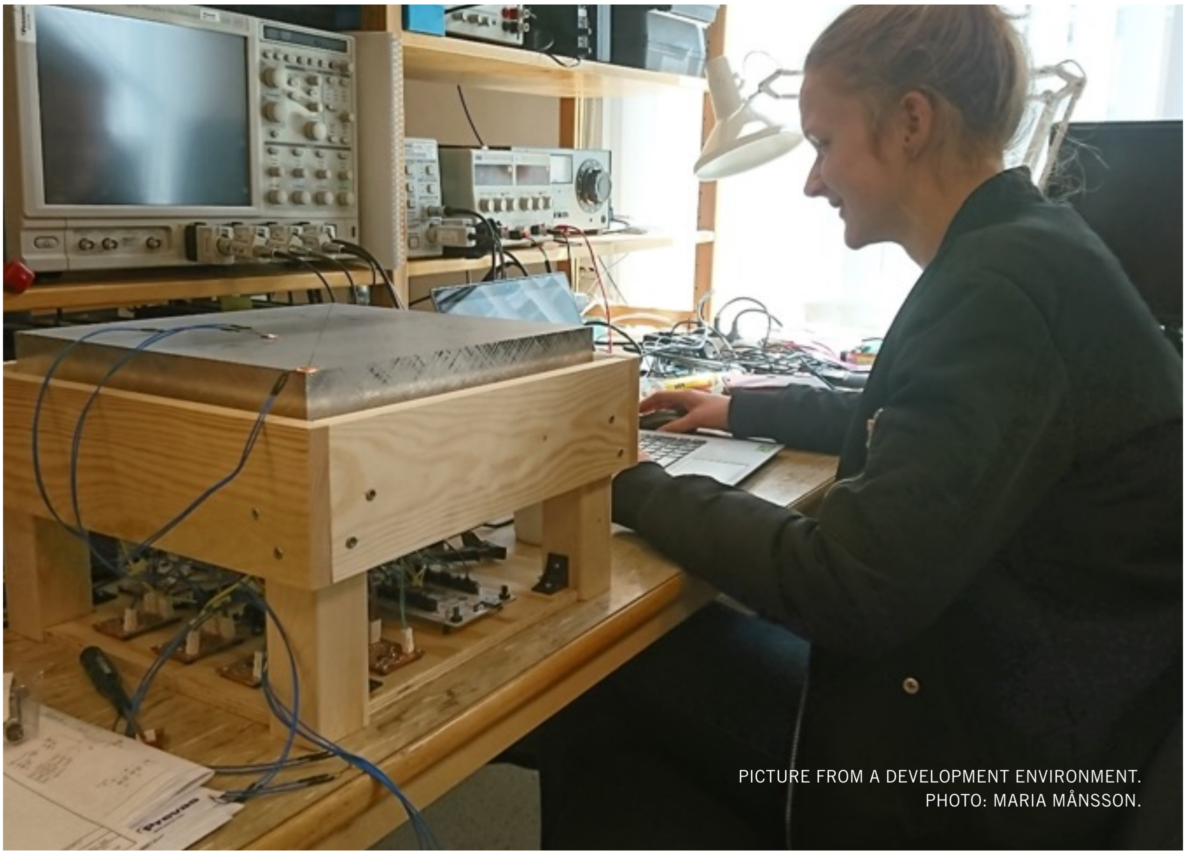
See chapter 9 for concrete examples of set of requirements and background information related to different use cases.

5. Cybersecure development

The actual development of an IoT product is just a small, but important and recurring phase, in the IoT product's life-cycle. Usually, there are a number of development iterations over time, for to make improvements and manage problems, resulting in regular new versions and updates/ patches. This will continue as long as the IoT product generates income and is possible to maintain and further develop. As the profitability is down or negative, the suppliers commonly raise the maintenance fee for customers (for to continue the 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 earlier mentioned: hardware, software on different levels (firmware, operating system, applications, databases and more frameworks on top of this), cloud services/servers, manual or automated services conducted on-site or remotely, and various processes and structures needed. Of course, there can be a lot more. However, all this puts requirements on the development process regarding the coordination of a number of commonly parallel development sub-processes whereof some need to have loose or very tight integrations. Unless these are well coordinated or have clear development contracts or standardized interfaces regarding how they shall fit together and function together, it is likely that there will be problems later on with poor results, drifting costs and low value created. The photo shows a development environment comprising measurements and test tools for IoT products with focus on hardware- and software integrations.

Besides to work efficiently, an environment as in the photo also needs to be cybersecure. The cybersecurity is needed as otherwise why would we make an effort and spend a lot of funding if someone else just can steal/copy the ideas, blueprints/drawings, patterns, code, documentation, additional IPR and patent applications. Further, not wanted things or code can unauthorizedly be added, data stolen, the development process disrupted and later on also the customers' processes disrupted or equipment encrypted/destroyed. Thus, a development environment must be protected and the security level depends on what is in it and, of course, how much it costs to develop and what profits that can be generated. There is a big different for an IoT product which is projected to generate revenue of a few million SEK compared to another one with billions of SEK, as well as the target operation environments are domestic or critical infrastructures. An analysis is required to map out what needs to be protected, what are weaknesses, threats and risks (see sections 3.4-3-6). Based on the analytic result, the cybersecurity-level for the development environment can be concluded. Common ingredients are segmented networks, encrypted communications and data, access control, multi-factor authentication, and authorization schemes for what different roles can do and if certain tasks require the four-hand principle (i.e., being two persons 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 with integration need. Anyways, this is just



PICTURE FROM A DEVELOPMENT ENVIRONMENT.
PHOTO: MARIA MÅNSSON.

the simplistic part and the harder part remains in the form of:

- To work 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 adequate protection and only be accessible and changeable in a controlled manner by authorized personnel. In some cases, changes should only be committed post an approval process or review (such as for software code or blueprints/drawings). To achieve the above, the following may be needed:
    - Train the development teams in cybersecurity and cybersecure development – know how to protect the own IPR and develop cybersecure design, code, ability to craft test cases for cybersecurity and automated test suites/test rigs including security tests (for such purposes OWASP's top-ten lists may be a good starting point together with similar ones from major software or hardware providers).
    - Ensure to have control of which requirements or limitations there are in potential open-source code or open design to be used, and store copies of such locally for future use if they disappear from Internet (as well as to have control of which version is in the IoT product).
    - Efficient testing of functional and holistic requirements (i.e., cybersecurity, digital preservation, quality/stability, availability, usefulness) as these often are connected as the holistic ones cut through all – this

requires a wide technical competence and understanding of test requirements (see earlier in the handbook) and scalability of the testing. It should be considered how a lot of testing can be completed with few persons 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 too). Naturally, security test tools should be part of the automated testing, which will result in that more security tests are executed during the whole development. Some of the tests can be executed during night time or in other time zones in order to shorten the total test time in calendar days – which makes to the whole development process faster.

- Use cybersecure development tools and review open designs, frameworks, libraries or open-source code that are used. Any open designs and frameworks should be analyzed and tested prior to being inserted and used, and may further need to monitored over time as the quality tends to become lower and the contents get additional contributors (which increases the risk of poor and dangerous code additions to the code base). This is not an easy task and is a large task over time – thus, resources to do this are needed. One should always map out the background of open-source code and open designs in terms of history, how much updates are made and by whom, is there continuous development and improvements, or is it dead code?
- Have a cybersecure test environment that no externals can change and make test results look good although they are not (i.e., falsify test results and reports).
- Use cybersecure collaboration tools for sharing of documents, instant communications and online meetings.

The above will require a bit of work, effort and cost compared to if neglecting cybersecurity. However, the positive effects may be increased efficiency in testing and improved test coverage as well as less problems and unnecessary costs incurred later on during the life-cycle. Further, such a set up and structure can be re-used for other development projects related to IoT products.

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

CLOUD-BASED CYBER SECURITY SOLUTIONS.
PHOTO: ADOBE STOCK.

6. Post development

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

A driver for cost and also a potential cybersecurity problem is if support, service, maintenance, additional supportive processes and services, such as optimization of hardware, software and operations, are not well thought through and there is low knowledge regarding the target environments for the operations of the IoT products. A supplier of IoT products may need to have a few options to manage the most common operations environments and use these to make any special adaptions needed using professions services (i.e., consultancy services). A few things to consider are how this all shall be managed – do it all on-site, mix on-site and remote work, do most of the work remotely except exchanges of hardware and potential mechanical maintenance? See section 3.7 for additional information on these requirements.

