DEALING SECURELY WITH THE INTERNET OF THINGS

A guide for information security officers

TNO REPORT
8 DECEMBER 2016

Ir. A.C.M. Smulders
L. Oosterheert MSc
R.H. ten Hove MSc
Drs. J. Adriaanse

FOREWORD

Internet of Things (IoT) is a domain that is in a state of flux. In many cases, this domain employs a different life cycle compared to traditional IT.

Many manufacturers of IoT devices regularly deploy updates, including security updates, while others may be less focused on development and security. In these cases, it could mean that support is not or no longer available. This in turn could mean that vulnerable equipment can not or no longer be updated, and thus remains vulnerable. The new domain of IoT device security therefore frequently requires additional insight and guidance. For this reason, this guide has been prepared.

This guide is the result of a collaborative effort between various experts from the worlds of industry, government and research. The guide aims to provide information security officers with an approach to ask the right questions for the benefit of more secure use of IoT. It explains the key questions for each of the eight main topics.

It would not be surprising if you have more questions after reading this guide. IoT is a new domain with a dynamic and very extensive playing field. As the guide explains, IoT is not a subject to which ‘one-size-fits-all’ applies. This guide offers various guidelines that could contribute to more secure use of IoT.

I wish you secure use of IoT!

Hans de Vries,
Head of the National Cyber Security Centre, The Netherlands

The new domain of IoT device security therefore frequently requires additional insight and guidance

CONTENTS

1 EXECUTIVE SUMMARY

If you are thinking of – or are – implementing equipment and processes that may be considered IoT, you can use this guide to structure this process and to identify pitfalls.

This guide is written for information-security officers of organisations that (will) use IoT. The aim of this document is to guide you in applying IoT in a secure and safe manner, based on various considerations and focal points, regardless its scale: From a minor experiment to an organisation-wide deployment. Although its primary target group is information security officers, this guide also contains useful information and practical insights for a broad group of readers that are involved with security and IoT.

Seven themes will guide you through the various facets of cybersecurity that are important (in preparing) for using IoT in your organisation. You will learn to recognise the pitfalls early-on so that you can take the appropriate measures, taking the life-cycle of IoT equipment and systems into account.

The Internet of Things can be defined in different ways, which is hardly surprising when considering the almost endless possibilities offered by (wireless) network connectivity that is both increasingly cheaper and computationally less expensive. IoT is characterised by a considerable diversity of application areas [1], the parties involved and the technical possibilities. Variations in the ecosystem that contain an IoT device are, accordingly, a major drive for increasingly new and innovative solutions or the smart(er) replacement of 'old' solutions. This does not really allow for IoT to be pigeonholed. The guide provides a number of criteria that enable you to determine whether something is IoT or not and, thereby, helps you identify IoT-specific aspects more quickly and include them in your approach.

The themes that will be described provide guidelines for defining the context of your IoT ecosystem and setting up a risk-management strategy. For risk management, you will have to deal with the dynamics and variation created by internal and external factors. For instance, the different stakeholders that play a role may not always have the same interests which, along with other factors, may cause scope creep.

Use these guidelines to deal with IoT in a secure way and to prepare for the future.

Seven themes will guide you through the various facets of cybersecurity that are important (in preparing) for using IoT in your organisation

2 INTRODUCTION

This guide can assist information security officers in making choices to deal with the Internet of Things (IoT) securely. It provides you with guidelines to go through the process before making a choice. The diversity of IoT means there is not a single, standard approach or way to deal with IoT securely. This guide offers a compilation of considerations, focal aspects and steps you can go through, based on experiences.

We hope this guide will give you insights into several aspects that influence the secure use of IoT. These aspects have been identified in consultation with experts from the field. Where possible, we refer to available standards that offer a solution.

2.1 INTERNET OF THINGS, WHAT IS IT?

The Internet of Things can be defined in different ways, which is hardly surprising when considering the almost endless possibilities offered by (wireless) network connectivity that is both increasingly cheaper and computationally less expensive.

IoT is characterised by a considerable diversity of application areas [1], the parties involved and the technical possibilities. Variations in the ecosystem that contain an IoT device are, accordingly, a major drive for increasingly new and innovative solutions or the smart(er) replacement of 'old' solutions. This does not really allow for IoT to be pigeonholed

This guide distinguishes:

- **IoT devices:** The physical devices that form the bridge between the virtual and physical worlds, such as temperature sensors or heart-rate monitors;
- **IoT systems:** *IoT devices* + the components required to enable services and applications, such as apps, webservers and cloud services; and
- **IoT ecosystem:** *IoT systems* + stakeholders.

2.2 RATIONALE BEHIND THIS GUIDE

More and more products are being connected, whether via internet or through closed networks, such as process control systems that monitor and control vital processes. Errors in the security of our standard ICT-based services and products, which were made in the past decades, are repeated in the IoT domain. It is, therefore, an excellent time to review lessons learned in the past and identify how they can be used in the new trend of IOT development.

This guide is the result of the Cybersecurity & Societal Resilience programme, funded by the Dutch Ministry of Security and Justice. We first describe a number of generic considerations, so you can confidently choose which (technical) standards and cybersecurity aspects are relevant to you in the context of IoT.

2.3 TARGET GROUP

This guide is written for information-security officers of organisations that (will) use IoT. It, therefore, aims to generate greater awareness among these groups for the cybersecurity of IoT systems where necessary [2], as well as provide guidelines for setting up information security in the context of IoT. We expect this document to also offer useful information and practical insights to a broader group, such as suppliers and manufacturers.

2.4 IS SOMETHING IOT OR NOT, AND HOW DO YOU DETERMINE THAT?

While there are many definitions for IoT, they do not tend to offer an adequate guideline for distinguishing between IoT and non-IoT. In order to draw this distinction, we use the following criteria:

A. IoT has a direct relationship with the physical world and without the need for human intervention.
B. IoT uses a communication link (wireless or wired).
C. The primary functions of IoT are aimed at measuring and/or influencing the physical world.
D. (Optional) The secondary functions of IoT are aimed at analysing information to reason about the physical world, or to prepare to influence the physical world.

In section 3.1, a number of examples is discussed to demonstrate how these criteria may be used.

We are conscious that using these criteria excludes applications and devices that are often considered to be IoT, such as an internet-connected digital video recorder or a cable modem that connects a home network to the internet. Although many aspects in this guide also apply to these devices, we wish to stress in this guide that the bridge between the virtual and physical worlds involves specific requirements and security issues.

2.5 SECURITY IN THE IOT

As becomes evident from the criteria outlined above, the IoT has a strong relationship with the physical world. The IoT, therefore, encompasses elements from both the physical world (such as sensors and actuators) and virtual world (such as a virtual representation of the physical world) [3]. The IoT covers a complex system of various parts, in which security issues are not restricted to a specific part but are, in actuality, created by the integration of – or interaction between – various parts. In order to properly organise the security of IoT, you should both employ different security technologies and evaluate the status and context of the IoT, while not forgetting the organisational aspect and human factor.

The IoT has such a wide range that no single architecture can be defined that describes all the solutions based on of IoT. As a consequence, it is not possible to define a single cybersecurity architecture for the whole IoT, although this may be possible for individual parts. The security architecture for the IoT parts is currently still in an exploratory phase. There are many initiatives taking place in this area, for example, the list of strategic design principles for IoT that was recently established by the American Department of Homeland Security [4].

To deal with the IoT securely, you will have to overcome a number of challenges. This guide offers you the guidelines for identifying such challenges and to tackle them.

2.6 CHOOSING STANDARDS

One of the purposes of this guide is to help prepare you in choosing from the available standards. Choosing the right standard is no easy task. This becomes clear when you look at the landscape of standards. An analysis carried out by an ISO working group [5] reveals that there were more than 400 standards [6] related to IoT in 2014, produced by ten standardisation organisations[7].

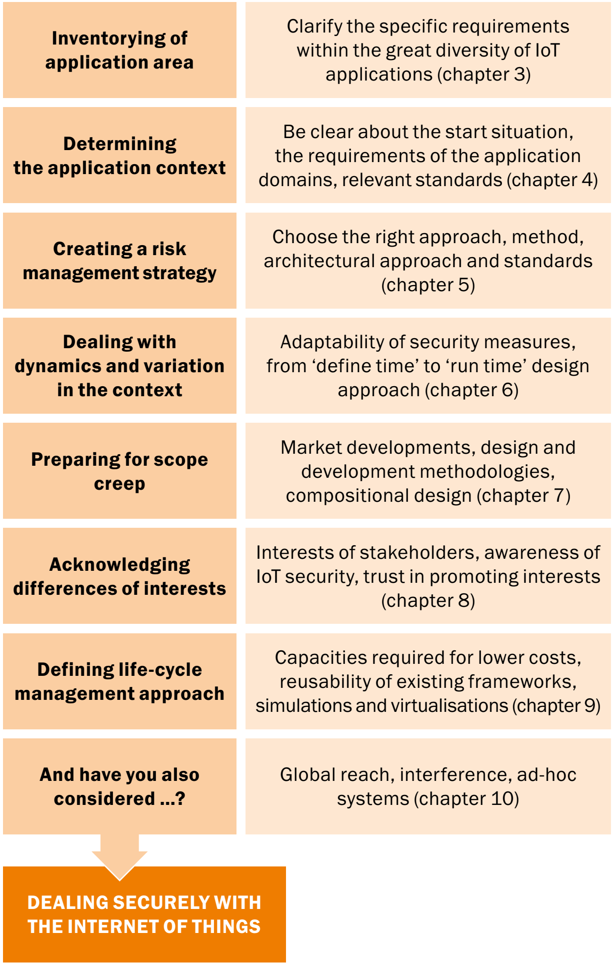
Given the large number of standards, it should not surprise you that standards conflict in practice. This can be attributed to the different and sometimes conflicting requirements from the various application areas and the disparity in stakeholder interests in the IoT ecosystem.

In addition, the standards developed for internet appear to be too complex for its limited capacity, such as computing power and storage space, and the functionality of the equipment that is usually developed for applications based on IoT [7] (page 49). It is evident that well established standards are not, by definition, usable.

Not all standards directly relate to security and/or privacy. From the standards developed by two leading standardisation bodies, ITU and IEEE , [7] (appendix 2 and 3) nearly forty of them are related to security and/or privacy. The standards cover a great variety of applications. These standards predominantly relate to the communication security with, and between, IoT devices and systems.

2.7 STRUCTURE

The guidelines are clustered around a number of themes relevant to the IoT. You don't have to follow these themes in any kind of sequence; rather, you should select the themes that are important to your approach, based on their relevance to your situation. Given the diversity of the IoT, it is not possible to give a standard approach. The different themes that are relevant to cybersecurity, selected on the basis of experience, are summarised below. Consider the respective chapters for more details, considerations and focal aspects.



