The development of cyber security standards for wireless IoT devices in a multistakeholder environment

Assche, Jean-Paul van

Universiteit
Leiden
Governance and Global Affairs

The development of cyber security standards for wireless IoT devices in a multistakeholder environment

Jean-Paul van Assche, MSc
s3088480

Master Thesis, Executive Master in Cyber Security
Supervisors:
Prof. dr. G. Smaragdakis
Dr. T. Tropina

Leiden University
Faculty of Governance and Global Affairs
Cyber Security Academy

January 9, 2023

List of abbreviations

CEN	The European Committee for Standardization
CENELEC	The European Committee for Electrotechnical Standardization
CSA	Cyber Security Act
CRA	Cyber Resilience Act
EC	European Commission
ENISA	The European Union Agency for Cybersecurity
ESO's	European Standards Organisations CEN, CENELEC and ETSI
ETSI	The European Telecommunications Standards Institute
EU	European Union
GDPR	General Data Protection Regulation
IACS	Industrial Automation and Control System
IoT	Internet of Things
NIS Directive	Network and Information Systems Directive
NLF	New Legislative Framework
OJEU	Official Journal of the European Union
RED	Radio Equipment Directive
RFID	Radio Frequency Identification

Acknowledgement

I would like to thank my first supervisor, Professor dr. Georgios Smaragdakis and my second supervisor, dr. Tatiana Tropina, for their guidance and flexibility.

I also want to thank my employer, The Dutch Authority for Digital Infrastructures, who made it possible for me to participate in The Leiden Executive Cyber Security Master's program in the context of which this thesis has been done.

Moreover, I thank my wife for her support.

Abstract

On 29 October 2021, the European Commission (EC) adopted a Delegated Regulation (Regulation (EU) 2022/30) under the Radio Equipment Directive (Directive 2014/53/EU).

This delegated regulation extends the existing requirements for radio equipment with “cybersecurity by design” requirements. Wireless internet-connected devices must comply with these cyber security requirements from August 2024 as a precondition for placing on the market IoT devices in the EU. The Radio Equipment Directive (RED) essential cyber security requirements objectives are to protect the network, ensure safeguards for the protection of personal data and privacy and contribute towards protection from fraud.

The RED cyber security product legislation is part of the New Legislative Framework (NLF). The NLF establishes common procedures for placing products on the EU market. Its goals are establishing a proper functioning of the internal market and a high level of public interest protection. It contains common methodologies for product requirements via essential requirements, demonstration of compliance by manufacturers and monitoring of the compliance by supervisory authorities.

In line with the NLF approach, the RED essential cyber security requirements set “objectives to be achieved” but do not impose technical solutions. A formal standardisation process exists in which essential requirements are converted to technical solutions in harmonised standards. The realization of this process is the responsibility of a specific joint committee of the multi-stakeholder standardisation organisations CEN (The European Committee for Standardization) and CENELEC (The European Committee for Electrotechnical Standardization CENELEC).

The EC requires, in its EC standardisation request, that technical solutions (to be included in the harmonized standards for IoT devices) are proportional to the cyber security risk they aim to address. However, the RED legislation and the EC standardisation request do not provide information on accomplishing this. Moreover, there is currently no harmonised standard available for the cyber security of products that can serve as an example for the harmonised standards to be developed in support of the RED cyber security essential requirements.

This thesis develops a model that can be used in standardization activities for the RED to determine whether technical solutions in harmonised standards for IoT devices are proportionate to the risk they aim to address.

The developed model is referred to as the “RED cyber security management system” The model maps the RED processes in three layers. The Risk Governance layer maps the legislators' processes regulating the cyber risks of IoT devices. The Risk Management layer maps processes that members of standardization organizations perform in the development of RED harmonized standards. The Risk Assesment layer maps the processes for selecting technical solutions for RED harmonized standards. This thesis proposes to incorporate the ISO 27005 Risk Management framework and the Open FAIR Risk Assesment framework in the “RED cyber security management system”.

The developed “RED cyber security management system” has shown to be beneficial for linking technical requirements to IoT devices. It was shown in a simple IoT scenario that the model could be used to determine the applicability of authentication and access control mechanism requirements for IoT devices.

Table of Contents

1 Introduction

Need for product legislation for Internet of Things (IoT) devices

When looking for the range of "smart" devices on e-commerce websites, it is noticeable that many smart devices are offered. These are products like smart cameras, smart doorbells, smart thermostats, smart baby monitors and smart lighting. These devices are called smart because they are connected to the internet and can be controlled and read remotely.
`

Studies such as [1] and [2] show that many of these devices are insecure because the design does not meet the "security by design" principle or because no or sufficient security updates are provided. Using insecure smart devices can pose privacy and security risks. They can become infected with malware, making them part of a botnet that attacks websites or sends spam. Sensitive data, such as camera images, can fall into the wrong hands, and smart devices can be manipulated.

The EC states that there are few disincentives for manufacturers to place insecure equipment on the market at a lower price. Because a consumer often has no insight into or expertise about the cyber security of a product, an insecure but cheap device will be sold more easily [3, p. 17]. Meanwhile, more and more IoT devices are being used. Cisco predicts that by 2023 there will be nearly two machine-to-machine IoT devices per capita of the world's population. Connected home applications will present half of this [4].

Regulatory gap analysis [5] by the European Commission (EC) shows that only a few product categories must meet cybersecurity requirements for market access. As a result, supervisory authorities cannot prevent insecure devices from being sold in stores. Not all consumers realise that the use of insecure devices entails risks in terms of privacy and security[1].

The cyber security legislation currently in force, such as the General Data Protection Regulation (GDPR) [6], the Network and Information Systems Directive (NIS directive) [7] and the Cyber Security Act (CSA) [8], are voluntary or are not aimed at manufacturers, distributors and importers involved in the manufacturing or sale of IoT devices. This lack of applicable regulation makes it impossible for supervisory authorities to prohibit manufacturers from placing insecure devices on the European market. This regulatory gap has also drawn the attention of Member States in Europe[2]. Several member states, including the Dutch Authority for Digital Infrastructures, indicated in European forums the importance of mandatory cyber security requirements for IoT devices [9].

Recent developments in product regulations for IoT devices

In the EU's Cybersecurity Strategy for the Digital Decade [10] of December 2020, the EC announced various measures to raise cybersecurity in Europe to a higher level. One of the proposals from this strategy concerns improving the cybersecurity of devices through “a

[1] The EC Special Eurobarometer from 2019 [59] states that 47% of EU respondents said they do not feel well informed about cybercrime.