It is a good idea to provide object owners and users at customers a recommendation for a cybersecure operations environment, to emphasize the importance of this if their current knowledge on this area is low and focused on the operation's processes. This should start already during the business development/sales phase and will normally not be a problem but on the contrary this signals responsibility and professionalism. If not bringing this up, or hiding it, for object owners and users at customers, this will later create problems for those who will be involved after the development phase of the life-cycle. Preferably, the documentation of the IoT product (see section 3.5 for requirements regarding this) should comprise cybersecurity within the running texts or brought together in an appendix. Besides the installation and setup, it should be described how to verify the cybersecurity-level using instructions, procedures or small utility applications that can be distributed along the IoT product. Helpful figures, which comply with the accepted cybersecurity standards and guidelines, should be part of the documentation as they help all involved. To consider is that if an IoT product has its own network or network segment and is connected to a larger network at the customer's users, then the larger network should have the same (or higher) level of protection required by the IoT product. Else, additional cybersecurity protection (i.e., controls) may be necessary to add. Further, it is necessary to outline the communication channels and which protection level for those that are needed/recommended, what and whom that can have access to the IoT product as well as what those with access are authorized to do (see example on such requirements in section 3.2.3).

The forthcoming EU Cyber Resilience Act will likely pose requirements on monitoring as well as continuous monitoring if the IoT product (or offers where such are involved) developed is or becomes vulnerable. A potential consequence of this is that, during the whole life-cycle, there is a need to provide updates to mitigate any vulnerabilities and that these updates can be distributed and installed in a cybersecure manner.

To monitor an IoT product, or potentially a whole fleet of IoT products installed at customers, is becoming more common in order to collect requirements (and learn what works and not works) and/or as an add-on service for predictive or condition-based maintenance and optimizations. As earlier mentioned, it is a good idea to separate/segregate the data pertaining to how an IoT product is used and further potential data collected about processes and quality-levels. To get such data, which can be used within fleet management functions and provide an overview if there are any weaknesses in the design, specific components, the whole concept or recurring problems (such as manufacturing flaws from a certain production site or too harsh handling) is an important part of cybersecurity but also to get specific understanding of stability/robustness, availability, what is worn/torn at different usage levels in various contexts. The level of wear/tear for an IoT product may not cause the same need for maintenance if it is used in a constant damp and dusty mining environment compared to usage in an outside environment at a road or railway where the weather changes. Thus, the data set should be considered and if different groups of data will be generated that can create value for the customers' users as well as the 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 customers and 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, etc. To achieve this afterwards is hard, and this discussion with customers should be 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, changed configurations or optimizations shall be retrieved by the IoT product from a cloud service/server, it can be made using a communication channel opened up by the IoT product as it sends data outwards (this enables to keep a good and simple cybersecurity with less connections initiated from the outside). The data from an IoT product can, depending on needs and cybersecurity requirements, as well as what is acceptable by the object owner at customers, be stored within the IoT product (that will require RAM-memory and disk or memory

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

card), in a local server at the object owner, in a central server at the supplier or other part of the value-chain, or in a cloud service. If wanted is to use an external cloud service, operated by for instance Microsoft or Amazon, the cybersecurity-level needs to be set up and configured correctly as well as regularly verified. A verification should always be made prior to starting to use a new clod service, or instance of such, and then on a regular basis so that applicable laws, regulations, and recommendations are OK and aligned with what is wanted. Unfortunately, many cloud service instances have flaws in the cybersecurity due to wrong configuration and set up in combination with the cybersecurity-level is not regularly verified.

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, to also consider is what must be conducted on-site, a mix of on-site and remotely, or if a majority (except what must be made physically regarding maintenance and repairs) can be conducted remotely. It is helpful wo draw up and visualize these processes to find out any collaborations and data sharing required. If the process caring for distribution, fetching and installing software updates can be executed smoothly and automated (without any virus or malware infections), it will be a great benefit for all. It is common that some customers have a test environment where all updates and upgrades are tested prior to being installed in the operations environment. These tests are often from a week up to six months long. Some customers allow that operating systems and firmware are updated without testing if the supplier of these is trusted and have a solid track record without mishaps. However, it is recommended to find the facts about this and draw up the processes needed and involved. If a customer's policies do not allow any external connections from the outside, it gets more complicated, but an option then is to use the same communications channel as data is transferred out to also fetch any data, configuration changes, software updates/upgrades, etc. If this is not possible, more things must be done on-site and this also requires routines to ensure that no viruses or malware are brought in along with the software and equipment physically brought in to object owners at customers. The object owner decides how data potentially can be exfiltrated, and it can be good to have for instance three options for how to do that in case one or two of these are not acceptable for the object owner. To have a continuously open connection for exfiltration of data is commonly not acceptable unless it is required for very quick reactions or changes. Further, some operations environments cannot have continuous connections open but only open connections at regular intervals. Thus, various middle-steps and buffering of data (for instance using a buffering gateway having some firewall functionality above the IoT product or built-in buffering into the IoT product itself) combined with different data transmission mechanisms (for instance 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, secure OPC-UA, mobile text messages, or other protected transmissions) crossing various types of networks and topologies may be needed to achieve a robustness and not lose any data while in transit. Commonly used industrial protocols[9] for collection of data and/or automation/control functionality are Profinet, Profibus, Modbus, OPC/OPC-UA, etc. OPC-UA is being developed in terms of cybersecurity and also has an information model which can be used to standardize for developers and object owners at customers. The smaller number of middle-steps and buffering, the better and easier to maintain availability and the cybersecurity-level. All middle-steps and buffering need to be monitored to detect any stops or problems. Further, customers do often not want, within sensitive operations environments, to have any mobile communications using SIM-cards as this can open up for cyberattacks.

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

This should be possible to find in the customer's policies and internal standards. If using mobile communications, this needs to be managed by for instance keeping this in a separated "island" in the network or having equipment (such as a diode) ensuring only outgoing network traffic.

In case it is OK to use controlled connections, initiated from outside of the network, these need to fulfil the customer's policies and standards regarding cybersecurity (this goes probably for both IT and OT as a connection likely will traverse both the IT- and OT environments). Preferably, the best is to be flexible to use the customer's standard external connection options and not limit this to a specific own solution. Then, if it is possible to access/reach the IoT product after using the customer's solution for external connections or there is a an additional gateway or firewall with an extra VPN-connection – it is usually possible to get it to work. The customers often limit the external connections. It is necessary to limit the possibilities for external connections, in particular if initiated from the outside, and it should be swift to shut down/terminate an external connection, for a specific user, or for a group of users. For suppliers of IoT products to be aware of, these are common configuration parameters for external connections initiated from outside:

- Requirement for fulfilled process for identification of user and set up of user account (i.e., enrolment) and potentially additional requirement on having passed a training on cybersecurity (i.e., with approved test result) to allow a user to use an external connection from outside of the network.
- Time-based access (when during the day and what weekdays are 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 the access be on a low or high level – what is necessary for to be able to conduct what is needed? To limit low-level access is harder (e.g., IPSEC VPN) compared to high-level access (e.g., SSL VPN). Many solutions for external connections from the outside often comprise both the low- and high-level ones, and to only have low-level is not to recommend. Thus, suppliers of IoT products need to aware of this and preferably not depend on having such a low-level access solution but also be able to cope with a high-level one.
- Cybersecurity-level of the device that is used to connect (e.g., end-point-security).
- Time limitations for access. The access should be time limited and require a renewal within 1-12 months. If not renewed, they shall be automatically inactivated and removed (to clean out old access set ups).
- If all the above is OK, should an external connection be possible to establish or does it firstly need approval and be opened up every time (e.g., by a user at the customer who clicks a box in an interface and approves) and that it is possible to, whenever during an active connection from outside, terminate it?
- Time limitations for sessions – common is to maximize the session time for external connections to 30-60 minutes unless otherwise is needed. It is risky to have unlimited session times and it is not recommended.

7. Monitoring of the IoT product throughout its life-cycle

Although already mentioned a few times, the monitoring of an IoT product's general status and need for maintenance is important enough to have its own chapter. As a supplier, or if it is another stakeholder or actor within the value-chain that assumes this responsibility, it is a great advantage to be able to follow up on an IoT product over time. However, this requires that some pre-conditions are met. One pre-condition is to agree with object owners at customers to be able to get the data needed, be able to exfiltrate it, and be able to (and allowed to) use the data for this purpose. A way to start is to craft an information model and map out the processes where the data will be used prior to proposing an agreement regarding this with the object owner. If prepared, it is easier to explain which data are needed for what purposes and this helps object owners to see the value and may prevent a reaction that "our data" shall not be 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-levels (e.g., tolerances for input materials, measurements during and after process steps, and tolerances on the output) as well as optimizations can be offered based on if there is access to such data. Figure 5 comprises an example where different groups of data have been separated and the supplier own what is related to monitoring and status of the IoT product, the object owner or other suitable stakeholder at the customer owns what is related to processes and quality, and the last is person-related data which needs to be handled according to the GDPR within EU and corresponding privacy laws in the USA, India, China, Australia, etc.