Inventorying of application area	Clarify the specific requirements within the great diversity of IoT applications (chapter 3)
Determining the application context	Be clear about the start situation, the requirements of the application domains, relevant standards (chapter 4)
Creating a risk management strategy	Choose the right approach, method, architectural approach and standards (chapter 5)
Dealing with dynamics and variation in the context	Adaptability of security measures, from 'define time' to 'run time' design approach (chapter 6)
Preparing for scope creep	Market developments, design and development methodologies, compositional design (chapter 7)
Acknowledging differences of interests	Interests of stakeholders, awareness of IoT security, trust in promoting interests (chapter 8)
Defining life-cycle management approach	Capacities required for lower costs, reusability of existing frameworks, simulations and virtualisations (chapter 9)
And have you also considered ...?	Global reach, interference, ad-hoc systems (chapter 10)

DEALING SECURELY WITH THE INTERNET OF THINGS

Figure 1 Structure of the guide

To deal with the IoT securely, you will have to overcome a number of challenges. This guide offers you the guidelines for identifying such challenges and to tackle them

3 IOT APPLICATION AREAS

Due to the great diversity in application areas [7] [6], it is not possible to give a definitive list of all the application possibilities of IoT. However, several examples are shown below to provide a picture. IoT is not a topic where 'one-size-fits-all'. If you are considering using IoT, it is important that you also take account of the law and legislation that apply to a specific application area.

Take, for instance, an ISO standard that applies to medical equipment [8] and which is aimed to employ risk management for IT networks and medical aids. It should be noted that this standard describes the process of developing secure systems and not how this can be achieved technically. The standard aims to achieve a good balance between four objectives:

- Patient safety;
- Secure connectivity;
- Data and system security;
- Interoperability.

Specifically, for the industrial application of the IoT, the Industrial Internet Consortium (IIC) has developed a security framework [9] that provides specific tips for the security of industrial IoT. For information security officers, this framework is a good supplement to this guide. The IIC framework has an additional focus on reliability in the context of industrial applications.

This framework, produced by the IIC, shows how you need to take the extra requirements of your specific application area into account in addition to the normal aspects of cybersecurity. To this end, it is a useful supplement to this guide, in line with your specific needs. The next section considers application-specific requirements.

3.1 EXAMPLES OF APPLICATION AREAS AND THEIR REQUIREMENTS

The Unlimited application possibilities of IoT devices make it an almost endless task to indicate the specific requirements, per application and application area, that one has – or will have to – consider.

In order to provide you with some guidelines, we give a number of (fictive) examples so that you can see how you can make the specific requirements for your application area transparent. The examples are described below on the basis of the criteria contained in section 2.4. These criteria form a guideline in identifying application-specific requirements without leaving room for any unexpected surprises.

Example
Sensors in a smart refrigerator are able to identify food products on the basis of RFID and can, thus, establish how much of each product is still present (criterion A). The refrigerator is also able to send and receive this information via a wireless connection (criterion B). The primary function of this is to obtain insight externally into the food products that are in the refrigerator (criterion C). Additional information about, for example, the optimum storage temperature and use-by date is available via a cloud service, where related analysis is also performed (criterion D).

The application-specific requirements can be derived from the relationship with the physical world, for instance, in food products, where it can be assumed that food safety regulations must be considered. In addition, the information can provide insight into the dietary patterns of the user(s), which may contain sensitive information regarding privacy.

Example
Smartphones are used to identify the location of loud bangs. Once the user has activated the relevant application, the noise of the smartphones surroundings is recorded constantly (criterion A). Each smartphone that has this application actively transmits the relevant data to a central server (criterion B). With the data on the level of noise and the location of various smartphones, the location of the bangs can be calculated (criterion C). This calculation is made on the central server that receives the data from all the smartphones (criterion D).

This application can, for example, be used in the period around New Year's Eve to simplify the detection of fireworks that are illegally set off. Since all the noise in the surroundings is recorded, one will have to consider the risk of exposing privacy-sensitive information. By processing the surrounding noise, it is also possible to record spoken information. To avoid violating privacy legislation, mitigating measures can be considered when designing this application. For example, the smartphone may calculate whether noise is a bang caused solely by an abrupt increase in noise level. This measurement is then sent, together with the location of the smartphone, to a central server.

Example
Traffic flow is supported by roadside sensors that measure the location, speed and direction of vehicles (criteria A & C) approaching a traffic light intersection. This information is sent (criterion B) to a central server that calculates the optimum traffic flow at the intersection and controls the traffic lights based on this information (criterion D).

In this application area, the traffic safety requirements must be considered.

Example
The smart meter is used to measure information such as current energy consumption or supply (criterion C) and to send this data (criterion A) to a central system (criterion B). The information collected can be analysed to gain up-to-the-minute insight into the current energy demand and to link this demand to the available energy supply (criterion D).

The requirements of the energy domain must be considered for this application, which relates the integrity of information to safety. The energy consumption may also reveal something about how a person lives and, therefore, privacy should also be taken into account.

When setting up an IoT system, it is advisable to take application-specific requirements into account at an early stage. This may prevent any supplementary regulations, or the risk that innovations, which are at an experimental stage, are hampered at a later stage.

4 DETERMINING THE **APPLICATION CONTEXT**

Choosing to use IoT is not always internally motivated; it can be prompted by what the market and competitors are doing. Furthermore, in application areas where security plays a significant role, such as vital infrastructures and healthcare, this choice should be made more explicitly compared to areas where security plays a less significant role.

4.1 A NUMBER OF QUESTIONS FOR YOUR STARTING POINT

Clarity on your starting point lays the basis for subsequent steps. The sections below comprise a number of questions that will help you clarify your starting point.

4.1.1 WHAT DEGREE OF CONTROL DO YOU HAVE OVER THE USE OF IOT?

To what extent you can – or cannot – exercise control of the use of IoT is important in the approach you take. It is essential to determine the aspects you can control yourself and those you cannot.

Example
Procuring a service that uses sensors to deliver information on which you make decisions yourself. Managing the sensor is a responsibility of the service provider. This probably gives you less control of the number, placement and security of the sensors and their communication.

The extent of your control is complex due to the fact that it is not always clear to parties in the IoT ecosystem who the owner of an IoT device is. Furthermore, it is often unclear whether this party can also be held responsible for, for example, the physical actions of the device. Apart from making access to the devices secure, it is therefore also important that you identify the responsibilities well, in order to be transparent to the users about the responsibilities concerning the access and use of the devices.

4.1.2 WHAT SPECIFIC REQUIREMENTS AFFECT YOU?

For a number of areas, specific requirements apply if you intend to use IoT. Initially, your IoT solution will be geared to one specific area, with a limited IoT ecosystem. However, if want to make your IoT solutions effective, flexible and cost-effective, it may be necessary for you to realise the use of IoT devices across several domains, which also grows the IoT ecosystem.

In doing this, it is a good idea to check in which domains you expect to use IoT devices in the long run and, accordingly, which requirements you will have to comply with. For example, safety (like safety and patent safety) is applicable for many ICS and medical applications. In addition, medical applications may, for example, involve supplementary privacy-related requirements.

This growing integration, therefore, requires you to think about future growth outside your own area of application and what the impact of this may be on the requirements for IoT devices.

4.1.3 WHERE DO YOU USE IOT?

Just because you use IoT in a specific application area with strict requirements, it does not automatically mean that these requirements also apply to your application.
For instance, you can use IoT to observe deviations in ICS without it being part of that ICS system itself.

Example
You are responsible for managing the groundwater level in a particular area and are, to this end, using an ICS that monitors the status of pumps and valves in the respective installation. You are considering to deploy an IoT system with sensors here and there to give you insights into the current groundwater level.

You can lay such an IoT system without any direct connection to your water management system, while it still offers additional functionality. Such a system enables you to create extra possibilities to measure the current water level without directly influencing the water level. The requirements for the ICS do not directly apply to the IoT system. However, these requirements will apply if you directly connect the IoT based applications or integrate with existing systems, for example, if you want to use IoT to directly control the pumps, valves and discs in the water management system.

4.1.4 ARE YOU AWARE OF POSSIBLE DISRUPTIVE DEVELOPMENTS?

In some instances, conscious choices will be made concerning the use of IoT devices in relation to the security requirements in a specific application area, such as the health domain. However, IoT has the potential to be disruptive, for example, when IoT is introduced without taking explicit account of security and/or privacy. This applies to both developments initiated by your organisation and innovations introduced from outside.

Example

The introduction of the smart meter, which replaces the normal meter, saw an IoT device enter the energy world and technically enable the current energy consumption to be metered and switched on/off remotely. Initially, the public reaction had been underestimated and, accordingly, the chance grew that consumers would not have enough trust in the smart meter or the market model[10].

An example of innovation coming from outside is the alternative IoT-based metering systems for medical applications. This innovation is made possible by relatively cheap technology for the acquisition of ambient and personal data, for example, the technology that enables people to meter their heart rate and blood pressure themselves. In the medical sector, such developments can have a significant effect on your information systems or the connection to them. For you, it is important to get a picture of these changes which have consequences for your organisation in the area of privacy and security.

All the parties must consistently apply the same governance, including the privacy and data protection regulations, regardless of the technology

4.1.5 WHAT DOES YOUR IOT ECOSYSTEM LOOK LIKE AND IS IT CONTROLLED?

For virtually every IoT ecosystem various parties deliver joint services and, thus, depend on each other. It is, therefore, essential that you make agreements with all the parties involved to ensure that the IoT ecosystem is reliable and practicable, and that it remains so. To this end, all the parties must consistently apply the same governance, including the privacy and data protection regulations, regardless of the technology.

There will always be a system owner within your organisation for the functionality used by your own organisation. It is also good to realise that there are often more parties involved throughout the IoT system, including the indirect stakeholders, citizens, supervisory bodies and consumer organisations. The parties involved each have their own changing vested interests and related implementation. We, therefore, speak of an IoT ecosystem in which the responsibility for different components of this IoT ecosystem are divided amongst different parties, which can make the management and control of the IoT more complex. Apart from the responsibilities that, for example, are established due to the privacy legislation, you may have to make additional agreements concerning who is responsible for what, although everyone remains responsible for his own part of the ecosystem. Mutual agreement on areas like organisation and technology is essential to allow the whole IoT solution to work. If you want to guarantee security across the whole ecosystem, you will have to deliberate in order to come to a suitable set of agreements.