[2] https://emagazine.one-conference.nl/2021/eu-mandatory-cyber-security-requirements-for-wireless-devices/

comprehensive approach, including possible new horizontal rules to improve the cybersecurity of all connected products and associated services placed on the Internal Market" [10].

On 29 October 2021, the EC followed this up and adopted a delegated regulation [11] under the Radio Equipment Directive [12]. This delegated regulation extends the existing requirements for radio equipment with "cybersecurity by design" requirements. Wireless internet-connected devices must comply with these cyber security requirements from August 2024 as a precondition for placing on the market IoT devices in the EU. From that date, supervisory authorities can withdraw insecure IoT devices (which are placed on the market after that date) from the EU market.

The "delegated regulation" with cybersecurity requirements is exclusively aimed at wireless internet-connected devices because the cybersecurity requirements are part of the Radio Equipment Directive (RED), which only concerns devices that can communicate wirelessly.
The disadvantage of the limited scope is offset by the speed with which the delegated act could be adopted and will apply. However, most IoT devices [3] contain a wireless communication function such as Bluetooth or WIFI and, if they can communicate via the internet, fall under the RED scope, which means that they must comply with the mandatory cyber security requirements under the RED from August 2024.

On 15 September 2022, the EC submitted[3] a new legislative proposal [13], the Cyber Resilience Act (CRA). This proposal concerns a horizontal (sector-wide) product regulation for the cyber security of hardware and software products. The law is aimed at manufacturers and other economic operators. The Council and Parliament are currently negotiating this. The requirements under the CRA may eventually replace the cyber security requirements under the RED.

RED essential cyber security requirements as a condition for placing on the EU market of wireless IoT devices

From August 2024, manufacturers must fulfil the RED cyber security product requirements to place wireless IoT devices on the European market. Manufacturers shall design and construct wireless IoT devices to comply with three essential cybersecurity requirements, which aim to protect the network, ensure safeguards for the protection of personal data and privacy and contribute towards protection from fraud [14],[11].

Development of harmonised standards

The RED essential cyber security requirements set "goals" but do not give technical solutions that are needed to fulfil these "essential requirements". Therefore, a formal process has been provided in which the essential requirements are elaborated in technical specifications. This process is called standardisation and starts with an official request from the EC (EC standardisation request) to the Official European Standards Organizations (ESOs)[4] to develop harmonised standards. The standardisation process applies to many European product legislation acts and is formally laid down in the Standardisation Regulation [15]. Harmonised

[3] Press release: https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act
[4] The three Official European Standards Organizations are CEN, CENELEC and ETSI

standards can help manufacturers with the conformity assessment because the requirements and technical elaborations contained therein are specific and formulated in detail.

If a manufacturer successfully applies (implements and tests) the standard's requirements, this is sufficient proof of conformity with the essential requirements. This gives legal certainty to the manufacturer.

CEN (The European Committee for Standardization) and CENELEC (The European Committee for Electrotechnical Standardization) facilitate the standardisation activities for the RED cyber security essential requirements. The CEN/CENELEC standardisation committee JTC13-WG8 started the standardisation work in August 2022. The committee is accessible to all interested parties so that it can be regarded as a multi-stakeholder platform.

Via a so-called "EC standardisation request" [16], the EC has requested CEN/CENELEC to develop three harmonised standards. The standardisation request also gives guidance concerning certain technical specifications the harmonised standards should contain to address each essential requirement adequately. However, there is freedom for the standardisation committee to decide which technical specifications the harmonised standards shall include. However, the harmonised standard must lead to compliance with the essential requirements and the provisions of the EC standardisation request.

This thesis answers the research questions below and proposes a model to determine if technical solutions (to be included in the harmonized standards for IoT devices) are proportional to the cyber security risk they aim to address.

The results will be used as input for the standardisation activities in CEN/CENELEC, which started in August 2022, and in which the writer of this thesis participates on behalf of the Dutch Authority for Digital Infrastructures (Ministry of Economic Affairs and Climate Policy).

Research question 1 (Risk-based technical solutions in standards)

The EC standardisation request [17] states: "The technical solutions laid down in the harmonised standards shall be *proportionate to the risk* they aim to address."

Which criteria and models could be used to determine if technical solutions in the harmonised standards for IoT devices are proportionate to the cyber security risk they aim to address?

Based on EC guidance documents, EU legislation and EC websites, **Chapter 2** examines the functioning of the internal market for products and the concept of essential requirements that apply as a condition for placing these products on the EU market. It also briefly discusses the origin of the NLF product regulations as we know them in Europe today. Finally, the adequacy of the NLF product regulations is questioned, and a look is given to the future in which product requirements must curb the risks of devices in the light of increasing digitalisation, the circular economy and artificial intelligence.

Chapter 3 examines how European product legislation, essential requirements, standardisation requests and harmonised standards are established, how they relate to each other and who is responsible for adopting them. Also, the level of protection pursued by the essential requirements is examined. The European Vademecum on Standardisation [18]–[20], EC guidance documents, EU legislation, and EC websites are the basis for this research.

Chapter 4 examines the Radio Equipment Directive and the three RED essential cyber security requirements, the requirements in the EC standardisation request, and the associated standardisation activities in CEN/CENELEC. For this research, the Radio Equipment Directive [12], the delegated regulation 2022/30, which activates the RED cyber essential requirements [11] and the EC standardisation request [16] are used.

Chapter 5 examines the European cyber security regulatory landscape. For this research, several relevant pieces of EU cyber security legislation and a regulatory gap analysis [5] made by the EC are used. With information and insights from the previous chapters in

Chapter 6 develops a fictitious management system with three layers to map all RED processes: The Risk Governance layer maps the legislators' processes regulating the cyber risks of IoT devices. The Risk Management layer maps processes that members of standardization organizations perform in the development of RED harmonized standards. The Risk Assesment layer maps the processes for selecting technical solutions for RED harmonized standards.

Chapter 7 examines various existing Risk Management and Risk Assesment frameworks. The chapter concludes by selecting a Risk Management and Risk Assesment framework that can be integrated into the fictitious "EU internal market" management system to address the standardisation processes. For this research, several Risk Management and Risk Assesment standards are used.

Chapter 8 answers research question 1 by explaining the proposed "RED cyber security management system" model. The model consists of the "Internal market management system", in which the ISO 27005 Risk Management system and the Open FAIR Risk Assesment model are incorporated. This model enables stakeholders participating in the RED standardisation process to determine whether technical solutions in harmonised standards for IoT devices are proportionate to the risk they aim to address.