A proposal, earlier mentioned too, is to clearly divide up/separate different types of data, which are stored in the IoT product prior to being transferred/exfiltrated further on using different tables in the database or even different databases. Probably, the simplest to do is to use different tables in the IoT product as an IoT product may not have the processing capacity to run too many processes in parallel. Other impacting factors are the cost for potential licenses, if it practical and doable, and if there are any such requirements among 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 to manage in an agreement or contract between the sales representative and object owner or another adequate role at the customer. Further, a division/separation also enables to have different cybersecurity-levels (e.g., encryption algorithms and key lengths) for the groups of data and also be able to improve access rights and authorization of what can be done with the data.

At the cloud service or server side (e.g., a local server operated at the customer or a central server operated at the supplier) there are some matters to consider as well. Is it OK to mix customers' 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)? The latter is often referred to as "multi-tier" or "single-tenant" solutions and increases the complexity and costs for operations and licenses. However, if it is required by the object owners at customers and they pay for it – it may be necessary to have.

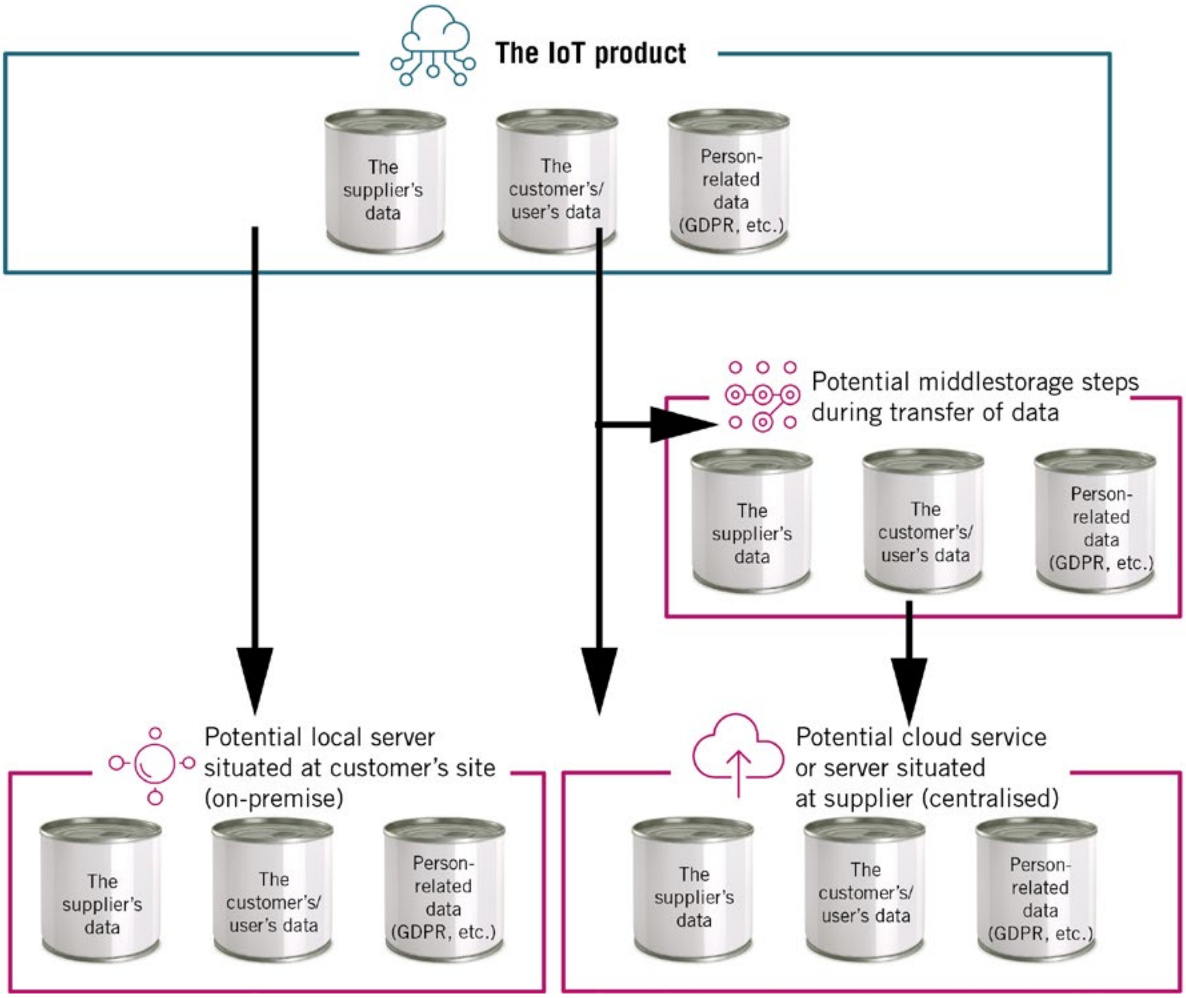

The IoT product
The supplier's data
The customer's/ user's data
Person-related data (GDPR, etc.)
Potential middlestorage steps during transfer of data
The supplier's data
The customer's/ user's data
Person-related data (GDPR, etc.)
Potential local server situated at customer's site (on-premise)
The supplier's data
The customer's/ user's data
Person-related data (GDPR, etc.)
Potential cloud service or server situated at supplier (centralised)
The supplier's data
The customer's/ user's data
Person-related data (GDPR, etc.)

FIGURE 5 – EXAMPLE OF SEPARATION OF DATA WITHIN THE IOT PRODUCT, LOCAL SERVER OR POTENTIAL MIDDLE-STORAGE STEPS DURING DATA TRANSFER, AND CLOUD SERVICE/CENTRAL SERVER, WHERE THE SUPPLIER OWNS THE MONITORING DATA, OBJECT OWNER AT CUSTOMERS OWNS PROCESS- AND QUALITY DATA, AND PERSON-RELATED DATA IS KEPT APART FROM THE OTHER TYPES OF DATA.

There are fine opportunities to capture new requirements to develop new versions or generations of IoT products if focusing on monitoring and the data pertaining to general status and maintenance need. However, the necessary agreement and pre-conditions are needed to be in place. The progress can be made through finding what works and not works, if there are common problems, and if there are problems related to the same root causes of an IoT product. If finding such root causes, the product manager and object owner can, together with the development team and other suitable stakeholders, analyze what needs to be done to get a further value-creating and sustainable IoT product. In some cases, there can be a need for instructions or training of installers and users that are needed instead of design changes if these damage the IoT product through harsh handling or it is installed in the wrong places. Another aspect is to also put limitations for the usage so that an IoT product cannot break itself doing certain operations or movements. Thus, the monitoring need to be structured so that the collected data can be analyzed efficiently. Further, the data collected from those who conducts support, service, maintenance and repairs should also be collected to complement the data collected from the IoT product. To simplify the data management and analysis of the human-generated data, it can be handy to have an application where data can be grouped into standardized groups and areas, which can then be complemented with free text at the entry of the data. To only have free text reports will make the analysis and data management harder and require a lot of effort as then it is required to categorize and harmonize the data using some common measurability or scale (i.e., normalization) in order to be able to make useful analytic results and comparisons.

The monitoring and follow-up on IoT products can be extended further and it is only the imagination of the own development team's abilities that limit what can be achieved. The monitoring and follow-up can be extended with for instance self-tests and self-diagnostics, which are run regularly to check up on all components, parts, all mechanics, as well as that all functions are working, and tolerances are within the wanted ranges. As a complement to the physical and functional, use of automated and built-in test suites can be used to verify that the cybersecurity-level of the IoT product is OK or not. Further, procedures executed by humans can verify 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 collected, stored and be used for further analytics and follow-ups.

A possible next step is if the requirements on availability-levels are extreme and it is hard to physically access an IoT product for humans. 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 if the IoT product is built into structures, is situated below water (or far under the surface level), is in the air or space. To consider is if there is a possibility to use robots or drones (unmanned aerial vehicle - UAV) which can do or assist in the repairs, service, or maintenance, unless humans can be present or if it too dangerous for humans. Likely, there will be a lot of non-human interactions with IoT products in the future.

Fleet management as a concept is being developed further. Additionally advanced business models, where it is required that the supplier-side can keep monitoring and control of what happens with what is installed at customers' users, will increasingly rely on fleet management functionality. It may not be an IoT product that is sole, but a product integrated with services, a Product-Service System, or a function that has been sold with an agreement regarding contractual parameters as: subscription, promised level of availability, promised level of improved productivity, risk sharing and revenue sharing from the IoT product's improved value-creation above a certain threshold. To be able to pull off all this, it is needed, besides ability to monitor and follow-up, to improve what can be accomplished remotely except what is required to be executed on-site such as physical service and maintenance (often referred to as MRO – maintenance, repair, and overhaul). Further, to consider are also potential later re-use and reinstating, through re-manufacturing or re-furbishment, of parts of or whole IoT products. This can improve the profitability and sustainability at the same time as lessening the environment impact. Commonly, the fleet management functions grow organically with time as needs and possibilities are discovered. Below, there are some examples of potential fleet management functions for monitoring, follow-ups, administration, and configuration from distance:

- **Prepare**, at the supplier of other suitable stakeholder, installation and initial configuration, either for an individual IoT product or a group of such with plug-and-play. This requires that the IoT product needs to be aware about some matters already from the start as it arrives to the customers' operations environment. A preparation with installation/configuration should be made at the supplier or the other stakeholder of the value-chain. Further, the IoT product should be prepared with where it can automatically fetch/download, in a cybersecure manner, the full installation and configuration.