4.2 WHERE DO YOU FIND RELEVANT STANDARDS?

Given the growing importance of cybersecurity, including that of IoT, national and international forums are active in identifying cybersecurity risk factors and defining measures to mitigate that risk. The challenge is to identify the documents that are relevant to you from all those initiatives and standardisation developments.

If you find a possible relevant standard, you must examine it critically. The standard may have been replaced by a newer standard or be considerably outdated. You can check for which application areas a standard has been developed, such as the ISO/IEC270001:2013, which is a generally applicable standard, while others are specific to one application area[8]. Furthermore, you can check, for example, the extent to which vulnerabilities are known for a specific technical standard and whether these are being solved actively.

To help you on your way, Figure 2 provides an overview of standardisation initiatives for various application areas. This concept overview has been compiled by the “Alliance for Internet of Things Innovation” (AIOTI) [11], an initiative of DG CONNECT of the EU. For the most recent information, please refer to the AIOTI working group [12].

An additional description of standards developed by various organisations can also be found in the report of the IERC [7], which considers a number of internationally operating forums.

The main international forums that operate in the area of cybersecurity and IoT globally are:

- Organisation for Economic Cooperation and Development (OECD)
- UN General Assembly (UNGA)
- International Telecommunication Union (ITU)
- World Summit on the Information Society (WSIS)
- Internet Governance Forum (IGF)

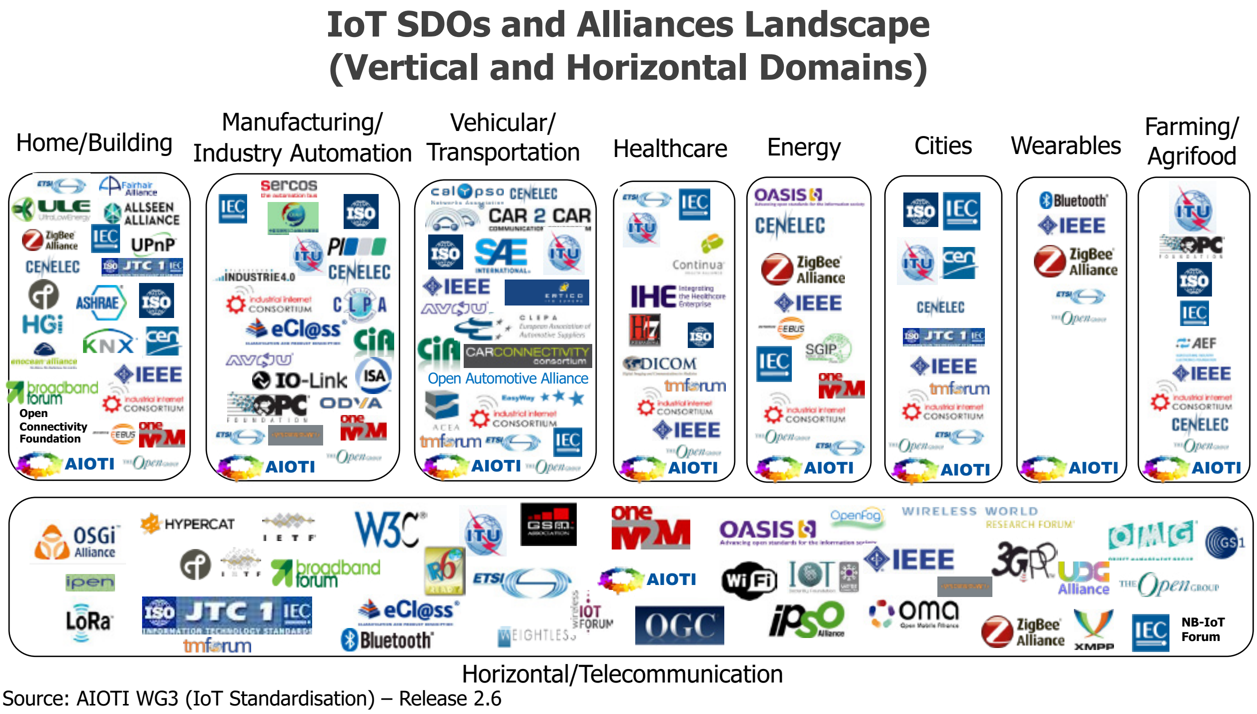
We add the following organisations with a focus on technical aspects to this list:

- European Telecommunications Standards Institute (ETSI)
- Institute of Electrical and Electronics Engineers (IEEE)
- Cloud Security Alliance (CSA)
  Comité Européen the Normalisation - Comité Européen the Normalisation Electrotechnique (CEN-CENELEC)
  The CSA has set up a special working group to focus on IoT security.

Various organisations are also active at European level, such as:

- European Network and Information Security Agency (ENISA)
- European Consumer Centre (ECC)
- Computer Emergency Response Team (CERT-EU)
- Organisation for Security and Cooperation in Europe (OSCE)

At national level, there are also cybersecurity initiatives you could make use of. In Germany, for example, there is the BSI, in France the ANSSI, in the UK the Office of Cyber Security and Information Assurance (OCSIA), in the United States the Office of Cybersecurity and Communications (CS&C) and in the Netherlands the National Cybersecurity Centre (NCSC).


IoT SDOs and Alliances Landscape
(Vertical and Horizontal Domains)
Home/Building
Manufacturing/ Industry Automation
Vehicular/ Transportation
Healthcare
Energy
Cities
Wearables
Farming/ Agrifood
Horizontal/Telecommunication

Source: AIOTI WG3 (IoT Standardisation) – Release 2.6

Figure 2 overview of standardisation and application areas by AIOTI

5 CREATING A **RISK MANAGEMENT STRATEGY**

The most characteristic aspect of IoT which has an impact on security is how IoT devices and their applications come to be. In these cases, the primary focus in the development of new IoT concepts and technologies lies on realising functionality [13]. Only when that functionality takes hold, a business case emerges and a number of cybersecurity incidents occur, does intrinsic attention focus on security among the parties involved like users, producers and suppliers. Because IoT is still relatively new and many standards are still under development, it is advisable to think about a number of scenarios that will be decisive in establishing a risk-management ¬strategy to deal with this development.

Another aspect of IoT that occurs in the ICS domain is the extent to which you can undertake modifications to make an apparently vulnerable system secure once again. It may, for example, be the case that a vulnerable system cannot be updated due to physical restrictions, such as a lack of memory. In the case of IoT, there are also instances known in which the manufacturer no longer publishes updates or even provides any support [14].

This chapter will look more closely at those aspects of IoT that will influence your risk-management approach and how to deal with it. Everyone occupied with cybersecurity has to realise that it will never be optimal. You have to stay alert in monitoring and maintaining the security of IoT devices and to constantly strive for improving it. Furthermore, a well-balanced approach is advised, in which you balance the risk factors and use of your resources, so that the business goals of your organisation can be supported. As IoT has a major impact on almost every aspect of an organisation, the uncontrolled use of IoT may lead to new threats, including violation of privacy, leaking of confidential business data or, for example, the manipulation of physical processes through breaches of IoT sensors.

5.1 KEY ASPECTS OF IOT FOR RISK MANAGEMENT

Apart from the aspects above, the following aspects, summarised in a few questions, are also important in determining your risk management strategy:

Do you know the contexts in which (a) part of your IoT ecosystem lies/will lie?

Given that the context in which IoT devices, such as portable sensors, may lie is not always known – or can even change – you cannot apply measures that secure the physical context of IoT devices, or only do so to a limited extent.

Are you able to anticipate the nature and manner in which your IoT ecosystem develops?

The number of components of an IoT ecosystem and how these are related to each other may vary significantly over time. In addition, the quantity of products and versions of IoT devices makes it difficult to predict what components will be used to create a specific functionality. Furthermore, the dynamic character of IoT can quickly create new functionalities, which may sometimes make it impossible to change or control the nature and manner in which IoT ecosystems are created.

Do you know the extent at which the respective parties that you depend on are informed about security for IoT?

The open character of IoT ecosystems and the number of players involved may cause a wide spread of background knowledge and expertise among these parties. It is important to not only secure your IoT devices optimally, but also to find the right security alignment so that they are complementary and don't interfere with each other.

Do you know what 'restrictions' the IoT systems you use exceed?

This may include the (political) policy, the technical platform on which the IoT systems are installed and the geographical separation through which engineering connects the systems in a single chain. Here, the organisation component and even restrictions that go beyond the organisation should be taken into account.

Do you know which actors you must be armed against?

Note that it is not just the IoT system itself that may be the target of an attacker, but it may also serve as a way of getting to the 'crown jewels'. What may initially appear to be an uninteresting system for attackers could well be the main opening to penetrate your organisation, so ensure that the whole chain is well secured. A recent DDoS attack has also shown that the IoT itself can be used as a weapon [15].

5.2 COMPLEXITY AND DYNAMICS AS A RISK-MANAGEMENT SPRINGBOARD

The complexity and dynamics make it too complex to take a 'checklist approach' to dealing with systems. Performing a risk analysis is becoming ever more complex because the physical environment of IoT devices is not always known and is constantly changing in some cases. The constantly changing context means that the physical security of devices cannot be brought under control. Furthermore, this is compounded by the different producers and parties you confront, each of whom has a different background.

The main cause of the complexity of risk management for the IoT is the state of flux in which an IoT device finds itself. What is acceptable in one environment may not be acceptable in another. This is especially relevant for IoT devices that are not connected to a fixed location, such as IoT devices that can move around, for example, drones and industrial robots, or portable IoT devices, such as heart-rate monitors and particulate-matter detectors.

Example
The functionality of a heart-rate monitor can be used in a sports school to ensure that a training programme is followed optimally. Use of that same functionality in a store environment is undesirable, certainly if this is used to determine which products may interest a customer. Privacy legislation provides a good guideline on what is and isn't allowed here. Technical support is possible, but it is necessary to be able to establish the environment in which the heart-rate monitor is located (sports school, store) and adjust the sharing of this information, or not, with other IoT devices in this environment.

Certainly, in the starting phase of IoT related developments, the 'checklist approach' can only be used to a limited degree as other applications are likely to bring new risk factors with them that will have to be managed in an innovative way.

In some application areas, there will be existing regulation that one has to take into account, see also section 3.1. To exemplify, the machine directive and the standard for CE labelling is well regulated and there is already a lot of IoT regulation on the basis of existing legislation. However, in terms of cybersecurity, little or nothing has been regulated. In contrast, in certain application areas, such as the medical domain, a lot of regulation has been established and the relevant risk-management standards should, therefore, act as a basis for the organisational and technical structure, among other things.