Research question 2 (Applicable and appropriate technical solutions)

The EC standardisation request states: "Harmonised standards "….." shall contain technical specifications that ensure at least that those" *IoT devices*, "where applicable: implement appropriate authentication and access control mechanisms."

Could the criteria and models identified in research question 1 be used

- to determine the applicability of authentication and access control mechanism requirements for IoT devices? and
- to determine the appropriateness of specific authentication and access control mechanisms for particular IoT devices?

Chapter 9 researches a standardized way to describe IoT devices and systems. To this end, a literature study is conducted into the functional components of an IoT device, conceptual models of IoT networks and IoT reference architectures.

Chapter 10 discusses the second research question. The proposed "RED cyber security management system" is used for selecting suitable and appropriate technical authentication solutions for an IoT device in a simple scenario. Information on technical solutions for authentication is gathered from standards IEC 62443-3-3 [21], ETSI 303645 [22] and NIST IR 8425 [23]. Information from IEC 62443-3-3 [24] is used for the threat actor categories.

The thesis ends with a conclusion in **Chapter 11**

2 European legislation for placing products on the market

This chapter examines the functioning of the internal market for products and the concept of essential requirements that apply as a condition for placing these products on the EU market. It also briefly discusses the origin of the NLF product regulations as we know them in Europe today. Finally, the adequacy of the NLF product regulations is questioned, and a look is given to the future in which product requirements must curb the risks of devices in the light of increasing digitalisation, the circular economy and artificial intelligence.

2.1 From national to European product legislation[5]

Since the establishment of the European Union, European product legislation has developed from predominantly national regulations to European harmonised product legislation. Gradually, attempts were made by the EC to remove trade barriers between Member States and to promote the "free movement of goods".

Before 1986, the so-called "Old approach", a traditional approach in which national regulators incorporated detailed technical product requirements into their national laws, applied. It proved difficult for member states to agree on these detailed requirements. As a result, European harmonisation was challenging to achieve.

In 1983, a European directive was adopted requiring Member States to notify other Member States and the European Commission of new national technical regulations. Case law on the application of European agreements on the "mutual recognition of goods"[6] led to the legal interpretation that Member States are only allowed to restrict trade from other Member States if the product does not meet "essential requirements". These are requirements to protect public interests (such as safety, health and security). Properties of products not related to the protection of public interests should no longer be a reason to restrict trade within the EU. In 1986, this heralded the era of the "New approach" to product regulation, which was further improved in 2008 and has since been named NLF (New Legislative Framework).

The " New Legislative Framework" (NLF) exists currently of "Decision 768/2008/EC Common framework for the marketing of products" [24], a "Regulation for accreditation and market surveillance" [25], and a "Regulation on market surveillance" [26].

[5] Information from the European Commission's "Blue Guide on the implementation of EU product rules 2022" [27] has been used in this paragraph.

[6] The Treaty on the Functioning of the European Union [31] include provisions on "mutual recognition of goods". These provisions indicate that national technical regulations may not lead to quantitative restrictions or measures having equivalent effects.

2.2 The New Legislative Framework (NLF)

European product regulation consists of several different product legislation acts. To be allowed to place products on the market, manufacturers must comply with the applicable product legislation acts. Some products must comply with more than one product legislation act[7]. In order to promote coherence and consistency between the various acts, these acts are aligned as closely as possible by including so-called "reference provisions".

These are standard texts that, where applicable and where possible, are literally included in the product act. These reference provisions are listed in Decision 768/2008/EC Common framework for the marketing of products" [24]. When drafting new product legislation, legislators may deviate from the reference provisions if there is a good reason to do so. Deviating too often would be detrimental to the coherence and consistency of product regulation.

2.2.1 Essential requirements

The NLF product regulations follow the following principles for the essential requirements [24],[27]:

- "Product legislation should be limited to the essential requirements that are of public interest;
- Essential requirements are designed to provide and ensure a high level of protection;
- Essential requirements define the results to be attained or the hazards to be dealt with but do not specify the technical solutions for doing so;
- The technical specifications for products meeting the essential requirements set out in legislation should be laid down in harmonised standards which can be applied alongside the legislation;
- Products manufactured in compliance with harmonised standards benefit from a presumption of conformity with the corresponding essential requirements of the applicable legislation".

In addition to essential requirements, the product legislation acts also contain provisions on the responsibilities of manufacturers, distributors and importers, the CE marking, the conformity assessment procedures, the use of harmonized standards, the declaration of conformity and the market enforcement.

The RED is one of the many[8] product legislation acts that is based on the NLF 'reference provisions' from Decision 768/2008/EC.

[7] For example, a medical device that communicates wirelessly must comply with both the Radio Equipment Directive [12] and the Medical Device Regulation [37].
[8] Annex A lists about 30 product legislation acts that are aligned with the reference provisions of the NLF framework of Decision 768/2008/EC.

2.2.2 Conformity assessment of products by manufacturers

Conformity assessment is the responsibility of manufacturers and concerns the process of showing that a product fulfils the essential requirements.
Manufacturers can use harmonised standards in NLF product legislation to demonstrate that their product meets the essential requirements. The manufacturer may determine the product's conformity with the essential requirements for many product groups without engaging an independent third party, provided that the manufacturer tests the product against the harmonised standards. However, the use of a harmonised standard is never mandatory. The manufacturer can choose to meet the essential requirements not using a harmonised standard. In that case, however, most product legislation acts (including the RED) require a third party (notified body) to be involved in the conformity assessment of the product.

2.2.3 Market enforcement

Verification of conformity with the essential requirements by national market surveillance authorities never takes place beforehand but always takes place after the manufacturer has placed the product on the market. National market surveillance authorities can carry out random checks or checks based on complaints, incidents or estimated risks and possibly impose measures.

2.3 Single EU market for goods[9]

With harmonised product regulations, the EU strives for a "single market for goods" in which the same conditions apply to the trade in products in every EU country. This internal market has already been established in Europe for many product categories (such as medical devices, radio devices, machines, toys, measuring and weighing devices, and elevators). Appendix A contains a list of various harmonised product legislation acts that are (highly) aligned with the NLF reference provisions.

As a precondition for placing the product on the EU market, each product from a particular equipment category must comply with specific requirements (essential requirements) which are equal for all EU countries. These requirements ensure that products do not harm public interests, such as safety, health and security. Member States may not impose additional requirements that could impede trade.