- **Remote administration and configuration** – centrally 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 too and be synchronized with various asset management functions below.
- **Emptying/removal/wiping of data and deinstallation** – the ability to remotely, at the end of the usage in the customer's operations environment or end of the life-cycle, empty/remove/wipe IPR and data from all parts where such are or have been stored (i.e., applies to the IoT product, any middle-steps and middle-storages, in cloud services or server parts). It should be possible to control if 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 last functionality should require that more than one administrator do it, i.e., it should require cooperation of 2-3 people with adequate authorizations to minimize mistakes and any sabotage. Further, there should be a verification notification (and logging) as such operations are completed. Read more on this in the following chapter.
- **An IoT product's functionality and operations-level should be possible to limit** in case of problems (e.g., graceful degradation) to lessen the load or in worst case automatically initiate a shutdown to avoid serious and costly damages or breakdowns. Depending on context, such decisions may sometimes require a human decision, but a high level of automation of such decisions can save dear expenses or in worst

s.slice(0, -1)), s
interface.state.filters, function(i, s) {
!== i && (1 += i + "_" + t(s),
face.state.filters.hasOwnProperty(
face.state.filters.price_range
user_interface.state

CODE DATA ON A MONITOR.
PHOTO: ADOBE STOCK.

TECHNOLOGY NETWORK BACKGROUND
PHOTO: ADOBE STOCK.

case to have to buy a new IoT product. If identifying such problems at an early stage, using the fleet management functions, the users/operations at the customer can then make decisions for how to handle it or if a temporary replacement is needed until the primary one is good to go again.

- **Collection of feedback and complaints from the customers' users on the IoT product** – if there are no other channel to the product manager, for instance via a web site, social media or user groups, for to collect feedback and complaints, the fleet management functions can potentially be used here as well. The feedback and complaints can generate new development requirements or ideas for improvements as well as the correction of errors or unclarities. The use of a standardized input for different areas and functions (using normalized measurement data and estimations) with possibility 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 the IoT products are installed and operating. An overarching asset management system should be connected to the below potential systems/functions pertaining to change/configuration/obsolescence management as the asset management is hierarchically above these:
  - **Change management** – store data about planning, execution, and results from changes in the operations (e.g., re-configurations and set-ups plus the context of operation).
  - **Configuration management** – store configuration data to know what hardware and components each IoT product has, which versions of software, and when updates/upgrades/patching are made to what version of such. This can save a lot of time and facilitate planning of updates/upgrades/patching and also enable searches at ongoing cyberattacks when there is a need for finding out if there is a certain software and what version. An example is the recent log4j issue.
  - **Obsolescence management** – this pertains to planning of storing of and how many spare parts/components and old versions of software that need to be available and for how long. This is expensive and binds capital, which is not certain to convert to revenue, and may also require a lot of space (which also may cost a lot). The obsolescence management can be a good and profitable part of the business if managed adequately and optimized.

To get a good overview and basis for decision-making, there is a need for a summary of that the status is, what happens and if there are any acute matters to take care of. A fleet management system or function can have a cockpit or management view, from where it is possible to drill down to further detailed operator views for those who continuously monitor and manages problems within the fleet of IoT products.

8. At the end (or a new start) of the life-cycle

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

Prior to the start of the operational phase of the life-cycle, it is hard for suppliers of IoT products to foresee how the actual use and operation will be as well as which users that will use/operate the IoT products. Further, it is also hard to foresee new areas of use and potential extensions of requirements, etc., that materialize and can be capitalized upon in terms of business, social, or ecological sustainability. In addition, it is rather common that object owners at customers wish to extend their agreements/contracts far longer than the supplier would like to. This is due to that the object owners find the IoT products to work well and still create value in an environment where new investments mostly are made as assets break down or cause to high risks or physical danger. To extend the life-cycle and offer support, service, and maintenance for an IoT product will cause an extra load on the supplier and value-chain. To compensate for this, it is common to raise the price for object owners to reflect the extra load and costs as well as the possibility to have less focus on the recent IoT products.

As the world's resources are used up, new forms of thinking and concepts are getting adopted among suppliers and value-chains, which manages some sort of physical product or system. In order to improve the resource management and optimize the usage, with increased sustainability as a result, there are some potential variants for how to extend an IoT product's life-cycle. This is often denoted as circular economy, but lately also the concept elliptic economy , where the life-cycle's usage phase is extended further to lessen the consumption of the world's resources, has emerged and is being investigated by suppliers. To be able to reach such sustainability, a supplier should also consider which existing/improved/new business model to use, how should the foundational and cybersecurity infrastructure look like, and what knowledge and training packages are needed. Thus, the below should be considered:

- Application of plus-1 strategy, which may entail that one or a few functions are added, and other features are improved a bit so that the IoT product can continue its life-cycle and be sold a few more years to create value at object owners at customers. In particular, this can made for satisfied object owners. Such a strategy has often been used by for instance personal car manufacturers, where some models have been sold up to 20 years or more.
- Application of re-manufacturing or re-furbishment, and extend the life-cycle through exchanging worn/torn parts or components and potentially combining this with upgrades or parts or components required to improve the IoT product's functionality further on. A similar concept is re-conditioning, which encompasses cleaning up and potentially restoring surface layers and test that all are OK. Sometimes a few parts can be exchanged, but that is commonly not part of the

[10] https://www.ltu.se/research/Framtidsomraden/creaternity/Aktuellt/Elliptisk-ekonomi-annu-mer-hallbar-an-cirkular-1.224542

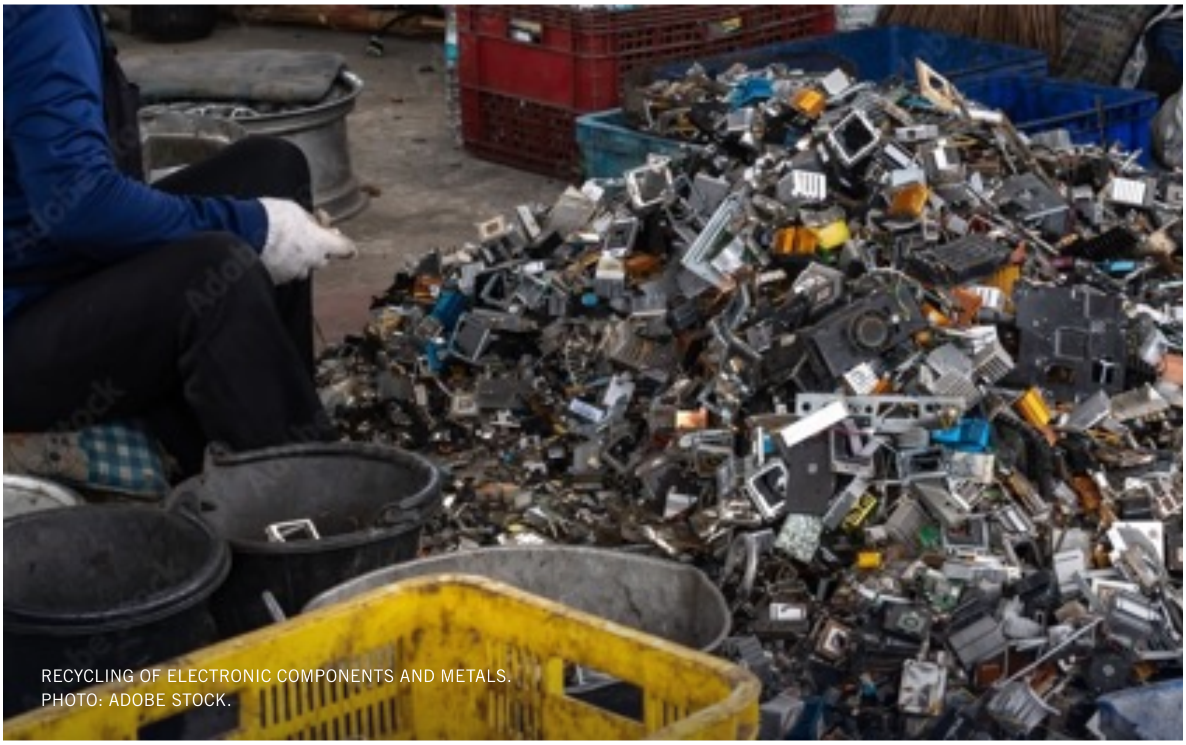
re-conditioning. Re-conditioning is applied by suppliers of used servers, network equipment, cars and mobile phones that are in good condition.