5.3 RISK MANAGEMENT AND PERMANENT VULNERABILITIES

While making, and keeping IoT secure is attracting increasing attention, it currently makes sense to assume that new vulnerabilities in IoT devices will no longer be resolved by the supplier after a certain time and will, thus, remain vulnerable. That IoT devices contain enduring and perhaps permanent vulnerabilities may, for example, arise if a supplier chooses to no longer support an IoT device on economic grounds, even though this is still being used in your organisation. If your security approach is fully geared to resolving vulnerabilities, which we refer to as "*resolve the vulnerabilities*", then this could be inadequate for IoT devices.

There are two distinct approaches to deal with this in general. The first approach is based on the replacement of an IoT device. This approach is facilitated by, when setting up an IoT system, taking into account that devices that are vulnerable to attacks – or that do not support new applications – may be removed, switched off or replaced. We call this approach "*remove the vulnerable components*". The drawback of this may be the unavailability of replacement components or that the replacement components offer only part of the required functionality and/or introduce cybersecurity vulnerabilities through offering more functionalities.

The second approach is geared towards isolating IoT devices, in which these devices are given extra protection by a putting a shell around them so that vulnerabilities in the IoT systems cannot be abused. We call this approach "*isolate the*

The main cause of the complexity of risk management for the IoT is the state of flux in which an IoT device finds itself

vulnerable components". Whether this approach is feasible depends largely on the structure of the IoT system and the composition of the IoT ecosystem.

We recommend combining the different approaches and drawing up a good crisis-management plan. This will be particularly necessary if vulnerabilities are suddenly abused on a large scale.

5.4 RISK MANAGEMENT STRATEGY, ARCHITECTURE APPROACH AND STANDARDS

Each of the approaches above influences how you can implement risk management and how this relates to an architecture and the associated role of standards. The appropriate risk-management strategy, and how you can deal with your architecture and standards, are described below. This must fit in a security-management system that is adequately set up in order to deal with risks and incidents.

For "*resolve the vulnerabilities*", an appropriate risk-management strategy targets measures that ensure the further prevention of the vulnerability in the system, for example, by using updates. By targeting the use of secure products (as much as possible), the risk of incidents is sharply reduced, although you must continue to be attentive to the detection of incidents and the subsequent follow-up. Furthermore, you must focus on standards that say something about the security and security assurance of devices.

For "*remove the vulnerable components*", it is important to know which components have to be replaced early on, that is, you need a risk-management strategy which focuses ondetection and threat intelligence. You should focus on standards for interoperability security. You can also examine best practices for monitoring, detection and threat intelligence.

If a vulnerable device is attacked, it will have to be isolated from other systems or system components where possible

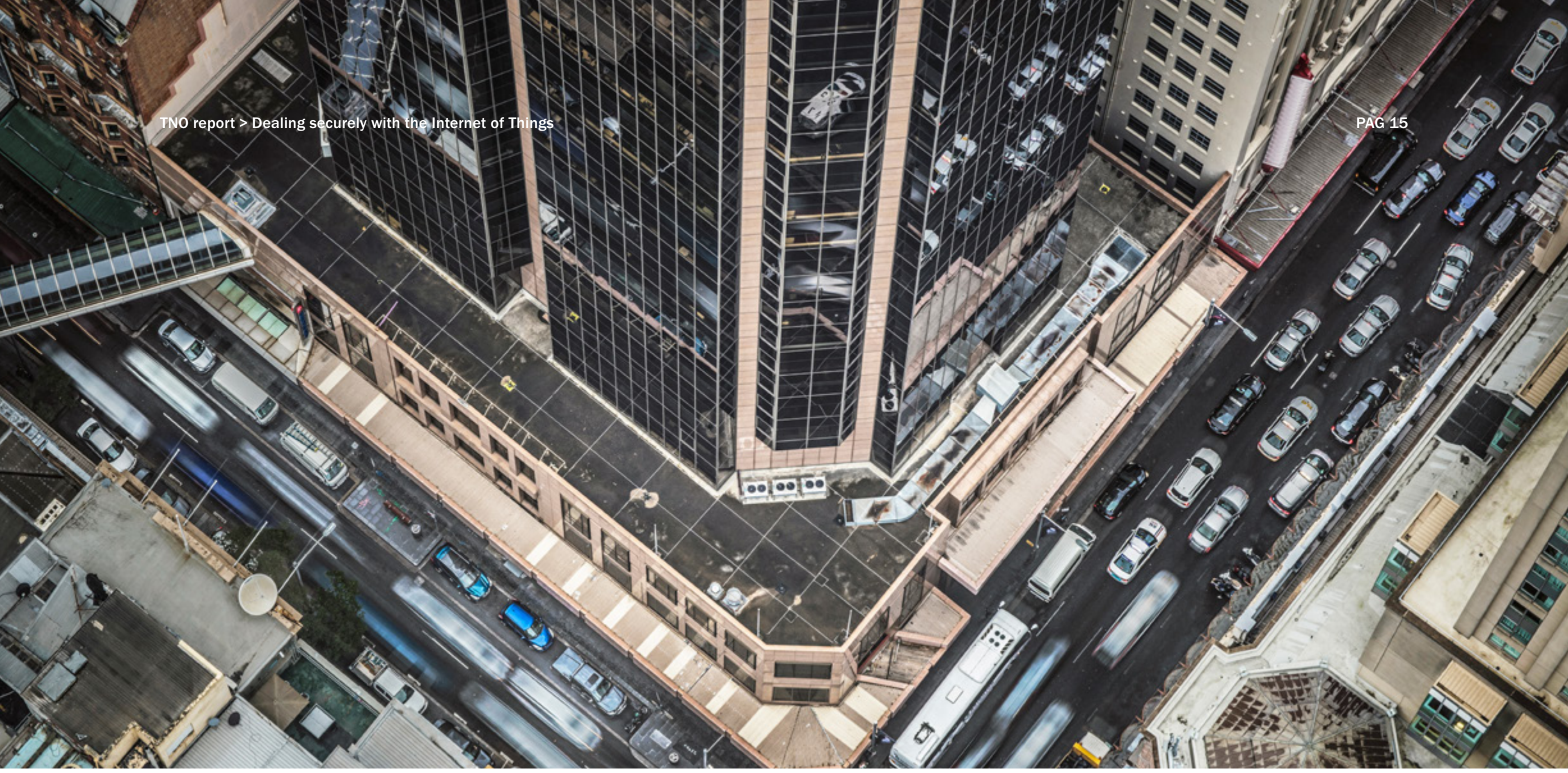
For "*isolate the vulnerable components*", choose a risk-management strategy that targets monitoring both within and at the network edges to determine what systems are vulnerable or may be attacked. You can also enhance this strategy by using threat intelligence. Focus on standards that support perimeter security, plus standards on monitoring and detection (at and within the perimeter). If a vulnerable device is attacked, it will have to be isolated from other systems or system components where possible.

Chart 1 type of approach and focal areas

APPROACH	FOCUS ON
resolve the vulnerabilities	Update or otherwise resolve vulnerabilities in the IoT system.
remove the vulnerable components	Determine which components of an IoT system are vulnerable and, subsequently, remove these vulnerable components.
isolate the vulnerable components	Detect vulnerable components and then isolate these from other components.

5.5 CONSEQUENCES FOR RISK ANALYSIS METHODOLOGIES

In the sketched IoT developments lies a hidden danger that risk analyses will become more and more complex, given the lack of clarity of where the technical and organisational limits of an IoT system lie. In addition, the dynamics of such an environment influence the method of analysis and probably demands modifications to the methodologies. Further elaboration of these aspects, however, is outside of the scope of this guide.



6 DEALING WITH **DYNAMICS** AND **VARIATION IN CONTEXT**

Wireless connectivity is a key element within the IoT ecosystem [1]. As a result, you will have to take the changing contexts in which an IoT device can be found into account. Furthermore, you should consider possible changes in how the connectivity of an IoT device is realised. There are different kinds of wireless connections* that can realise this connectivity, each of which has its own characteristics and possible vulnerabilities.

Since it is becoming increasingly difficult to predict the context in which an IoT device or other parts of an IoT system can be found, it is all the more important to ensure that security measures, where possible, can be adapted to changes in the environment. This chapter considers a few guidelines on how you can take the dynamic character of the IoT into account and the variation in its contexts when determining security measures.

Example

A portable health monitor is used to register heart rate, among others. While this is perfectly suited to following a specific training schedule within a sports school, in the context of privacy concerns, it is not desirable to use the same functionality in another context. Consider, for example, the possibility to monitor your heart rate when shopping to determine the product range you may be interested in as a customer.

6.1 INFLUENCE ON USER CONVENIENCE

To facilitate user convenience, you will have to think about why and what cybersecurity measures must be applied in the IoT ecosystem. For applications with varying contexts, you should – when using a ‘checklist approach’ –, prevent measures that generate (additional) security problems or lower usability when the context changes.

6.2 SENSOR QUALITY

For applications that use IoT devices acting as a sensor, it is essential for you to determine the extent of which the context and correctness of these sensors play a role. The quality of – and trust in – IoT partially depends on the quality of the data delivered by the sensors. Given that new sensors can be connected, there is also a dynamic character present. To this end, you must continually monitor the quality of all the components in an IoT system, including the quality of the data. This creates trust in IoT systems. Monitoring of these components does not only apply to the connection of new devices. It also makes sense to take the decline in the quality of existing devices into account. Over time, the quality of a sensor can decline to below a minimum requirement level. It is, therefore, advisable to calibrate periodically without forgetting to assign minimum and maximum values to the sensors and even statistically determine if there are any

*Like LTE, LoRa, Zigbee and Wi-Fi. It should be noted here that within a group of standards there are also variants that may be developed for a specific application area, such as the Wi-Fi standard IEEE 802.11p specially developed for Intelligent Transport System applications with their own characteristics and security mechanisms.

deviations from expected values. It is important to raise an alert in case deviations are found and to indicate the consequences. An alert may point to an exceptional situation, technical failure or, potentially, a cyberattack.

6.3 COMPOSITION

For a few devices, you can probably predict how they will behave, but this is virtually impossible for a collection of different devices in an IoT system that may differ from each other. Furthermore, the dynamic composition of IoT systems may lead to an unforeseen risk, for example, when a basic functionality of an IoT system is combined with other IoT systems or devices, which may introduce new functionalities or cause existing security measures to no longer perform.

Example
A monitoring system uses information from sensors managed by a third party. Because the sensors are difficult to access, this third party decides, whilst retaining the existing functionality, to replace these sensors with new sensors that support remote firmware updates. This enables, for example, a more flexible adjustment of the intelligence in the sensors without requiring someone to (physically) go to the sensor location.

If this possibility is not taken into account in the security architecture of the monitoring system, a new threat is introduced. Due to a modification of the firmware, this sensor may enable access to the monitoring system and underlying systems.