The characteristic of the single market of goods is that product requirements may only relate to protecting public interests (such as safety, health, security and the environment). The (mandatory) product requirements are defined in the product legislation acts (directives and regulations) as objectives without specifying the technical details and are referred to as “essential requirements”. Harmonised standards, which are created by recognised standardisation organisations[10] (via multi-stakeholder technical committees) and subsequently approved by the EC and published in the Official Journal of the European Union (OJEU), contain technical elaborations that allow manufacturers to demonstrate compliance with the essential requirements.

[9] Information from the EC website [60] is used in this paragraph.
[10] CEN, CENELEC and ETSI.

The use of harmonised standards has the advantage that, based on the precise technical details in this standard, the manufacturer has a straightforward assessment framework to determine whether the product complies with the harmonised standard and, thus, with the essential requirements. In the “single market for goods”, manufacturers can market their products throughout the European Union without trade barriers, provided that the essential requirements are met. The manufacturer indicates, with a CE mark on the device, that it meets all essential requirements.

The "single market" has the advantage for manufacturers that they have relatively easy access to a large market with 450 million consumers. Since there are no trade barriers in the single market, the same type of product can be sold in all EU countries without the need for national technical adjustments, which benefits the unit cost of products. EU citizens can benefit from lower prices, more innovation and faster technological development, while high levels apply to safety, environmental protection and other public interests.

2.4 Evaluation of the NLF

On 11 November 2022, the EC published a “commission staff working document” on evaluating the NLF [28]. In the context of this evaluation, a consultation was held, and an external research agency produced a research report [29] that the EC used in the evaluation document.

The researchers indicate that the NLF reference provisions are no longer always appropriate due to new market developments and trends in digitisation, artificial intelligence and the circular economy. The procedures and reference provisions of the NLF should be better designed for this. For example, cyber security protection should not only apply when placed on the market, but economic operators (manufacturers, distributors, importers) should take responsibility for this throughout the entire life cycle through security software updates.

The NLF is based on fulfilling the essential requirements at the moment of the “placing on the market”. This is when a manufacturer first makes available on the market a product in the EU in the course of commercial activity. According to the traditional NLF, the essential requirements are met then, and the manufacturer's responsibility ceases after this moment. To adequately curb the cyber risks of a product with digital elements, it is necessary to be able to set post-market requirements, such as mandatory software updates. The changing behaviour of a device through machine learning and artificial intelligence is also difficult to regulate if no post-market requirements can be set.

With the development of the circular economy, new types of economic operators, such as repairers, refurbishers, remanufacturers and software developers, are emerging. These economic operators are currently not addressed in the NLF. The researchers argue for the harmonisation of roles and obligations of these market participants over the entire life cycle of products. The EC concludes that to remain relevant; the NLF must be adapted to new market developments such as digitalisation, AI and the circular economy. Otherwise, legislators will increasingly deviate from the common NLF framework when making regulations, jeopardising the coherence and consistency of product regulation.

3 The establishment of essential requirements and related harmonised standards

This chapter examines how European product regulations, essential requirements, standardisation requests and harmonised standards are established, how they relate to each other and who is responsible for adopting them. Also, the level of protection pursued by the essential requirements is examined.

3.1 Harmonised standards

Harmonised standards play an important role in European product legislation [30]. The formal role of harmonised standards in the NLF is laid down in the "Standardisation Regulation 1025/2012 [15]. In this regulation, a "harmonised standard" is defined as a "technical specification[11], adopted by a recognised standardisation body adopted on the basis of a request made by the Commission for the application of Union harmonisation legislation" [15, p. 19].

An important element in the definition of the harmonised standard is that it has to be developed for the benefit of "Union harmonisation legislation" (referred to as product legislation acts in this thesis). Legislation must first have been developed and approved before a harmonised standard can be developed. Another important element is that a harmonised standard is developed in response to a request from the EC to a recognized standardisation organization.

3.2 Development of EU product legislation

Figure 1 concerns the development of the product legislation act. The European Commission has "the right of initiative" in this law-making process. This means that the EC is competent in planning, preparing and proposing new European legislation. Proposals are planned in an "Annual work program"[13].

Annex A contains a table in which various realised product legislation acts are included. The type of legislation can be a directive or a regulation. A "regulation" is a binding legislative act. It must be applied in its entirety across the EU. A "directive" is a legislative act that sets out a goal that all EU countries must achieve[12]. In practice, this means that when implementing European legislation into national regulations, Member States must implement the literal legal texts in the case of a "regulation". In contrast, in the case of a directive, national laws may be

[11] 'Technical specification' means "a document that prescribes technical requirements to be fulfilled by a product… and which lays down one or more of the following: the characteristics required of a product including levels of quality, performance, interoperability, environmental protection, health, safety or dimensions, and including the requirements applicable to the product as regards the name under which the product is sold, terminology, symbols, testing and test methods, packaging, marking or labelling and conformity assessment procedures " [15, p. 19].

[12] https://european-union.europa.eu/institutions-law-budget/law/types-legislation_en

made that pursue the directive's objectives. The legislator decides to choose between directive and regulation. For example, the RED is a directive and the CRA recently proposed by the EC is a regulation.

Before the EC makes a legislative proposal, if a significant impact is expected, an impact assessment is carried out to determine the law's impact. The Regulatory Scrutiny Board, an independent committee within the EC, assesses the quality of the impact assessment[13]. The EC submits the legislative proposal to the Council (Member States) and the European Parliament. In the case of "Ordinary legislation", the Council and Parliament decide on the final text before it is implemented into EU law.

In various product legislation acts, the Member States and European Parliament have authorised the EC to adopt acts. These acts are called delegated acts which give the authority to the EC to amend or supplement existing legislation[14]. This special power of the EC must then be included in the relevant product legislation acts.

3.3 Development of essential requirements

Each product legislation act specifies the essential requirements that products must meet. The essential requirements must provide a high level of protection. This follows from Art. 114 of "the Treaty on the Functioning of the European Union" (TFEU) [31], which states:

> "The Commission, in its proposals … concerning health, safety, environmental protection and consumer protection, will take as a base a high level of protection, taking account in particular of any new development based on scientific facts. Within their respective powers, the European Parliament and the Council will also seek to achieve this objective".

Decision 768/2008 [32] "on a common framework for the marketing of products" states ([32] preamble 11 and 17).

> "The essential requirements should be worded precisely enough to create legally binding obligations. They should be formulated so as to make it possible to assess conformity with them even in the absence of harmonised standards or where the manufacturer chooses not to apply a harmonised standard. The degree of detail of the wording will depend on the characteristics of each sector."