- Application of re-purposing, which may comprise using the IoT product for applications it was not initially intended for, and where an older version of an IoT product will be adequate.
- Application of down-cycling, which means that an IoT product can be continued to use 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. An example market is development countries.

The above requires that, at the end of the primary life-cycle, an IoT product is emptied/wiped regarding IPR and data/information or that such is replaced with factory settings or dummy contents. The picture below shows a part of the re-cycling process of electronics and metals, where IoT products should have been emptied/wiped prior to being input to such a process.

At the very end of the life-cycle, the documentation/user manual should comprise instructions for how to prepare the IoT product and its parts for end of life/scrapping/destruction/re-cycling without compromising any IPR or data/information (such as configurations, set-ups, recipes/programming, operational information as IP-addresses, etc.) to unauthorized persons. Thus, all mentioned need to be emptied/wiped regarding IPR and data/information as well as that it should be possible to verify.

To observe is that the emptying/wiping is applicable for locations where IPR and data/information are stored, which may include a lot more than just the IoT product. Cloud services, servers and middle-step storages used should be included too – and be possible to verify. Thus, it is favorable to have a function which empties/wipes all IPR and data/information at all places, concerning one IoT product, a group of such, one customers' IoT products, a group of customers' IoT products, or all customers' IoT products, at the very end of the life for an IoT product.



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

9. Use cases

It is hard, at an early stage, to get an understanding for and capture a complete set of requirements for an IoT product, as when it starts to be used new ideas and experiences are generated. To facilitate the capturing process, the usage of adequate and relevant use cases may provide a better initial understanding of the set of requirements for all involved in the development process. Chapter 9 is a continuation of chapter 4 and provides a few examples of use cases. Prior to starting up the development process, such use cases should be complemented with additional information regarding the operations/usage of the IoT product.

9.1 Use cases with concrete examples

Below, there are five different use cases ranging from domestic (home) to various professional environments. The purpose of the use cases is to enhance the understanding that the various contexts' requirements on cybersecurity are not the same. The more cybersecurity needed, the more it will cost to develop, test, certify, etc., later on during the IoT product's life-cycle. Further, the more functionality the more effort will be required later on as well for further development and maintenance.

To outline the use cases, a common structure has been used to make it easier to compare them. The structure is as follows:

- Organizational type – brief description.
- Operations/processes – introduction of the operations/processes to understand the set of requirements for the IoT product. The requirements may emancipate from: customers/users, laws/regulations, industry standards and other stakeholders.
- Type of IoT products and how these are used.
- Cybersecurity requirements around IoT products.
- Other – here is what else that can be of interest which is not already brought up

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. The domestic context gets an increasingly improved standard, which also applies to infrastructure in the form of Internet connections via fiber, cable-TV, or mobile networks. Most households have a low level of cybersecurity awareness and related knowledge about how to cybersecure the household and reach a hygiene level for cybersecurity.
- Many persons spend a lot of time in the household and use a variety of connected products, machines and systems. There are requirements for sustainability/recyclability, energy efficiency and cybersecurity. Further, there are also mandatory requirements for electric safety and type approval with CE-marking, and recently added also for personal data (GDPR), IoT-security for consumers (ETSI TS 103 645/TS 103 701) and the forthcoming EU Resilience and Cybersecurity Acts comprising expected requirements for a hygiene level of cybersecurity within digital consumer and professional products.
- In a domestic setting, there is an ongoing replacement of unintelligent home electronics and appliances, machines and systems to 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

MANY PEOPLE SPEND A LOT OF THEIR TIME AT HOME AND USE MANY DIFFERENT CONNECTED PRODUCTS, MACHINES AND SYSTEMS..
PHOTO: ADOBE STOCK.

A PROCESS ENGINEER.
PHOTO: SHUTTERSTOCK.

armatures/lighting. All these increasingly smarter IoT products are used to increase the comfort, ability to remotely monitor and control functions or control per automation (e.g., control by energy cost level), be able to learn the status of locks- and alarm system including water leakage. Thus, all this should improve the daily life and simplify as much as possible. There may also be instances of e-health or home care, which use sensors and safety alarms. In such cases, the personal data and its integrity plus availability are of great importance.

- The domestic context requires cybersecurity considerations regarding what the habitants want to protect. Usually, there are plenty of personal data, which should only be accessible by whom are concerned, which implicates that also mobile phone security must be part of this. There are many apps that collect 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 from cyberattacks and intrusions. Preferably, the protection should be made in layers starting from the Internet connection and inwards to prevent malicious actors to: destroy IoT products, learn if the habitants are at home, access alarm/surveillance system cameras, be able to open locks or disable alarm systems, plant encryption viruses, or use the IoT product as part of bot-nets. The hygiene level comprises having a competent firewall/router at the Internet connection and to preferably also segregate/segment the network or networks. If there are individual IoT products that need a higher level of protection due to sensitivity, such as alarms, cars, mobile phones, computers, building automation, these should be extra protected. Above the network, there should also, if possible, be protection by anti-virus or anti-malware solutions, local firewalls, etc. However, some current IoT products may not have the capacity for that and will therefore be vulnerable. At high requirements for availability, for instance at instances of e-health or home care as well as for alarm and monitoring systems, extra measures may be needed regarding the cybersecurity-level as well as possibly having a redundant Internet connection via fiber, cable-TV or mobile networks. Further, hardening of the network and IoT products should be considered to improve the cybersecurity-level. Hardening encompasses that not needed services are removed or inactivated, the communications is limited to only authorized and needed communications (i.e., not needed communication ports should be closed and, if possible, only the needed protocols allowed on the open ports and in between network segments). Concerning hardening, it would be good if the supplier had already from start hardened the IoT product and if needed it can be opened up at commissioning (i.e., secure-by-design). The main issue for households is the cost level, as an adequate level of cybersecurity costs, leading to that many households spend too little and get a poor hygiene level which in turn is not maintained over time. Another large issue is if the supplier has not developed an adequate level of cybersecurity, as it seldom gets improved over time. Further, it is good practice to enable automatic updating/upgrading and get cybersecurity updates installed timely (i.e., fast) and that a warning is issued in case there is something that are or seems not to be OK.

- In addition, a common sense of cybersecurity hygiene and basic knowledge what to do and not to do, are necessary. This should include: to not click on unknown links or files sent by unknown persons, to not open up attached files which have not been checked by an anti-virus solution, to not get conned/frauded by strangers calling on the phone, or by text messages/emails with links. This is also 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. There is often a possibility to apply a high level of cybersecurity, but this may require that the basic configuration is walked through, following reading the instructions, and be elevated using for instance stronger encryption algorithms and authentication level.

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

- Within manufacturing- and process industries there are often an administrative environment (IT) and another environment where the manufacturing/production is (OT). Further, distribution processes are sometimes connected to the OT environment with the manufacturing/production but are commonly partly or wholly separated. Previously, in many cases only the IT-environment was connected to the Internet. However, now it is common that OT environments are also connected and possible to connect to from the outside. Some OT environments still do not have any connection, or a poor one, to Internet. The cybersecurity awareness and maturity have always been satisfactory in parts of industries. However, the awareness and maturity need to be strengthened among almost all employees and the industries must organize their cybersecurity for both the IT- and OT environments as these are usually connected to each other.
- Many industrial companies and organizations have their processes operating outside of normal working hours, often run multiple shifts or around the clock, having only stops during one or a few weeks per year. The increasingly continuous the operations is, the harder it is to make any changes in the production processes and this requires detailed planning for all changes or new installations to be able to complete these within the planned stops. Further important is to be able to re-start and be operational as soon as possible again after the planned stop – preferably without problems or disruptions. For efficiency reasons, it is getting more and more common that suppliers and consultants need to be able to connect in from the outside in order to provide services. Further, many IoT products need to share data with both internal and external recipients. There are a number of sustainability requirements

posed on IoT products, for instance related to the surrounding environment, to have a robust and stable function, as well as being recyclable, energy efficient and cybersecure. In addition to workplace environment requirements, electric safety requirements and type approval with CE-marking, there are the EU GDPR and the forthcoming EU Cyber Resilience and Cybersecurity Acts with requirements for a hygiene level of cybersecurity for digital consumer and professional products.