6.4 FROM ‘DEFINE TIME’ TO ‘RUN TIME’

Many current design and architecture approaches are based on designing a system as ’define time’. In practice, however, you will see that IoT systems increasingly have to be adjustable to ’run time’ during the whole life-cycle. To exemplify, this ‘run-time’ dynamic character can be seen in the intelligence incorporated in IoT devices through, for example, *artificial intelligence* (AI) or *machine learning* that allows a device to react to cyber or physical environments through self-learning functions. Determine the behavioural limits of your IoT system in advance to ensure that this behaviour can be controlled. Instead of monitoring a static environment, you will have to employ new technologies that are able to deal with the dynamic character of an IoT system and support the analysis of specific ‘run time’ conditions [16]. In this way, you can also deploy AI and machine learning to safeguard the security and resilience of the IoT device or IoT system.

Note that all the above can have an impact on how you approach security-by-design. This development is expected tomake it increasingly difficult to predict which physical environment has to be taken into account. For example, it may have an impact on being able to determine the reliability through assurance testing. See also section 7.4 Compositional design.

Many current design and architecture approaches are based on designing a system as ’define time’

7 PREPARING FOR **SCOPE CREEP**

In IoT, an ever-increasing diversity of technologies is being used in an increasingly less controlled environment [17], leading to a growing complexity for security. The fact that the subsystems from which an IoT ecosystem is made up are so diverse, will ultimately generate a large quantity of security threats that will not be easy to counter. The possibility to get more out of the fundamentally open design of many IoT devices – and the often-open infrastructure in which IoT devices are located – will lead to scope creep. It is therefore important to stay up to date with the existing and changing law and legislation. These are vital to being able to manage the scope and possible creep.

Scope creep is the uncontrolled change in – or growth of – the scope of, for example, an (operational) functionality. This may occur if the scope is not well defined, documented and/or managed. If changes occur within the scope, or if there is consensus about the change, then one does not speak of scope creep. The chance of scope creep in IoT arises through the quantity of stakeholders and emerging, sometimes explosive, growth in possibilities. The causes of scope creep are diverse and have an influence in different ways. Different causes are referred to below, along with their influence and an explanation of how you can mitigate these causes.

In addition to scope creep, IoT has the potential to be disruptive. IoT enables new stakeholders to manifest themselves disruptively in an application area.

Example
The availability of new IoT devices for consumers to measure heart rate and blood pressure at home. The sudden emergence of these possibilities has a potentially disruptive effect on a hospital where one is treated. The potentially new information could have an impact on the way one or more hospital information systems operate and are designed.

You may opt to not use IoT within your organisation for reasons of security, yet it may be that innovative, IoT-system based, solutions cause your own business approach to have to be modified in order to comply with the business demands.
This is nothing new. Look at the development of business resources: In the past, the ICT department decided which resources for information processing were used for business and industry. This is now being driven by developments in theconsumer market and by other company departments, such as facility management. This development can also beexpected for IoT and probably at a higher tempo.

7.1 ENGAGING STAKEHOLDERS AND ROLES

You will have to engage a number of stakeholders during the deployment – and updates – of your IoT systems to prevent scope creep. Key stakeholders are:

- From the supplier and system integrator; the project manager. This role anticipates changes in the scope and plans for the healthy growth of requirements, while taking the effect on the (potential) buyers into account.
- From the buyer; the product manager. IoT devices are often subject to updates and changes, and the management of this is, for example, the responsibility of a product manager who will supervise the scope in this role. Note that this may be a task that is outsourced to a third party. Should there be any changes here, he is obliged to inform relevant stakeholders. In some cases, this is explicitly specified in a standard, for example, in healthcare where the ISO/TR 80001 applies. This specifies that suppliers must provide sufficient information to enable a risk assessment.
- Those responsible for business operations: They use IoT and may be various people, both inside and outside your organisation. You should note that these people may have diverse and sometimes conflicting requirements and wishes.
- Users: given that scope creep ultimately affects the end users, they must be represented and engaged as a group.
- Supervisors: If you can provide better insight into your service provision using IoT, the supervisors may also request additional information.

Also, don't forget to engage the relevant people from within your own organisation, like the purchasing department, lawyers, privacy officer, security officer, enterprise architect.

It is recommended to identify all the stakeholders that play a role in your ecosystem and to specify their responsibilities. It is important for you to know all the stakeholders that are relevant to your scope. This will enable you to engage the right stakeholder at the right moment to prevent scope creep.

7.2 MARKET DEVELOPMENTS

The market of IoT solutions is very fleeting, and thus also the (potential) users and their wishes, but this means that the demand on which the initial scope of the IoT is based is no longer relevant for the market. Therefore, as a buyer, you must track the market to recommend the right choice for the purchase of products from producers. This may, for example, relate to the protocols used for communication and to the security standards used. These changes are not easy to predict, but they must be taken care of. It may, therefore, be a healthy reaction to change the scope of your IoT-based solution according to market developments.

The following points help you, as a user, to take account of market developments:

- Pre-align the scope more broadly than the current demand;
- Identify relevant developments in requirements and wishes from other sales markets according to the impact on your application areas;
- Align these developments, where necessary, with relevant stakeholders [18].

Market developments may also affect the required level of security, such as increasing the minimum-security standards. If the dynamics are high, this also requires constant risk management fostered by risk analyses.

7.3 DESIGN AND DEVELOPMENT METHODOLOGIES

The content of scope creep is difficult to predict, yet you can assume this will happen. If you design a process capable of dealing with changes, then this gives you the flexibility to manage scope creep and prepare your organisation for it, while at the same time taking relevant external changes into account, such as amendments to law and legislation.

Security-by-design is a commonly used approach to implement security. It implies that the scope of use of possible stakeholders and the security requirements are already known during the design phase. This contrasts with a long expected duration of use of IoT devices, together with a rapidly changing use context. When designing you could, for example, opt to restrict the functionality of IoT devices as a security measure, taking the restrictions of security-by-design in the context of the aforementioned scope creep into account. This may imply that changes in the composition of functionality – or changes in one of the components used – will affect various other components.

Development methods like agile development actually comprise an open scope that limits the current scope to one or a few iterations. The end product is only realised after a number of iterations whereby a subsequent iteration is regarded as scope creep. In actuality, this can be controlled due to the focus on the scope at every iteration. It is important, however, that you are capable of indicating where and when the security requirements must be incorporated during these iterations.

7.4 COMPOSITIONAL DESIGN

Individual devices can be restricted in functionality, but can also be used as components of a greater whole and, thereby, form an IoT system in which the combination of individual functionalities provide more functionality than can be derived from the sum of the functionalities of the individual components. This can make the scope of the functionality of an IoT system broader, which has implications for its security, for example, because a new functionality also offers new attack possibilities.

Many IoT devices depend on data collection, specifically by sensors. A sensor can be integrated into a larger device and serve this only. However, the availability of the data generated by the sensor also enable the sensor to be used for broader goals, such as the smart meter that can be used to collect data to send consumption and cost summaries every two months. Technically, this can be extended to communicate the actual consumption per second, for example, to very precisely match demand and supply. However, it must be determined whether this technical extension is commensurate with the statutory framework for the smart meter. Any change in use must be considered in terms of the possible consequences for security and privacy.

> Performing an evaluation can lead to gaining a degree of certainty (assurance) that a security solution complies with the requirements. These evaluations are often made for parts or components which, however, are increasingly being employed together with other components. Compositional Assurance [19] is geared to providing assurance for a composite of evaluated components and aims to enable the evaluation (of the security) of different individual components, so as to also apply when these are used together as a whole, even where different combinations are possible.
>
> Compositional assurance is a growing collection of methods you can use. Depending on the application areas, assurance requirements apply. In making the choice about the most suitable method, these requirements will have to be adhered to.

Security-by-design is a commonly used approach to implement security. It implies that the scope of use of possible stakeholders and the security requirements are already known during the design phase

7.5 LIFE-CYCLE MANAGEMENT

Managing scope creep occurs mainly during the maturity phase of the life-cycle of a product, which is when market forces come into play more that causes developers to add functions that may not target the original goal of the buyer. There is also internal pressure to realise other functionalities by drawing on functions of the installed IoT not used to date, with the risk of function creep occurring without taking adequate account of the privacy and cybersecurity aspects, for example, the requirements imposed by European and national law and legislation.

To be prepared for this, you could consider organising pilots on a smaller scale before you scale up and actually deploy. These pilots can teach you where the application of your IoT stands with respect to security by requesting explicit feedback. Should your security be revealed as insufficient during the pilot, then you can still stop the transition and not scale up. This way of dealing with security is also known as security-by-experiment.

In the context of life-cycle management, it should also be taken into account that a component, which is essential for you, may no longer be maintained or supported by a supplier or producer. This situation may arise due to economic grounds with better or cheaper alternatives becoming available in the market. An example of this is a thermostat in the home, whereby the supplier turns off the underlying cloud service [20]. It can be expected, certainly for low-cost devices, that this life-cycle may be a few years, even though the operational function for it demands a significantly longer life cycle. You should bear this in mind during acquisition and use by reflecting on expectations concerning life-cycle management and stipulating in a contract, for example, that support is provided for a minimum period. You must also consider that manufacturers may decide to no longer offer support, causing a vulnerable device that cannot be given a security update.

In addition, it may be the case that new devices cannot work with older IoT devices, for example, because there has been a protocol update and the new device no longer supports the old protocol. Given the speed of a number of developments, this may quickly become the case.

For independently operating devices you will have to consider how actively you can and want to exercise the scope creep on life-cycle management. This is particularly the case when these autonomously operating devices can also be automatically updated. Despite the use of clear descriptions of the change in functionality, a specific functionality could still change or be added. This affects the security scope of products. How you structure control of scope creep depends on how rigorous the control must be and whether this control needs to be fully, or partially, performed each time.

7.6 PRIVACY

Consumers, as well as organisations, must be aware of the fact that privacy can play a role in IoT devices and all the data they collect. An important aspect here is to differentiate between complying with statutory frameworks and the perception of the users. Something which is legally permitted is not necessarily accepted by the users. How your organisation wishes to profile itself in terms of privacy may be a consideration that affects choices in designing and using IoT. In any case, be transparent to your stakeholders about which law and legislation you apply.

Privacy is vital because IoT devices have a direct relationship with the physical world and, thus, potentially have a more powerful impact on the environment. From the very outset of using the devices, it is important to acknowledge and be clear about the possible impact on the privacy of individuals, in particular where this also affects the physical private environment.