> "Products that are placed on the Community market should comply with the relevant applicable Community legislation, and economic operators should be responsible for the compliance of products, in relation to their respective roles in the supply chain, so as to ensure a high level of protection of public interests, such as health and safety, and the protection of consumers and of the environment, and to guarantee fair competition on the Community market."

[13] https://ec.europa.eu/info/law/law-making-process/planning-and-proposing-law_en
[14] https://ec.europa.eu/info/law/law-making-process/adopting-eu-law_en

The EC guidance document (Blue Guide [27, Para. 4.1.1]) states:

> "Essential requirements are designed to provide and ensure a high level of protection. They either arise from certain hazards associated with the product … or its performance …, or lay down the principal protection objective ... Often they are a combination of these".

3.4 The development of the EC standardisation request

The EC standardisation request is the assignment the EC gives to the ESOs (recognised European Standard Organisations) to develop standards supporting Union product legislation. When formulating the assignment in the standardisation request, the EC provides direction and explanation about the process and contents to the relevant ESOs, which forms the basis for the standardisation activities.

The "Vademecum on European Standardization" [18]–[20] guidance documents clarify this. It is intended for the EC and all parties involved in standardisation, such as the recognised European Standards Organisations (ESOs). The vademecum consists of three parts [18]–[20] and describes, among other things, the role of the EC in developing a standardisation request in support of Union product legislation. It states [18, pp. 9–10]:

> "The legal requirements, e.g., essential requirements laid down in legislation and requirements in a standardisation request, should be defined precisely in order to avoid misinterpretation on the part of the ESOs or leaving them to make political choices. This is fundamental to allow those preparing standards in support of Union legislation to provide high-quality specifications, as all political choices are to be made by the legislator".

> "A standardisation request may ask that deliverables (such as harmonised standards) be based on legally binding requirements in Union legislation".

The Vademecum on European Standardisation [19] explains the preparation and adoption process of the European Commission's standardisation request. The EC draws up the standardisation request. Internal (within the EC) and external (Member states, stakeholders) consultations occur. In the committee on standards, the Member States vote. If the result is positive, the standardisation request is accepted by the EC and sent to the ESOs.

3.5 Development of draft harmonised standards

With the standardisation request, the recognised European standardisation bodies (ESOs) CEN (The European Committee for Standardization), CENELEC (The European Committee for Electrotechnical Standardization) and ETSI (The European Telecommunications Standards Institute) are invited to develop draft harmonised standards for product regulation. If the ESOs accept the standardisation request, the harmonised standards will be developed within the framework of the EC standardisation request.

Harmonised standards contain technical specifications that take into account the provisions of art. 10 of the "standardisation regulation" [15]. This regulation states that "European harmonised standards shall be market-driven, take into account the public interest as well as the policy objectives stated in the standardisation request and are based on consensus."

The preparatory work is carried out in technical committees of the ESOs.
Standardisation activities take place in CEN, CENELEC or ETSI and are based on consensus in the technical committee. The draft harmonised standard is sent to the CEN CENELEC or ETSI members for comments or votes. If the vote is positive, CEN, CENELEC or ETSI send the draft standard to the EC for approval.

3.6 Assessment of draft harmonised standards by the EC

Article 10(5) of the Standardization Vademecum [18] lists the criteria on which the EC assesses the draft harmonised standard. The most important criteria concern whether the requirements in the standardisation request are met and whether the essential requirements are sufficiently addressed.

3.7 Publication of Harmonized Standards in the OJEU

The EC checks if the draft harmonised standard fulfils the criteria mentioned in paragraph 3.6. After approval, the reference of the harmonised standard is published in the OJEU and gives a "presumption of conformity" with the essential requirements.

According to article 11 of the standardisation regulation [15], the Member States and the European Parliament may submit a formal objection against the standard, resulting in an amendment or withdrawal of the harmonised standard.

3.8 Conclusions

Figure 1 shows the process of establishing harmonised standards based on essential requirements in EU product legislation and requirements in the standardisation request.

Essential requirements conclusions[15]
Essential requirements, as described in product legislation acts, must provide a high level of public interest protection, be precisely defined and aim at protection against 'hazards', guaranteeing a minimum performance or the achievement of protection objectives.

The EC prepares and proposes product legislation acts, but Member States and European Parliament must approve them (see Figure 1). In special cases, the EC is authorised to adopt

[15] See Chapter 3.3 for references.

legislation itself. These acts are called delegated acts. In these cases, the EC itself has the authority to amend or supplement existing legislation.

EC standardisation request conclusions[16]

The requirements in the EC standardisation request must be based on the legally binding requirements (essential requirements) from the relevant product legislation act. Furthermore, the requirements must be precisely formulated. Political decisions about interpreting the standardisation request must be prevented from being taken in the ESOs. Political decisions may only be taken by the legislator (Member States, European Parliament and the EC).

The EC prepares the standardisation request. Member States are involved in the approval of the EC standardisation request (see Figure 1).

Harmonised standards conclusions[17]

European harmonised standards are prepared by ESOs, shall be market-driven, take into account the public interest, and the policy objectives stated in the standardisation request and are based on consensus.

The EC checks the draft harmonized standard to see if the requirements of the standardisation request are met and whether the essential requirements are sufficiently addressed.
Member States and the European Parliament may submit a formal objection against the standard, which may result in an amendment or withdrawal of the harmonised standard (see Figure 1).

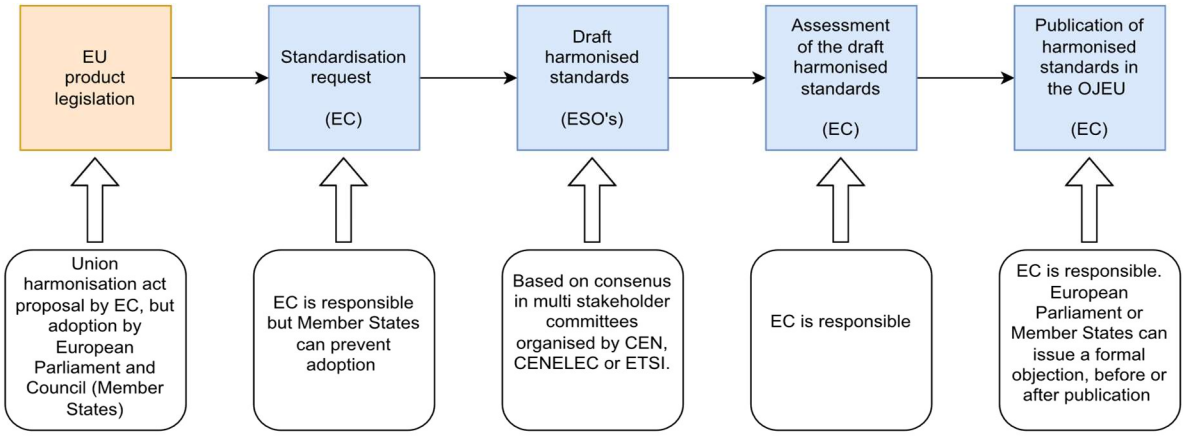

Figure 1: Establishing harmonised standards based on essential requirements in EU product legislation and requirements in the standardisation request. Source: [15] *and* [18]–[20] *adapted for this thesis.*