- Within the manufacturing/production environment, there is often a wide variety of IoT products with for instance sensor solutions for monitoring and control of processes and production equipment. Further, common are also alarm/lock systems, building automation with ventilation/heating/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 bar-codes for production output, etc. Distribution processes also use IoT products to keep order of where output is and that the output quality is kept at a wanted level (e.g., moisture, cooling or keeping the right temperature) until delivered. Within distribution environments, the physical security is often lower than in the manufacturing/production environment and this must be considered properly. Manufacturing/production and distribution environments can be tough on IoT products concerning physical protection (i.e., environmental protection for water/dirt/dust/cold/heat, impacts and physical intrusion attempts trying to connect to internal networks via the IoT product) and cybersecurity.
- Within industrial companies and organizations there are protectable information in both 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 within the manufacturing/production processes are often the most important. Further, the integrity of the processes must be kept high and avoid variations, stops or disruptions, to ensure that the resulting output have an even and wanted level of quality. There are large amounts of information in such processes, whereof some can be confidential encompassing knowhow regarding processes and implementations, methods, recipes/patterns, programming, etc. Just to know if a manufacturing/production process is operational or not can be valuable. Thus, IoT products, such as sensors, measurement equipment, monitoring systems, and maintenance systems, need to have proper physical protection combined with a wanted least level of cybersecurity hygiene. If there are weak areas, these are where problems mostly occur. Regarding a hygiene level, the first to do is to segregate the networks into IT and OT and further to divide up/segment the OT environment into smaller segments to keep the processes apart and isolated to protect these from problems and only allow authorized communication in and out of the segment (as well as between the segments). Besides the above, the users should only be allowed to do what they must (and not more) and any external connections should be controlled and that data is shared only with the right recipients. In addition, monitoring of networks, patch routines, incident management, backup and restore processes, etc., are necessary to have. Unfortunately, many IoT products have poor inherent cybersecurity and it is not possible to upgrade or replace in a rational way. Thus, some IoT products should not be connected into the OT-networks but be in islands.

Another issue in OT environments is to manage third parties (i.e., suppliers/vendors and consultants) moving around in the environment, and to ensure that these do not bring in any virus/malware or connects “things” without having proper authorization from the OT-security responsible to do so. Distribution environments often comprise IoT products that are exposed and can be used as entry points to get access

INDUSTRIAL TECHNOLOGY CONCEPT. COMMUNICATION NETWORKS. FACTORY AUTOMATION.
PHOTO: SHUTTERSTOCK.

to networks and spread viruses/malware. Thus, these IoT products need physical protection and there should be control who can communicate with these too. Thus, the cybersecurity must be considered and kept up over time as well as at decommissioning when these may otherwise be thrown away in public recycling containers together with their packaging box.

In addition, IoT products should be hardened. This entails removing or inactivating not needed services, and limiting the communication to only what is needed on specific ports, applications and protocols. The supplier should do this hardening as part of the basic configuration, and that if wanted or needed some things can be opened up during the installation. General basic configurations for hardenings should be applied as general practice. The main problem for industrial organizations and companies is often lack of competence and clear rules on this, which may cause cybersecurity problems within the OT environment as a result. Another problem is that the cybersecurity in OT environments is underinvested compared to the IT-environment, which is somewhat strange as most value is generated in the OT environment. An additional, but smaller problem, is that suppliers' function warranties require that upgrades and patches must be approved/authorized prior to installation and that this often lags in time causing open vulnerabilities.

- Else, in general, needed is a good cyber hygiene and knowledge on what to do and not do. For instance, mobile phones must not be charged via USB-ports on equipment, to not use non-controlled media (USB-disks), to not

CYBER SECURITY RISK ANALYSIS TEAM REDUCES RISKS..
FOTO: ADOBE STOCK.

install unauthorized/uncontrolled software, to not click on unknown web-links, or open attached files from unknown senders or which have not been checked for virus/malware, to not be a victim for social engineering initiated via phone to get access to login information. Further, all new procurements or re-installations of an IoT product should entail that all factory/basic configurations must be changed in terms of device name, user accounts, passwords, network addresses and IP-masks. The cybersecurity-level should be set to the same or a level exceeding the hygiene level decided.

9.1.3 Use case – maritime industries

- Within maritime industries, spanning vessels, platforms and harbours, there is commonly an administrative environment (IT) and another for the production (OT). This differs a bit from the land-based settings as the maritime industries, including parts of their distribution processes, are most often situated in ecologic sensitive areas. The distribution processes are sometimes connected to the OT environment of the production, for instance if there are pipelines from oil/gas platforms, but usually they are separated by having vessels caring for the transport and having their own IT/OT environments (which may be connected to the Internet to share data or fetch updates etc.). Previously, only the IT-environment has been connected to the Internet but more and more OT environments get connected (which requires a high cybersecurity-level depending on type of operation, criticality and risks perceived). The cybersecurity awareness and maturity within parts of the maritime industries have been good for a long time, but now it needs to be strengthened also for almost all employees and these companies need to organize their cybersecurity for both the IT and OT environments.
- Many maritime industries have around the clock operations and only stops the production during one or a few weeks per year. The further continuous the operations are, the harder it is to make changes and, in such cases, all changes or new installations must be planned so to ensure that they all get completed during the stop and then can be smoothly moved back into operation again without any disruptions. Due to reasons of efficiency, it gets more and more common that suppliers and consultants need to exfiltrate data from IoT products to be able to plan for activities and optimizations (and potentially also make external connections from the outside to provide services remotely). Thus, there is an increasing need for to be able to exfiltrate and share data from maritime IoT products for both internal and external usage. However, this requires an Internet connection which is not always available, and the bandwidth may be very low as well as expensive (if using satellite communications). Mobile networks get improved coverage but still do not cover many remote places on earth. IoT products for maritime use have a number of requirements pertaining to sustainability in terms of the environment they are used within, a robust and stable function, that they are recyclable, energy efficient and cybersecure. Besides common workplace safety regulation, electric safety requirements and type approval, there are also the UN's/IMO's/IACS's requirements for cybersecurity (if class action and based on IEC 62443 3-3), EU's GDPR and forthcoming EU Cybersecurity and Cyber Resilience Acts concerning cybersecurity for digital consumer and professional products. Regarding vessels which travel the world, there are a number of additional legal frameworks to cater for as well as physical security and cybersecurity in harbours, to prevent nothing unwelcome getting aboard.

- In production processes aboard, there are a number of IoT products for monitoring and control of processes, production equipment and propulsion. Further, there are commonly IoT products used in steering/navigation and communication systems, physical security (warnings, evacuation, fire extinction systems, etc.), alarm/lock systems, automation for ventilation/heating/cooling, measurement systems for cargo and tanks, etc. In addition, distribution processes use IoT products in similar ways as in production processes but also to keep track of where output/products are and that their quality is kept intact (e.g., pressure, moisture, cooling, keeping within the right temperature range). Within distribution environments, physical security often depends on the age of the vessel and may require improvements so that unauthorized persons cannot get access to IT and OT. Production- and distribution environments can be tough on maritime IoT products in terms of physical endurance/protection (environmental protection in terms of water/dirt/dust/cold/heat, resist impacts, sabotage and physical intrusion attempts to connect to the networks via the IoT product) and cybersecurity.
- Within maritime industry, there are a great deal of information in both the IT- and OT environments which need to be protected as most of the 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 kept high and even, and stops and disruptions should be avoided, for to achieve output with an even and wanted level of quality. Significant variations in production processes may cause danger in many ways. There are large amounts of information in a production process, whereof some may be of secret nature, such as process and implementation knowhow, methods, recipes/patterns, programming, etc. Further, to know if a production/distribution process functions or not may be valuable if it can affect for instance stock market prices.
IoT products, e.g., sensors, measurement equipment and systems, monitoring systems, operation systems, control/navigation/planning systems, communications systems, and maintenance systems, thus need to have an adequate physical protection in combination with an approved level of cybersecurity. The level needed depends on what operations and context as well as which class a vessel or platform have. The level is often considerably higher than for land-based industries. The basic level commonly requires that the IT- and OT-networks are segregated, and that the OT environment is divided into smaller segments so that different processes are isolated and protected from others and having only authorized communications inside the segment as well as in between segments. Besides that, there is need to ensure that users only can do what they are supposed to do (and not more), have control of any external connections and how data can be shared with the right recipients/partner in a secure manner, monitor networks, ensure patch routines, have an updated incident management, and ensure that backups and restore works. Unfortunately, many older IoT products have a poor inherent level of cybersecurity, which is not possible to upgrade or replace in a rational way, and this leads to that these are not allowed to be connected into the OT-network but will reside in isolated islands. In January 2024, there will be tougher requirements and some 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 moving around in the OT environment and ensure that they do not bring in any virus/malware or connect “things” without having authorization from the OT-security responsible.

There are often, within maritime distribution environments, IoT products which are exposed and can be used as a steppingstone to get into networks and spread virus/malware. Thus, there is a need for physical protection, to keep control of whom can communicate with them, as well as to consider how to maintain the cybersecurity-level over time and what happens at the end of the life-cycle. Further, hardening of maritime IoT products are necessary. The hardening encompasses to remove or inactivate services not needed, strictly limit the communications to only the ports, applications, and protocols where authorized traffic should pass. The supplier should make the hardening, as part of basic or factory settings, and if needed this can be opened during the installation. Base configurations for hardenings are good to use to minimize human error. The large problem for the maritime industry is often lack of enough competencies and organization as well as locally implemented rules, which may cause, as a consequence, cybersecurity-related problems in the OT environment. A smaller problem is that the suppliers' function warranty commonly needs approval by the suppler prior to upgrades and patches can be installed. Unfortunately, the suppliers take some time to do their own testing required and this leaves a time gap where the IoT product is vulnerable.