Privacy is a much-debated subject in the context of IoT and proposals are being made to safeguard privacy [21]. The Internet Engineering Task Force (IETF) has acknowledged that

IoT has the potential to carry out far-reaching monitoring [22]. Like the Internet Architecture Board (IAB), it has drawn up guidelines [23] to secure privacy in internet protocols, although the protection this offers against privacy violations in a shifting scope is limited.

Innovations on the basis of IoT can lead to new issues about the place of privacy in processing data. In the report "Big Data in a free and secure society" [24], a WRR publication, this subject is explored extensively. In the context of this report, it has been decided to not pursue this subject any further, although a number of guidelines are provided for you below to deal with the matter of privacy in the IoT in a proper way.

In any case, you are advised to allow the end user to keep control, for instance, by asking for approval or confirmation from the user (informed consent) for the use of data. It is important for you to think about how you want to receive approval from the user and at what point in the life cycle this isrelevant. This is essential for compliance with law and legislation, noting that this depends on the country in which the IoT device of the user is found. The earlier the user uncouples his transaction and the data, the more this safeguards the privacy.

Apart from informing the end user about the use of data, it is either way a good idea to be transparent to your end users as well as other organisations with whom data derived from IoT is shared and with whom the data sources of the collected data are shared. In this respect, it is important to take account of how data security across the whole IoT ecosystem can be realised.

To be able to share resources from the IoT, you must stipulate and monitor the access rights and possibilities to use the resource based on the applicable privacy regulations. In addition, ensure that you have an access-control mechanism that is effective against possible attacks on the IoT solution, but which can also be realised in the distributed environment of the IoT and with the sensors and actuators that are used in it.

The literature roughly defines two kinds of access control: role-based and attribute-based. Recently a third method has been defined, the Identity Authentication and Capability Access Control (IACAC) 25, that integrates authentication and access control, which is suitable for the distributed character of devices in the IoT. For the IoT it is important that you have a robust and efficient solution to able to cope with different attacks and whichcan be implemented on different kinds of devices (including the devices with limited processing capacities). IACAC or similar methods are expected to replace the current methods in time, as they are better aligned to the security needs and properties of the IoT.

In addition to these aforementioned forms, you may also consider incorporating activity-based access control in the security-by-design approach for IoT. Depending on the application, the context for use of (sensor) data may be relevant in determining whether data may be used.

However, your focus may not only be on the security of IoT devices themselves. You may also realise that there could be a risk in storing the data coming from these devices. However, this is an issue that lies outside the scope of this document.

It is important for you to think about how you want to receive approval from the user and at what point in the life cycle this is relevant

8 ACKNOWLEDGING **THE DIFFERENCE OF INTERESTS**

Many IoT systems work across several application areas. You must consider that different stakeholders will demand an assertion that the IoT system will not be used for malicious practices. However, in complex IoT systems in which many different stakeholders play a role, you will also be confronted by varied and sometimes conflicting demands.

So, for IoT solutions that will often cross application areas, you must take account of the following:

- Difference in politics (plus a possible difference in law and legislation);
- Difference in country of application (plus a possible difference in law and legislation);
- Difference in organisation (difference in processes, organisation goals, requirements);
- Platform geography (systems at more than one location, data storage, possible influence of law and legislation);
- Components technically connected together as a chain.

Because several parties tend to be engaged in an IoT-systems-based solution, it is important that in managing the risk, you anticipate changes that will emerge from a difference in interests among the different stakeholders. In addition, the costs of security for the producers and value of the security for the buyer must be weighed up for IoT. The difference is that the producers see state-of-the-art security as valuable, while the buyer has to be able to consider the value of the security for the whole life-cycle.

8.1 POSSIBLE STAKEHOLDERS AND THEIR INTERESTS

The figure below illustrates possible stakeholders and their interests. For you, as information security officer, it is essential to know the interests of all the stakeholders, as well as the weight that each stakeholder gives to defending a specific stake.

In the mind map above, the Secure requirement is one of the possible stakeholder interests. Although security should have a major influence on a buyer's decision to purchase an IoT device [27], this does not always have the necessary priority, given the impact that inadequate security (including privacy protection) can have. In addition, security is often not a central aspect among producers [28], suppliers and system integrators, so this has little influence of the selection and set-up of an IoT device. The question you need to ask yourself is whether the low prioritisation of this interest has come about due to a lack of awareness, or is the result of a concrete consideration of the costs and benefits of security. In this matter, it is important for you to realise that there is an interplay in the interests of the buyers and the producers, suppliers and

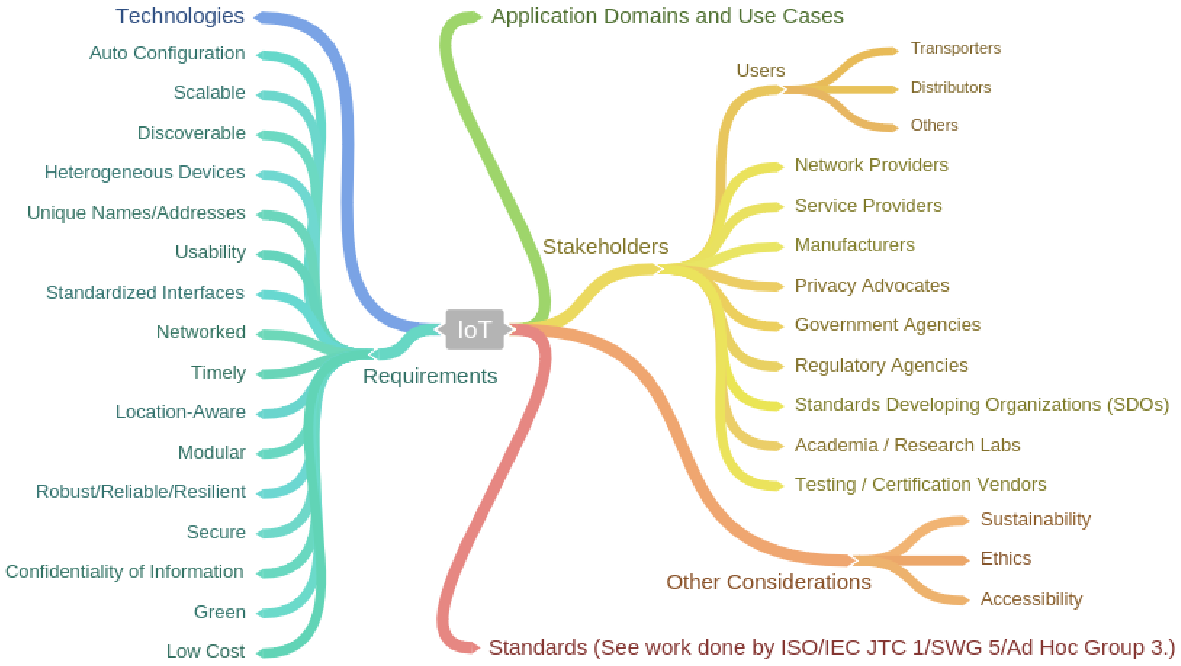


Figure 3 mind map of stakeholders and interests (requirements) [26]

system integrators. If security has a higher priority for the buyer, these parties will also attach greater value to it. And if producers, suppliers and system integrators see the benefits of security, the chance increases that IoT products will become more secure.

As suggested at the beginning of this section, there is a need to identify the interests of all the stakeholders, not forgetting to include the stakeholders in your own organisation, such as the legal department. In the context of the IoT, there is often not only a bilateral relationship between the buyer and supplier (or system integrator). If you see the importance of security yourself, you have another task to convince other stakeholders of this. Only when an entire chain or network takes measures from this perspective, the necessary security can be realised. In this respect, you must take into consideration that the stakeholders and their interest scan vary over the whole life-cycle. To safeguard the acceptance of an IoT system, it is essential for you to consider whether the end user has been considered sufficiently.

To safeguard the acceptance of an IoT system, it is essential for you to consider whether the end user has been considered sufficiently.

8.2 AWARENESS OF THE IMPORTANCE OF SECURITY

The importance attached to IoT security has a lot to do with being aware of the specific risk factors that the absence of IoT security brings with it [2]. Creating this awareness requires the necessary time and money, but it is only after this awareness has been created that a good costs-benefits picture can be drawn for security. This applies both to the end users and certainly also to the management of organisations that co-decide on using IoT in their operation. Are people in your organisation sufficiently aware of how IoT can be abused and how they can be a target of attacks on IoT devices? Be mindful that growing awareness and insight into the possible harm that cyberattacks may lead to security being subjected to changing requirements and interests. Good cooperation with the decision-makers and people in the normal business operation is crucial. You will be asked to identify possible vulnerabilities within your organisation (people and systems) based on the knowledge of the business processes.

8.3 REVIEW AND CONFLICT OF INTERESTS

Stakeholders and their interests may change, as can the context in which the IoT employed is used. Both affect the risk when using IoT devices. Accordingly, you will be aided by having a method that helps review risk factors effectively and iteratively based on changes in (the interests of) stakeholders. You can expect complexity mainly in the many possibilities of connectivity, and the ease of change in the application of IoT devices.

Conflicts of interests may arise at any stage of the life cycle of an IoT system. In addition, conflicts can arise between the interests of stakeholders of IoT devices and non-IoT devices because, for example, these devices conflict in the use of a specific radio spectrum.

Once it becomes clear what the intended goals and technologies of an IoT system are, you should find out what (non-) IoT devices still make use of the same technologies. This may be a cabled internet connection, a specific radio frequency (spectrum) and/or power connections. You need to know this to clarify the possible undesirable effects of an IoT system to relevant stakeholders.

The next step is for you to identify the influence of the IoT system (also the possible use of several versions of the same device), in consultation with relevant stakeholders when possible. The result is that you will have a guide that enables a choice about which IoT system has the least negative impact on the interests of all the relevant stakeholders. This includes other aspects that play a role, such as the points requiring attention concerning management and use of the IoT, for example, the human factor aimed at creating awareness and identifying training needs. In addition, there are additional measures that should be take care of the concerns of the different stakeholders properly. The recommendation here is: work together, share relevant knowledge and learn from each other where possible.

8.4 CREATING TRUST IN PROMOTING INTERESTS

Apart from catering to the interests yourself, you need to create trust that the interests of others are also promoted by an IoT system [26]. This goes together with the required security features of an IoT system. Both depend on the aims of the IoT system. Realise that trust is one of the primary yardsticks of an IoT system becoming accepted.

Trust in the IoT will increase as time goes on, given that the user will transfer part of his/her autonomy to the IoT. The IoT devices will become a physical and mental extension of the user in many cases. The delegation of observation, interpretation and decision-making to an IoT device or IoT system, which will act on behalf of the user in many cases, will contain a major privacy and security risk. It is, therefore, essential for you to take the interests of the users into account and promote these through reliable ICT solutions.