[16] see Chapter 3.4 for references
[17] see Chapter 3.5 for references

4 The Radio Equipment Directive's cyber security requirements

This chapter examines the Radio Equipment Directive and its three RED essential cyber security requirements. It also discusses the requirements in the EC standardisation request and the associated standardisation activities in CEN/CENELEC. Also, some challenges are identified related to developing cyber security standards.

This chapter provides context for the research questions that refer to the risk-based processes stated in the EC standardization request.

4.1 RED scope

The Radio Equipment Directive (RED) covers all devices that meet the definition of radio equipment as stated in the RED [12, p. 71]:

> "Radio equipment means an electrical or electronic product, which intentionally emits and/or receives radio waves for the purpose of radio communication and/or radiodetermination, or an electrical or electronic product which must be completed with an accessory, such as antenna, so as to intentionally emit and/or receive radio waves for the purpose of radio communication and/or radiodetermination".

The scope of the RED concerns devices transmitting or receiving information via radio waves. There are some exceptions for marine, airborne, and equipment intended exclusively for public/state security and Defense.

Examples of devices under the RED are WIFI routers, mobile phones, Bluetooth headsets, radio broadcast receivers, wireless remote controls, and mobile base stations. The RED also applies to devices that contain a radio module, regardless of whether this serves a primary or secondary function which is explained in an EC supplementary guidance document [33]. For example, so-called "smart washing machines", smart doorbells and everything that has the potential to communicate wirelessly are covered under the RED.

4.2 Cyber security requirements as part of the Radio Equipment Directive

The Radio equipment directive has been in force since 2014 (via an official publication in the OJEU) and applies from 13 June 2016. The RED contains four essential requirements which apply to all radio equipment: The protection of health and safety (art. 3.1(a)), an adequate level of electromagnetic compatibility (art. 3.1(b)), and efficient use of the radio spectrum to avoid harmful interference (art. 3.2) [12].

In addition to these requirements, article 3.3 of the RED contains nine essential requirements which the EC can activate via delegated acts for specific categories of radio equipment. Manufacturers must only meet these requirements if the EC has declared them applicable (via a delegated act) for the indicated categories of radio equipment. At least three of the nine essential requirements can be interpreted as cyber security-related requirements. This follows from an EC discussion document [34] in which the EC discusses the interpretation of art 3.3(d), 3.3(e) and 3.3(f) and concludes that these essential requirements (as stated in Table 1) can be used as cyber security requirements for radio devices. Various Member States, including the Netherlands, have pushed the EC to activate these essential requirements because, with this relatively quick process, the cyber security of many IoT devices can be improved [9].

In October 2021, the EC adopted a delegated act which came into force in January 2022 through an official publication in the OJEU (delegated regulation 2022/30 [11]). This act activated the essential cyber security requirements 3.3 (d), (e) and (f) for the categories of radio equipment as stated in Table 1. The requirements will apply from August 2024. The delegated regulation was accompanied by an associated impact assessment report [3], which substantiated the activation of the essential requirements.

Table 1: (RED) essential cybersecurity requirements and their scope. The table comprises information from the RED[12] and the delegated Regulation [11].

RED article	Essential requirement RED	Scope
Article 3(3), point (d)	Radio equipment does not harm the network or its functioning nor misuse network resources, thereby causing an unacceptable degradation of service.	Any radio equipment that can communicate itself over the internet, whether it communicates directly or via any other equipment ('internet-connected radio equipment').
Article 3(3), point (e)	Radio equipment incorporates safeguards to ensure that the personal data and privacy of the user and of the subscriber are protected.	Internet-connected radio equipment (capable of processing personal data, or traffic data and location data); and Non-internet connected radio equipment (capable of processing personal data, or traffic data and location data) being toys, childcare products or wearables
Article 3(3), point (f)	Radio equipment supports certain features ensuring protection from fraud."	Internet-connected radio equipment (if that equipment enables the holder or user to transfer money, monetary value or virtual currency)

4.3 RED Standardization Request on essential cyber security requirements

As discussed in Chapter 3, harmonized standards play an important role in European NLF product legislation. In August 2022, the EC published the EC standardization request [16] for developing three harmonized standards for the essential cybersecurity requirements, as stated in Table 1. The deadline for the harmonized standards to be ready is September 30, 2023. CEN and CENELEC have accepted the standardization request.

4.3.1 General requirements for the development of cyber security standards

The standardisation request [17, p. 2,4] states (among other requirements) the following general requirements, which shall apply to all three harmonised standards:

> - "Each harmonised standard shall include **detailed technical specifications** in support of the essential requirements
> - Each harmonised standard shall include **test methods** or equivalent approaches and conditions to verify compliance of the radio equipment with the corresponding specifications.
> - Test methods shall be **verifiable, objective and reproducible** to ensure comparable verification of the technical specifications for all the products covered by the harmonised standards.
> - The technical solutions laid down in the harmonised standards shall be **proportionate to the risk** that they aim to address.
> - The harmonised standards shall be drafted and revised by applying the **iterative process of Risk Assesment and Risk Reduction"**.

Bullet points 1,2, and 3 are well-known principles that also apply to the standards developed for the other, long-standing, RED essential requirements art 3.1 (a), 3.1 (b) and 3.2.
While these principles are known for other essential requirements under the RED, they can be challenging in cybersecurity. For example, the test methods must be verifiable, objective and reproducible. As a result, the test methods must be precise and leave little room for interpretation so that every user of the harmonized standard for the same device comes to the same conclusion about compliance with the technical cyber security specifications. Another challenge is that the security of an IoT device can strongly depend on the environment in which it is used and the application for which it is used. The specifications in the standard will need to address this clearly to ensure reproducible results.