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

9.1.4 Use case – municipalities (which are affected by the laws of public procurement)

- Swedish municipalities have operations with a wide range and varying extent, where certain parts are very similar to critical infrastructures, industrial organizations and companies, and healthcare, while other parts are oriented towards administration. There are only a few very large municipalities, some middle-sized and most are small with a population of a few thousands to ten thousand. The small number of populations in most municipalities, and if situated in rural areas, causes a negative effect on the possibility to find adequate competence within IT, OT, IoT products and cybersecurity in general. Some parts of the operations are further challenging than others, e.g., the primary and secondary schools where almost all pupils are connected as well as public locations such as libraries, sport arenas, busses and squares all having public municipal Wi-Fi-connectivity.
- A municipality is commonly 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, harbours, etc. In addition, there may be election and guardian districts/areas. Regarding urban construction/building, there is often a technical office that deals with real estate, traffic control and lights, sewage and clean water production, as well as IT (unless that is an own function within the municipality). The other districts/areas have responsibility for schools, libraries, sport arenas and facilities, elderly care and shelters, local public traffic (busses and trams etc.), which all may have their own IT-, OT-, or MT (medical technology) infrastructure using IoT products in multiple locations. Within a municipality, the boundary and definitions regarding what is classified as critical infrastructure may be somewhat unclear and should be given more attention. The critical context con-

JUSTICE. JUDGES CLUB.
PHOTO: SHUTTERSTOCK.

cerns for instance sewage management and clean water production, energy production/ distribution, traffic, rescue services, and elderly care. Further, also larger roads, airports, and harbours with large logistical impact should be part of the critical context. Depending on the size of a municipality's population and the operation's impact on society in large, the critical districts/areas mentioned may be subject to national security protection laws and secondary laws form the Swedish Civil Contingencies Agency and Swedish Food Agency as well as other authorities. There are sensitive personal data/information within many of the districts/areas, which requires a high level of cybersecurity. Thus, legal and regulatory frameworks, such as EU GDPR and potentially NIS/NIS2 and the forthcoming EU Cybersecurity Act need to be considered.

- Due to the wide extent of a municipality's operations, there are numerous IoT products installed at many locations (depending on the level of digitalization). Many IoT products are used in similar ways as in industrial organizations and companies as well as critical infrastructure to monitor and control, and examples of application areas are building automation (ventilation, heating, and cooling), surveillance/locks/alarm systems, etc. Within health and elderly care, IoT products are used for monitoring of patients, in equipment for remote care (which likely will increase a lot), safety alarms, and other applications enabling health and elderly care at the care takers' own homes at increasingly higher age. Thus, there are a lot of IoT products installed and used within the operation of a municipality – and the number will increase as long as the cyber-security-level allows that.
- Common problems in municipalities, which are related to cybersecurity and the use of IoT products, are the lack of required competencies, tough and prioritized budgets, and that the law on public procurement discourages some potential suppliers. In addition, the wide extent of the operations add burden to this too. Regarding small and mid-sized municipalities, often the main problem is to acquire the right competencies. The use of consultants is a short-term solution, and due to the COVID pandemic and the digitalization efforts following it is nowadays easier to get support or help via distance. Small municipalities usually have small budgets and an IT-department comprising 2-3 employees, who shall manage 100+ systems and cybersecurity plus everything else. This equation simply does not add up. To find solutions for the future, adjacent municipalities have started to collaborate and share systems and competencies.

Larger municipalities usually have access to a wider range of competencies and consultants. Unfortunately, the law on public procurement discourages IoT-suppliers to do business with larger municipalities too.

- In general, municipalities need to adhere to the increasing requirements for improved cybersecurity, as they store and process a lot of both sensitive information and have critical operations and infrastructures. Thus, a general improvement of the cybersecurity-level is needed, which also applies for the IoT products used within the wide range of operations in the districts/areas. Of course, there is a variation in terms of cybersecurity requirements depending on type of operation and if 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 competencies and the additional competencies needed for IoT products. The usage of IoT products is likely to increase a lot within the next 20-30 years as older infrastructure is gradually replaced and additional monitoring using different types of sensor solutions will be applied. Previously, mentioned was that small and mid-sized municipalities ought to cooperate and share systems, staff and competencies. If such cooperation and collaboration is initiated, the municipalities need to agree upon coordination of which IoT products to use and what cybersecurity-level to apply – so that the adequate competencies can be acquired.

9.1.5 Use case – critical infrastructures

- There are many similarities in between industrial organizations/companies as well as maritime industries (see earlier use cases), but critical infrastructures have further importance for society and are therefore classified as critical. Of course, parts of industrial organizations/companies and maritime industries can have a significant impact on society and cause large disruptions, in particular if value-chains involved with production of components and merchandise, food production, and logistics, are impaired. Operations within EU, which by the NIS Directive are classified as critical infrastructures, differs slightly from the USA's classification as EU has seven sectors and the USA sixteen sectors part of the classification. The EU's seven sectors today comprise the following ones (these are likely to be augmented within the next following years): banks, infrastructure for financial markets, digital infrastructure, energy, healthcare/hospitals, distribution of clean water, and transports. The USA also further includes chemical industries, critical manufacturing/process industries, food production, farming, and emergency services – all of which should be of interest for the EU as well.
- Most critical infrastructures, having production and distribution, operate their processes around the clock and may only have possibilities for shorter stops 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 while sewage management and distribution of electricity must operate continuously. The more continual the operations are, the harder it is to change in the production and distribution processes. In such cases, all changes and new installations must be planned and coordinated well so that when there is a suitable stop, they can be executed and operations resume smoothly again afterwards. Employees may, due to efficiency reasons, need to connect from the outside and conduct work tasks and monitor that all progress well. Concerning third parties, these should not be allowed to connect from the outside unless there are strong reasons for to do so. Further, there is an increasing need for sharing of IoT products' data both internally and externally. In addition, there are a lot of requirements pertaining to environmental sustainability, for

a robust and stable function, that they are recyclable and energy efficient, as well as adequately cybersecure. Besides laws related to national security and safety, there are also requirements for work safety and environment, electric safety and type approval with CE-marking. In addition, there are guidelines from the ENISA, Swedish Civil Contingencies Agency, and Swedish Food Agency, as well as laws/regulations concerning EU's GDPR, NIS/NIS2 and the forthcoming Resilience and Cybersecurity Acts (with requirements for a hygiene level regarding cybersecurity for digital consumer and professional products).

- IoT products operated within critical infrastructures are often very similar to the ones used in industrial organizations/companies and maritime industries but may have further challenges in the distribution processes due their exposure and that these are hard to physically protect due to their extent ranging over vast geographical areas. Unfortunately, sabotage operations/activities are nowadays something that must be factored into the risk analyses. Thus, the physical and cybersecurity-related requirements are higher compared to in the industrial and maritime settings. This requires a very high physical security level in production environments, strict access management, clearer separation of environments, hardening of the networks and equipment/devices (including the IoT products). Regarding the distribution processes, monitoring and intrusion detection are commonly required in terms of physical access and cybersecurity wise. The monitoring of distribution processes and networks' function are needed to ensure that they function well (i.e., are available and operate as expected). If these processes fail, fast pinpointing of the issue is needed for to be able to fix the issue accordingly.

HIGH VOLTAGE LINE.
PHOTO: SHUTTERSTOCK.

- Within critical infrastructures, the cybersecurity requirements for, and surrounding, IoT products are higher or considerably higher compared to industrial settings. The baseline level for cybersecurity must be adequate and there should not be any weak spots or areas. The large problems for critical infrastructures are lack of enough staff with adequate competencies and security clearance combined with sometime unclear local rules, which may cause cybersecurity issues in OT environments because of the extent and need for continuous improvement. Not adequate budgets are another pressing issue. A smaller problem is the suppliers' function warranties, which often require that upgrades and patches are pre-approved by the supplier prior to that they can be installed. An issue is that this results in a time window with potentially open vulnerabilities. Due to the continuous operations, a certain level of redundancy is needed, which further enables that some updates can be installed in a controlled way without disruptions (unless installed at planned stops). In general, IoT products need to be simple and fast to upgrade or change.
- Finally, needed is a very high level of knowledge concerning cybersecurity and what not to do. Examples are to not charge mobile phones in USB-ports, to not use uncontrolled media (USB-disks), to not install uncontrolled software, to not click on unknown links or open any attached files that have not been checked for virus/malware, etc. Further, all new procurements or re-installations of an IoT product's base 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 – whereof there are many as well as extensive ones.