Delivering a reliable ICT solution is additionally made more difficult by the large amount of connectivity and the distributed nature of many IoT systems, creating greater risk of vulnerabilities and associated security incidents.

Example

That there may be a relationship between vulnerable equipment and possible security aspects, is evident from an attack whereby consumers and small-office routers were compromised and the DNS-server setting modified. This gave the attackers control of all DNS requests so that they could trace them to their own IP addresses. While this does not relate to IoT in respect of the criteria applied, it does present a picture of what may be the effect of vulnerabilities in IoT devices. This vulnerability gave the attackers the possibility to simulate trusted websites and present a valid URL, while they had control of the content of the website and the data entered on it by a user.

An IoT system is often constructed of a distributed composite of large and small subsystems. If you want to guarantee trust in – and reliability of – this composite system, mechanisms will be needed that exert security for all subsystems of the IoT system and their mutual interactions. To this end, you must consider how these security solutions can be managed. A mechanism that is useful is the definition of an 'organisational root of trust', in which you assign all the systems used within your organisation authentication data (a certificate or a key) and set up a central environment that validates and authorizes the authentication of the systems used [29] [30]. In this way, you can manage an IoT system securely. The responsibility for authentication and authorisation is, thus, centralised. In addition, modifications and extensions can be performed securely. Existing and new systems can, then, always be authenticated by a central authority [31] [32] [33].

Trust in the IoT will increase as time goes on, given that the user will transfer part of his/her autonomy to the IoT. The IoT devices will become a physical and mental extension of the user in many cases

9 DEFINING A **LIFE-CYCLE-MANAGEMENT APPROACH**

Problems with the security of IoT devices tend to be signalled only when a security problem arises. To safeguard the security of the IoT, security-related criteria must be incorporated during the design and you must ensure that it is reviewed throughout its life-cycle [34]. This enables the security and integrity of IoT systems to be safeguarded from development through deployment, maintenance and to dismantling. This includes, for example, carrying out updates or a method to safely dismantle the IoT system when it comes to the end of its life-cycle.

The costs of life-cycle management can become excessive if the later stages of the life-cycle of IoT devices are not considered from the start. However, you can cut these costs significantly if you consider the following capacities and corresponding, preferably integrated, instruments:

- The possibility to remotely monitor and manage devices. It is not feasible to maintain a growing number of IoT devices if the IoT device must be physically present.
- The possibility to (re)install and (re)configure software on devices that have already been deployed, with the criterion that it is not necessary to be near the IoT device to do so.
- The possibility to test applications using simulation models that are able to replicate the whole system, in which the IoT device is contained, throughout its entire life-cycle. Thisenables you to test applications on a large scale before you use them.
- The possibility to have access everywhere and always to the aforementioned instruments. To this end, the instruments must be in a secure, distributed environment that is accessible for all authorised persons.

9.1 TAKING SECURITY DURING DESIGN, DEVELOPMENT AND TESTING INTO ACCOUNT

Already during the design, you need to consider how security can be safeguarded over the entire life-cycle of the IoT device and IoT system. Therefore, you must take the possible change in the context in which the IoT device is used into account. Security must be addressed in such a way that it remains safeguarded in the event of a changing context. Because different standards exist for connectivity, you must make choices during the design to enable easy integration with th diversity of platforms.

Your development methods must be flexible to enable developers to easily develop applications for deployment on different devices. You can accelerate and design the development more efficiently by using a development platform that is optimised for IoT devices. The risk of error and delay will force you further backwards if it is not stipulated that you must use the devices themselves on the development platform. The development process can also be accelerated by making the development platform accessible everywhere and always to those with authorisation, thereby enabling development teams to work in a distributed manner.

You can also consider using other instruments that can proactively help you find and resolve vulnerabilities, such as external security evaluations and assessments. This can, for example, be done based on the design or a technical assessment, possibly combined with a penetration test. In addition, there are organisations that use bug-bounty programs to invite the security community to search for vulnerabilities and resolve them responsibly[35] [36].

9.1.1 REUSE OF EXISTING FRAMEWORKS

Be aware that incorporating a security-related functionality makes the design more complex and may affect the applications performance. By using a platform that is already configured from a security perspective (secure-by-default), you ensure that the required software components have already been integrated. Known security-related problems in such issues have often already been addressed, which reduces the overall complexity and helps reduce the risk of security gaps due to incorrect configuration. Finally, reuse of such platforms is a time saver. However, you should realise that the more popular an IoT device, the more attractive it is for actors to find and abuse security problems. To this end, consider using existing certification options.

9.1.2 SIMULATE THE APPLICATION BEFORE DEPLOYMENT

Given that an IoT system often contains many components and the performance expectations of such a system are high, developers need a way to test applications on a large scale before they are actually deployed. Particularly when IoT devices that were primarily developed for low power consumption – and not necessarily for performance – are used, such tests can be useful to arrive at an optimal design. Simulation and virtualisation can provide a solution to assess the reliability of an IoT system in advance, making it possible to simulate an entire system without using the actual hardware. You can set up a security-test lab yourself to test the security and reliability of your IoT system.

Additionally, simulation is a useful way to anticipate the risk aspects that may arise during the life cycle of a device through scenarios. Moreover, using a virtual environment makes it easier to detect and resolve errors. You can ensure that not only the instances of where things go well are simulated, but also situations where disruptions are deliberately introduced, for example, as the result of a system breach. A challenge in these simulations is to take the sometimes indistinct borders of an IoT system into account.

9.2 TAKING SECURITY IN INTEGRATION, IMPLEMENTATION AND DEPLOYMENT INTO ACCOUNT

For each IoT device that is deployed, it is important that there is a support infrastructure which can monitor and manage the security of the device, in addition to being able to monitor and manage a large number of same or similar IoT devices. You can achieve this with a platform that can start up, control and modify IoT devices remotely.

In deploying an IoT device, this tends to be part of an existing network of IoT devices with pre-existing agreements on the set of measures to be implemented, such as:

- The influence of the security of this device on the security of the whole network;
- Establishing of the unique identity (certificate management) of this device;
- Distribution of security elements like key material and trusted certificates;
- Checking the security of the device, including the compatibility of the configuration, verification and validation.

This provides you with a good idea whether the system in practice has been implemented according to the security requirements or not. Whether this approach works for your situation is highly dependent on the insight you have into the operational and security features of IoT devices in your whole system. For example, it may be that you only receive the data from a sensor without knowing how this sensor has been set up.

9.3 TAKING SECURITY IN MAINTENANCE INTO ACCOUNT

To prevent working with IoT devices that are no longer secure, you must monitor the security during the operation of the device. A part of this effort is to ensure that the data collected by the IoT device over its entire life-cycle is secure and can only be used for legitimate goals.

It must be possible to request the status of an IoT device when in operation. The management environment must contain a functionality that allows the management and maintenance of the device. This gives you the possibility to discover security leaks and perform updates. Note that this may affect other requirements in certain cases, such as CE labelling or machine guidelines. You can automate many security related tasks, such as performing updates or checking whether a device has security problems. This partially depends on the

Be aware that incorporating a security-related functionality makes the design more complex and may affect the applications performance

updates that the supplier provides and how these take place. It is, therefore, important to take into account how updates are made available and within what period these are made available by the producer. If vulnerabilities are known, for example, because a producer or researcher informs you about them, it is important to know the extent of the vulnerability of your configuration. Having a policy for reporting vulnerabilities [37] can help you deal with vulnerabilities found by third parties in a coordinated way. Try, for example, to gain clarity about which software versions are vulnerable and which ones you have in use. Checking of this can be brought under asset management within your organisation.

Using patches and performing updates on an IoT device must only be carried out by people authorised to do so. This may work well for a single device, but for may present a considerable challenge when considering many devices. In addition, this must not be allowed to influence the intended operation of the device. The security of the IoT device may not be (temporarily) compromised by this or it should be accounted for by, for example, breaking the connection temporarily. Furthermore, the required bandwidth and downtime play a role. This is particularly the case when it comes to IoT devices that perform critical functions, for which thorough updates must be done to ensure minimal downtime, the use of minimal bandwidth, and the elimination of the threat of a security compromise .

Plan in advance how to deal with problems or incidents that do occur. Define procedures to follow up on these incidents. A part of these procedures may be a plan that security analysts can follow for the purpose of escalation, and to have people on standby to investigate and resolve problems.

In drawing up regulations for the maintenance and management of IoT related systems (such as system monitoring and performing updates), a distinction must be made between what can be incorporated during the design and what must – and can – be done once the systems are operational. Take into account that the context in which the system works may change over time, which may affect its maintenance.

9.4 TAKING SECURITY IN DISMANTLING INTO ACCOUNT

Producers should be able to determine the end of the life cycle of an IoT device during the design phase and ensure that the device is replaced at the right moment. You can also consider the condition required to start replacement and the procedures for doing this. This will stop you from working with devices that are no longer secure, or that a device should have been replaced because its life cycle has been exceeded.

Given the large quantity of IoT devices that are in operation, it is likely that you will have to regularly replace IoT devices. Assuch, create a policy and procedures to securely dismantle devices on which sensitive information – such as configuration data and (physical) environment information – is stored or which provide access to such information. Each device must be cleaned up in such a way that all information such as certificates, key material and sensor data is removed and/or the information carriers are sufficiently destroyed. If a device is no longer in service, you must ensure that it does not expose any vulnerabilities through improper use.

Producers should be able to determine the end of the life cycle of an IoT device during the design phase and ensure that the device is replaced at the right moment

10 AND HAVE YOU **ALSO CONSIDERED ...?**

10.1.1 ADDRESSING/GLOBAL REACH

Currently there is no single standard that enables for addressing and reaching all IoT devices. The question is whether this standard will ever come. However, you must – in all cases – consider that IoT devices may and should be reachable in different ways, that they cannot all be managed remotely, and that this may create problems in keeping the security of the IoT devices up to date.

10.1.2 RADIO SPECTRUM

Many IoT devices are connected via a wireless connection that uses frequencies in the radio spectrum. There are several aspects you must consider when using IoT devices that make use of wireless communication. Note that if a device is connected through a cable, a wireless connection may still be active.

The introduction of more wireless IoT devices increases the chance of interference, yet, the different parties that should be playing a role regarding this aspect do not seem to be giving it much attention. Interference may sometimes come from an unexpected source.

Example

The power of a light-advertising board interferes with the frequency of wireless car keys. As a result, cars in the vicinity of these light-advertising boards cannot be opened. Furthermore, the ignition using this wireless key is disturbed, causing it to take several attempts to start a car, or even not at all as long as the light-advertising board is active.