Bullet point four states that technical solutions included in the harmonised standards shall be based on *Risk Assesment and reduction*. This approach is new under the RED because the Risk Assesment and reduction process is not explicitly mentioned in the standardization request [35] for the non-cyber security-related (long-standing) RED essential requirements.
Therefore, using risk analyses in developing standards under the RED is new and only applicable to developing harmonised cyber security standards. The EC standardisation request, however, does not provide information on the Risk Management or Risk Assesment methodologies to be used. Also, no information is given on the Risk Acceptance level, which is the acceptable level of risk to which the Risk Reduction, via technical solutions in the standards, must lead.

The question can be asked whether this unclarity is inconsistent with the "Vademecum on European Standardization" [18]–[20], which is a guide for the EC to draft standardisation requests, and which states that requirements in standardisation requests must be precisely formulated to prevent ESOs from making political choices.

This question is discussed in later chapters. Also, in later chapters (chapters 6, 7 and 8), a model is developed that could be used to determine if technical solutions in the harmonised

standards for IoT devices are proportionate to the cyber security risk they aim to address. The model is realised in the framework of research question 1, as stated in Chapter 1.

4.3.2 Specific requirements for the development of cyber security standards

The EC standardization request also contains specific requirements indicating which technical solutions the standard must contain to fulfil essential requirements. For example, technical authentication and access control solutions must be included in the standard for all three essential cybersecurity requirements.

The Annexes to the standardisation request [17] state that harmonised standards in support of the essential requirement set out in Article 3(3), points (d), (e) and (f) "shall contain technical specifications that ensure at least that those radio equipment, where **applicable**: .. implement **appropriate** authentication and access control mechanisms" [17, pp. 5–7].

Chapter 11 discusses the second research question related to the above requirement: *"Could the criteria and models identified in research question 1 be used to determine the applicability and appropriateness of authentication and access control mechanism requirements for IoT devices?".*

All requirements that apply to the harmonised standards for the essential cyber security requirements can be found in the EC standardisation request [16].

4.4 Standardisation activities on RED essential cyber security requirements

In August 2022, CEN and CENELEC jointly accepted the standardisation request. The technical committee CEN/CENELEC/JTC13 "Special Working Group, RED Standardization Request" is working, within the framework of the standardisation request [16], on developing three standards for the essential cyber security requirements, as stated in Table 1.
The standardisation request mentions 30 September 2023 as a deadline for the three harmonised standards. From August 2024, internet-connected radio devices must meet the essential cyber security requirements. Manufacturers need to have harmonised standards available then. Suppose no harmonised standards are available; in that case, the manufacturer may also test the product directly against the essential cyber security requirements without using harmonized standards. A third party (notified body) must then be involved (art. 17(3) of the RED [12]).

4.5 Cybersecurity standards not related to the NLF

The EU Strategy on standardisation [36] of February 2022 states that "harmonised standards are at the core of the European Single Market for products" and that over the last 30 years,

more than 3600 harmonised standards have been developed to support the product regulations.

Under the European legislative framework for the placing on the market of products (NLF), there is currently no availability of harmonised standards for the cyber security of products that can serve as an example for the harmonised standards to be developed in support of the RED cyber security essential requirements.

The development of the RED harmonised standards for the cyber security of radio devices is, therefore, a first in Europe. There are currently standards and specifications available on product security, such as the ETSI standard ETSI EN 303645 on cyber security for the consumer internet of things baseline requirements [22] and the EN IEC 62443-3-3 on System security requirements and security levels for industrial communication networks [21]. However, these standards have not been developed in the framework of European product legislation, which means they do not meet the associated criteria (see chapter 3).

However, elements from these standards, such as specific cyber security requirements, can be useful for the RED harmonized standards, provided they are used within the context of the EC standardization request.

5 European cybersecurity regulatory landscape

The first paragraph of this chapter discusses the current cyber security legislation for placing products on the market. These regulations are aimed at economic operators such as manufacturers, distributors and importers, and the requirements are mandatory. The Radio Equipment Directive (RED) and the Cyber Resilience Act (CRA) fall under this category.

In the second paragraph, other cyber security regulations are identified where the requirements are not mandatory or requirements must be met by parties other than manufacturers.

Products are often used in systems and installations. Manufacturers are responsible for the cyber security of their products if they are used as intended. However, they cannot be held responsible for their incorrect use by, for example, a service provider. That is why different legislation is needed that calls different actors to account for their responsibilities.

5.1 Cyber security legislation for the placing on the market of products

After a long period of legislative silence, cybersecurity legislation for placing products on the EU market is evolving quickly. Regulators are well aware of the digitization of society. In the EU's Cybersecurity Strategy for the Digital Decade [10] of December 2020, the EC announced various measures to raise cybersecurity in Europe to a higher level. The massive use of digital products entails cyber security risks if these products do not comply with the principle of security by design and default throughout their whole product's life cycle. This awareness leads to several new regulatory initiatives to close the cybersecurity gaps in product legislation.

A regulatory gap analysis [5] made by the EC shows that only a limited number of product legislation acts set cyber security requirements as mandatory requirements for EU market access. The Medical Devices Regulation [37] and the In Vitro Diagnostic Medical Devices Regulation [38] already impose mandatory cyber security requirements for medical devices under their scope during their entire life cycle. The Regulation on motor vehicles[18] and an associated delegated regulation also[19] regulate the cyber security of connected motor vehicles, including software updates.

In addition, the Radio Equipment Directive contains essential cyber security requirements that will apply from August 2024 for internet-connected wireless equipment.

[18]https://eur-lex.europa.eu/eli/reg/2019/2144/oj
[19]https://eur-lex.europa.eu/eli/reg_del/2022/545

Various initiatives are currently underway to amend product legislation acts. The “General product safety regulation”[20] and the “Machinery regulation”[21] are currently being revised, paying attention to cyber security.

A significant recent development is a publication (of September 15, 2022) of a new legislative initiative from the EC, namely the Cyber Resilience Act (CRA).
This proposal concerns a horizontal (sector-wide) product legislation for the cyber security of products with digital elements (hardware and software). The law is aimed at manufacturers and other economic operators. As with the RED, compliance with the cyber security essential requirements is a condition for placing products on the market.
The proposal's scope concerns all hardware and software products with digital elements. The proposal excludes medical devices and motor vehicles because cyber security product legislation already exists. The proposal also excludes devices within the scope of product legislation acts which already have similar requirements. This exclusion could (partially) apply to devices covered by the RED. However, it is expected that the CRA will eventually completely replace the cyber security requirements from the RED because the cyber security of wireless devices can more effectively be arranged via the horizontal CRA. The disadvantages of the RED, a limited scope (only wireless devices) and no life cycle approach, would be resolved.