10. Suggested readings

– frameworks/standards, references and explanation of technical terms

Below, there are lists with suggested readings within: frameworks/standards, new upcoming EU regulations and directives, and reference literature for those who wish to build a deeper knowledge and find more details for various areas and contexts.

Frameworks and other relevant tests which can be of interest in order 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)
  - Regarding connected building automation systems – see further below
  - NIST Cybersecurity for IoT concerning Consumer IoT Products (https://www.nist.gov/itl/applied-cybersecurity/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 Civil Contingencies Agency pertaining to industrial control systems, cyber physical systems and IoT (a number of such publications are available at www.msb.se)
  - Swedish Civil Contingencies Agency – guidelines on cybersecurity for connected building automation, 2015, https://www.msb.se/sv/publikationer/fastighetsautomation--cybersakerhet-inom-fastighetsautomation/
  - NIST standards (mainly aimed for public organizations within the USA but comprise 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 centre for cybersecurity has many cloud- and IoT-related cybersecurity publications available on their web site (www.enisa.europa.eu)
  - ISO/IEC 27019 regarding information security for process control within energy production and distribution (can be found at https://www.iso.org/standard/68091.html)
  - IEC 62443 (where part 3–3 is probably of most interest – https://www.en-standard.eu/)
  - ISA95/98 with the automation pyramid as well as the Purdue-model (https://www.isa.org/)
- Maritime environments
  - IMO's guidelines for maritime environments MSC-FAL.1/Circ.3 and Resolution MSC.428(98) – there are comprehensive frameworks made by, 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 E26/27.

- General IoT-security (and also if the data will reside 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 national states – IoT in various environments within Sweden
    - Robust & Säker IoT: Vägledning för Robust och Säker IoT ver 1.0, Svenska Stadsnätsföreningen (SSNF), 2020, https://www.ssnf.org/nat-i-varldsklass/avtal/nyhet-avtal-robust--saker-iot-version-1.0/#:~:text=V%C3%A4gledning%20f%C3%B6r%20Robust%20%26%20S%C3%A4ker%20IoT%20beskriver%20ett,Webbinarium%20om%20avtalet%20f%C3%B6r%20robust%20och%20s%C3%A4ker%20IoT
    - Stödmaterial till Klassa, there are 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/klassaforiot.65074.html
    - Informationssäkerhet inom fastighetsområdet & IoT, Swedish Association of Local Authorities and Regions, 2022, https://webbutik.skr.se/skr/tjanster/rapporterochskrifter/publikationer/informationssakerhetinomfastighetsomradetiot.65014.html
    - Informationssäkerhet i fastighetsorganisationen, Swedish Association of Local Authorities and Regions, 2022, https://skr.se/skr/tjanster/rapporterochskrifter/publikationer/informationssakerhetifastighetsorganisationen.66960.html
    - Referensarkitektur för IoT (till smart stad och digitala tvillingar), Arkitekturgemenskapen (kommuner och regioner), 2022, https://inera.atlassian.net/wiki/spaces/AR/pages/2753593356/Referensarkitektur+f+r+IoT
    - NIS/NIS2 Directive (there are information about this on EU's and the Swedish Civil Contingencies Agency's web sites https://digital-strategy.ec.europa.eu/en/policies/nis-directive and https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/nis-direktivet/)
- 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)

Some upcoming regulations and directive on 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

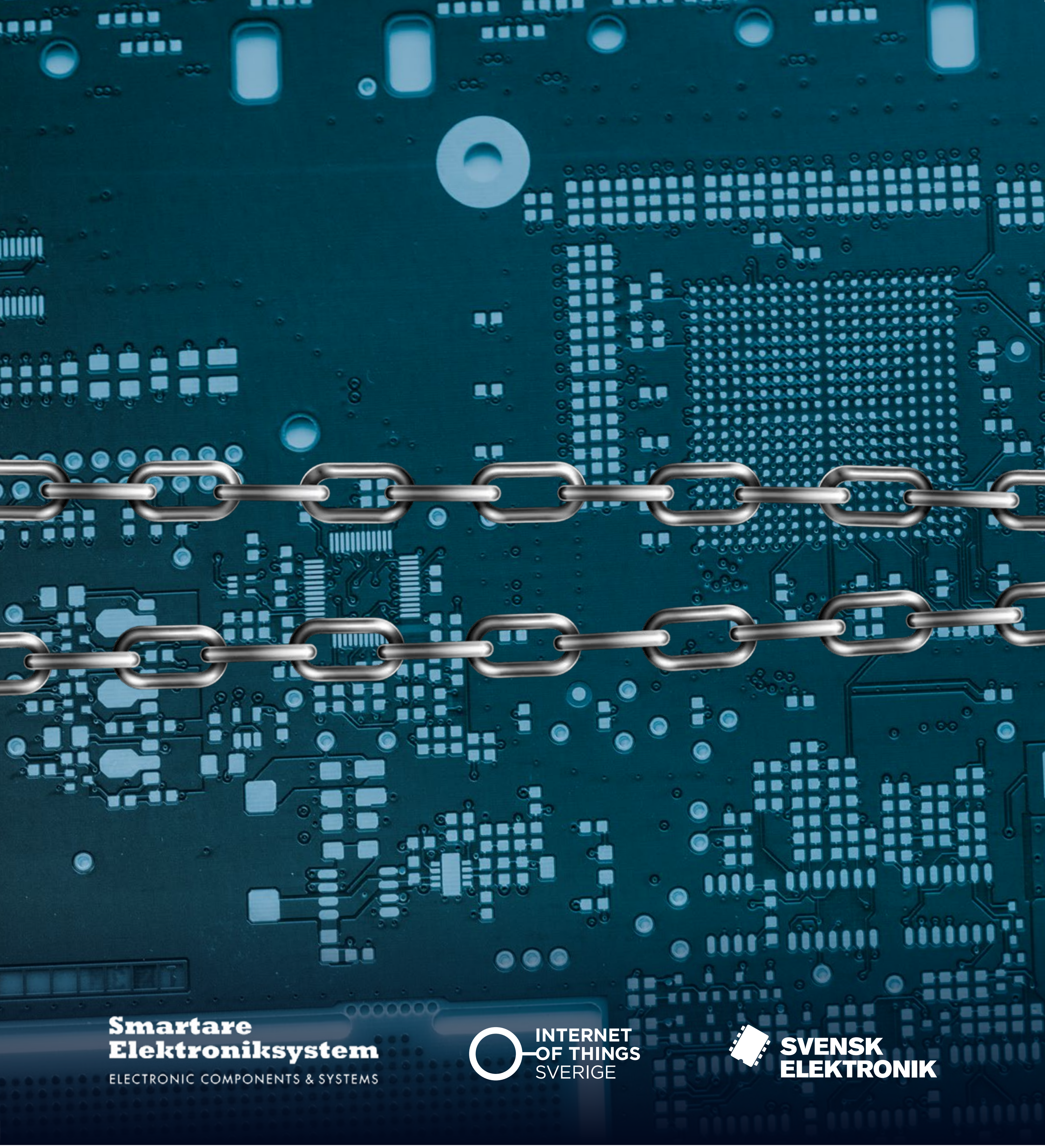
Reference literature:

- *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 administrative purposes.
- **OT** – operational technology, used in for instance production- and distribution environments within industry and critical infrastructures. Sometimes, OT-equipment are similar to the equipment used within IT environments, and in the future a lot of IT and OT will likely converge from a technology standpoint although their functionality differs. Within 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 within health care and is similar to OT but often has even higher requirements pertaining to time criticality, performance and availability.
- **Fleet management** – if there are a lot of IoT products installed and running at different customers, these are often called a fleet. A fleet management system, or functions, can be used to keep track, monitor, remotely maintain or support a fleet of IoT products from distance. Such a system or functions can improve efficiency and speed up the time until necessary actions are taken. An alternative, if remote maintenance or support is not possible, is to ask the customer's users/operations to lower the load/speed or stop operations if there are signs of serious problems prior to that a breakdown occur.

THERE ARE MANY FRAMEWORKS/STANDARDS, NEW LAWS AND REGULATIONS THAT REQUIRES YOU TO STAY TUNED WHEN IT COMES TO CYBER SECURITY AND IOT PRODUCTS.
PHOTO: ADOBE STOCK



Smartare Elektroniksystem
ELECTRONIC COMPONENTS & SYSTEMS

INTERNET
OF THINGS
SVERIGE

SVENSK
ELEKTRONIK

With support from:

VINNOVA

Swedish
Energy Agency

FORMAS

STRATEGIC
INNOVATION
PROGRAMMES

smartareelektroniksystem.se
svenskelektronik.se

ISBN: 978-91-985741-5-9
PRICE: 374 SEK EXKL. MOMS