In industrial surroundings, interference can destabilise or prevent the operation of wireless systems used for monitoring or control after the introduction of IoT devices. This can affect the critical functionality for which, if not accounted for, there is no direct alternative available, such as less accurate, cable-connected sensors.

Note that in all situations where different wireless systems are located near each other, interference may arise. Interference is restricted with the policy of assigning small frequency bands for specific purposes, yet, this leads to saturation in these bands if there is an explosive growth of similar devices. An example of interference is Wi-Fi networks on 2.4GHz where, in view of the high urban population density, there is a strong decline in the signal due to the limited choice of frequency channels to establish a Wi-Fi network. Disturbances can also occur outside the communication context. Microwave ovens generate a large amount of energy at different frequency bands and this may cause serious disruption to

Many IoT devices are connected via a wireless connection that uses frequencies in the radio spectrum. There are several aspects you must consider when using IoT devices that make use of wireless communication

wireless communication, such as Wi-Fi. There are also examples of smart meters interfering with telephony networks that operate using LTE* systems.

When acquiring IoT devices you are recommended to check whether the purchased devices comply with current legislation or not. Some IoT devices produced for the American market use frequencies that are not permitted in the Netherlands. The advice is to check which wireless devices are in use and what part of the radio spectrum they use. Furthermore, consider the interference of IoT devices that are not aimed at wireless communication, as these may operate at different frequencies in different countries.

You can anticipate these aspects while designing an IoT system by drafting a plan of emergency in case, for example, the connection fails or becomes unstable. Another option is to use IoT devices that can both detect interference and respond accordingly. In particular, for critical systems, it is recommended that wireless systems are not used whenever possible, or to provide a back-up.
If you find yourself in a situation in which it is difficult to establish the cause of instability, it is good to know that there are agencies that specialise in investigating the causes of interference and/or disruptions.

10.1.3 AD-HOC SYSTEMS

The nature of IoT devices makes it possible to interact in dynamic compositions and configurations. An example is an ad-hoc network , in which mobile or portable IoT devices interact with other devices from different application areas. In such cases, you can use technology that technically facilitates trust structures like a Public Key Infrastructure (PKI). You should supplement this in your own environment by taking extra measures. It may well be that a device is part of a trust structure, but disseminates incorrect information due to an attack. You should consider how this incorrectly functioning device can be recognised and how you can, then, isolate or remove it, in order to ensure that it cannot cause a disruption in your environment or that this disruption can be restricted.

10.1.4 SAFETY, SECURITY AND ASSURANCE

IoT is a key link between the physical and virtual worlds. In cases where these worlds merge, you will have to consider the degree to which physical safety [38] is compromised.

Example
If IoT is used to remotely switch on a hand blender, there is potentially a threat to safety. On the contrary, IoT may also be used to provide a timely alert of high concentrations of particulate matter, in which case the safety context must also be considered. For example, the performance and robustness of the IoT system if it is the primary warning system for a possible health risk. Aswith security, these are requirements supplementary to the functional requirements.

> **If you find yourself in a situation in which it is difficult to establish the cause of instability, it is good to know that there are agencies that specialise in investigating the causes of interference and/or disruptions**

If IoT systems, which are used for safety applications, employ machine learning and artificial intelligence, it generates additional challenges for the interaction with the safety and security domain. While safety requirements demand that the safety level is determined in advance, it will be difficult to demonstrate this if, for example, IoT devices are used that were not designed from a safety perspective. It is, therefore, expected that the use of artificial intelligence or machine learning for safety applications is less acceptable than for the application of those technologies in other IoT-based applications.

*Long-Term Evolution is a fifth-generation standard for wireless mobile networks.

11 BIBLIOGRAPHY

1. Stratix, “Internet of Things in the Netherlands. Applications, trends and potential impact on radio spectrum,” Stratix, 2015.
2. P. De Goede van Eijk, “Meer focus op awareness vanwege IoT,” december 2014. [Online]. Available: https://www.computable.nl/artikel/opinie/security/5209810/1509029/meer-focus-op-awareness-vanwege-iot.html. [Accessed juli 2016].
3. ITU-T, “Y.2060 Overview of the Internet of things,” ITU-T, 2012.
4. U.S. Department of Homeland Security, “Strategic design principles for the Internet of Things (IoT),” U.S. Department of Homeland Security, 2016.
5. S. Yoo, “Working group on Internet of Things,” ISO/IEC JTC1 / WG10, 2015.
6. ISO/IEC, “ JTC 1 Internet of Thing (IoT),” ISO/IEC, 2014.
7. European Research Cluster on the Internet of Things (IERC), “Position Paper on Standardization for IoT technologies,” European Communities, 2015.
8. NEN, “ NEN-EN-IEC 80001-1:2011, Toepassing van risicomanagement voor IT-netwerken en medische hulpmiddelen,” NEN, 2011.
9. Industrial Internet Consortium Security Working Group, “Industrial Internet of Things Volume G4: Security Framework,” Industrial Internet Consortium, 2016.
10. B. t. Ir. Paske, C. Dr. Cuijpers, M. v. Prof. Dr. Eekelen, E. Dr. Ir. Poll and B. v. Drs. Schoonhoven, “Risicoanalyse Slimme Meter Keten,” TNO, Delft, 2012.
11. Alliance for the Internet of Things innovation, “Alliance for the Internet of Things innovation,” [Online]. Available: http://www.aioti.eu. [Accessed September 2016].
12. European Commission, “Alliance for Internet of Things Innovation Online Community,” [Online]. Available: https://ec.europa.eu/digital-single-market/en/communities/alliance-internet-things-innovation-online-community. [Accessed Oktober 2016].
13. A. L. Tao, “IoT security not a priority for Asean organisations,” [Online]. Available: http://www.computerweekly.com/. [Accessed juli 2016].
14. K. Finley, “https://www.wired.com/2016/04/nests-hub-shutdown-proves-youre-crazy-buy-internet-things/,” [Online]. Available: https://www.wired.com/2016/04/nests-hub-shutdown-proves-youre-crazy-buy-internet-things/. [Accessed november 2016].
15. B. Krebs, “KrebsOnSecurity Hit With Record DDoS,” [Online]. Available: https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/. [Accessed november 2016].
16. K. Zhao and L. Ge, “A Survey on the Internet of Things Security,” in Ninth International Conference on Computational Intelligence and Security, 2013.
17. S. Ranger, “Internet of Things: Finding a way out of the security nightmare,” 2016. [Online]. Available: http://www.zdnet.com/article/internet-of-things-finding-a-way-out-of-the-security-nightmare/. [Accessed maart 2016].
18. K. Wiegers, “Defining Project Scope: Managing Scope Creep,” juli 2013. [Online]. Available: http://www.jamasoftware.com/. [Accessed juli 2016].
19. J. Rushby, “Compositional Security Evaluation: The MILS approach,” 2005.
20. WIRED, “Nest’s Hub Shutdown Proves You’re Crazy to Buy Into the Internet of Things,” [Online]. Available: https://www.wired.com/2016/04/nests-hub-shutdown-proves-youre-crazy-buy-internet-things/. [Accessed September 2016].
21. B. Russel, C. Garlati and D. Lingenfelter, “Security guidance for Early adopters of the Internet of Things (IoT),” Cloud Security Alliance, 2015.
22. S. Farrell, It's Often True: Security's Ignored (IOTSI) - and Privacy too, Network Working Group, 2016.
23. Internet Architecture Board, “Privacy and Security Program,” [Online]. Available: https://www.iab.org. [Accessed juli 2016].
24. WRR, “Big Data in een vrije en veilige samenleving,” University Press, Amsterdam, 2016.
25. N. Mahalle, “Identity, Authentication and Capability Based Access Control (IACAC) for the Internet of Things,” in Journal of Cyber Security and Mobility, 2013.
26. ISO/IEC, “ JTC 1 Internet of Things, Preliminary report,” ISO/IEC, 2014.
27. R. Tolido, “Internet of Things staat of valt met security,” 2016. [Online]. Available: http://www.computable.nl. [Accessed juli 2016].
28. Capgemini Consulting, “Securing the Internet of Things Opportunity: Putting Cybersecurity at the Heart of the IoT,” Capgemini Consulting, 2016.
29. IETF, “Internet X.509 Public Key Infrastructure, Certificate Management Protocols,” IETF, 1999.
30. IETF, “Internet X.509 Public Key Infrastructure, Certificate Policy and Certification Practices Framework,” IETF, 2003.
31. GSMA, “GSMA IoT Security Guidelines,” GSMA, 2016.
32. Trusted Computing Group, “Guidance for Securing IoT,” Trusted Computing Group, 2016.
33. ISO/IEC, “11889-1: 2015 Information technology - Trusted platform module library,” ISO/IEC.
34. Wind River, “Managing The Iot Lifecycle From Design through end-of-life,” Wind River, 2015.
35. A. Greenberg, “Chrysler Launches Detroit’s First ‘Bug Bounty’ for Hackers,” juli 2016. [Online]. Available: https://www.wired.com/2016/07/chrysler-launches-detroits-first-bug-bounty-hackers/. [Accessed juli 2016].
36. Bugcrowd, “Fiat Chrysler Automobiles,” [Online]. Available: https://bugcrowd.com/. [Accessed 2016].
37. Nationaal Cyber Security Centrum, “Leidraad om te komen tot een praktijk van Responsible Disclosure,” Nationaal Cyber Security Centrum, Den Haag, 2013.
38. W. Steijn, R. Gallis and E. Luiijf, “Opkomende risico's voor arbeidsveiligheid als gevolg van IT-koppelingen van en tussen arbeidsmiddelen,” TNO, 2016.
39. Embedded France, “S3P Project Announcement,” Embedded France, 2015.
40. R. Orlove, “Here's Everything NHTSA Wants To Know From Tesla,” juli 2016. [Online]. Available: http://jalopnik.com/heres-everything-nhtsa-wants-to-know-from-tesla-1783529317. [Accessed juli 2016].
41. R. Khan, “Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges,” in 10th International Conference on Frontiers of Information Technology, 2012.
42. J. Smit, “Industry 4.0, Study for the ITRE Committee,” European Union, 2016.
43. H. Solomon, “Best spending value is on security awareness, says Microsoft official,” april 2016. [Online]. Available: http://www.itworldcanada.com. [Accessed juli 2016].
44. W. Steijn, E. Luiijf and D. v. d. Beek, “Opkomend risico voor arbeidsveiligheid door inzet van robots op de werkvloer,” TNO, 2016.

AUTHOR(S)

Ir. A.C.M. Smulders
L. Oosterheert MSc
R.H. ten Hove MSc
Drs. J. Adriaanse

REVIEWER

Ir. H.A.M. Luiijf

TNO innovation for life

TNO.NL