A notable element of the CRA proposal is that the essential requirements are based on a life cycle approach, meaning that the product shall remain in compliance with the cyber security essential requirements throughout its lifetime. This is realized by a mandatory vulnerability handling process, including updates to ensure secure cyber products during their life cycle.
The life cycle approach is still rare in European product regulations. However, it is necessary for cyber security because the practice has shown that vulnerabilities that arise after the device has been placed on the market pose risks. As indicated in paragraph 2.4, the evaluation of the NLF has shown that the NLF should also contain standard procedures that can be used in new regulations to impose after-market requirements throughout the life cycle.

The life cycle approach does not apply to the RED. Although the cyber security requirements in the RED were recently activated in January 2022 (and will become applicable from August 2024), the RED has existed since 2014, and a life cycle approach was not yet familiar. As a result, it is difficult[22] within the RED framework to force manufacturers to issue regular software security updates. The RED can, however, enforce that a mechanism for secure updates is present in the device.

Another notable element of the CRA is that standalone software also falls within the scope.

The European Council and Parliament are currently negotiating the CRA proposal. It may still be several years before the CRA requirements will apply.

[20]https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12466-General-Product-Safety-Directive-review_en
[21]https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/2019-Machinery-Directive-revision_en
[22]or only with certain legal interpretations such as found in the answer to question 8 in an European Commission’s Q&A document [34].

5.2 General European cybersecurity legislation

5.2.1 Cyber Security Act (CSA)

The cyber security act defines a framework for voluntary certification schemes for specific ICT products, services and processes [8]. An EC's website states:

> "The certification framework will provide EU-wide certification schemes as a comprehensive set of rules, technical requirements, standards and procedures. The framework will be based on agreement at the EU level on the evaluation of the security properties of a specific ICT-based product or service. It will attest that ICT products and services that have been certified in accordance with such a scheme comply with specified requirements."[23]

However, there are currently no certification schemes available. Although the cyber security act provides for cyber security certification schemes for specific products, these requirements are voluntary for manufacturers. They are not mandatory for products to be marketed in the EU, as is the case with the RED and the CRA. However, other legislation may refer to the requirements from the certification schemes. For example, the CRA proposal excludes[24] devices that comply with a CSA scheme from the cyber security act. These devices, therefore, do not have to meet the requirements of the CRA.

5.2.2 Network and Information Systems Directive (NIS)

The NIS Directive was the first piece of EU-wide legislation on cybersecurity[25] and concerns measures for a high common level of security of network and information systems across the Union. The NIS directive "establishes security and notification requirements for operators of essential services and for digital service providers" ([7], art 1.2.d).

The negotiations between Council and Parliament on a new EC proposal for the NIS 2 directive, presented by the EC on 16 December 2020, are currently in the final phase[26].
Under the NIS regulations, operators of essential services and digital service providers are responsible for meeting requirements to achieve a high common level of network and information systems security. The difference with the RED or the CRA proposal is that the NIS regulations are not aimed at manufacturers of products. Insecure products cannot be withdrawn from the market due to non-compliance with the NIS directive. However, measures can be taken against operators of essential services and digital service providers.

[23] https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-certification-framework
[24] Legislative proposal for Cyber Resilience Act [13], Article 2(4).
[25] https://digital-strategy.ec.europa.eu/en/policies/nis-directive
[26] https://www.consilium.europa.eu/en/press/press-releases/2022/11/28/eu-decides-to-strengthen-cybersecurity-and-resilience-across-the-union-council-adopts-new-legislation/

5.2.3 General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR) “lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data” ([6], art 2.1). The requirements under the GDPR are set for controllers and processors. Their definitions are [6] art. 4:

> “controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;”.
>
> “'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller”.

One of the requirements of the GDPR concerns “Data protection by design and by default” ([6], article 25). However, it does not regulate the placing on the market of products. If controllers or processors do not comply with the GDPR requirements, it is impossible to ban devices from the European market.

6 Mapping RED processes in a fictitious “EU internal market” management system

This thesis aims to develop a model that can be used in standardization activities for the RED to determine whether technical solutions in harmonised standards for IoT devices are proportionate to the risk they aim to address. The model will be presented in Chapter 8.

This chapter discusses a top-down approach to ensure that the model to be developed fits within the broader EU internal market for products framework. The top-down approach starts with presenting a structure, a fictitious management system, to organize policies, objectives and processes according to two main goals of the EU internal market: A high level of public interest protection and proper functioning of the internal market.

As a second step, the fictitious management system is refined with three layers to map all RED processes. The Risk Governance layer maps legislators' processes regulating the cyber risks of IoT devices. The Risk Management layer maps processes that members of standardization organizations perform in the development of RED harmonized standards. The Risk Assesment layer maps the processes for selecting technical solutions for RED harmonized standards.

6.1 A management system for the “EU internal market for products”

ISO 27000 defines a management system as “a set of interrelated or interacting elements of an organization to establish policies and objectives and processes to achieve those objectives” [39].

There are two objectives the EU wants to achieve with the internal market of products: A high level of public interest protection and proper functioning of the internal market. The EC states: “*The European Commission's main goal in the EU single market for goods is to ensure the free movement of goods within the market and to set high safety standards for consumers and the protection of the environment*” [40]. The EU has established many policies, objectives and processes to achieve these goals while creating and implementing the NLF framework.

This thesis aims to develop a model that can be used in standardization activities for the RED to determine whether technical solutions in harmonised standards for IoT devices are proportionate to the risk they aim to address. This model is a process and must fit within the larger whole of NLF policies, objectives and processes for the EU internal market. This thesis chooses a top-down approach to ensure that the model to be developed fits within these frameworks. The top-down approach starts with providing a structure, a management system to organize policies, objectives and processes according to the two main goals of the EU internal market: A high level of public interest protection and proper functioning of the internal market. This structure is shown in Figure 2. All EU policies, objectives and processes for the internal market of products can be mapped in one of these two boxes.

According to the ISO definition of a management system, Figure 2 can be considered a management system with established policies, objectives and processes to achieve the two goals mentioned. The responsible organization of this fictitious management system would be the European Union consisting of the EC, Member States and the European Parliament.

The part "**Proper functioning of the internal market**" in Figure 2 maps all policies, objectives and processes related to that goal. In [29], a list of related sub-goals is mentioned. Policies, objectives, and processes of these sub-goals should also be included in this part of the fictitious management system, which are: Free movement of goods within the EU; Innovation-friendly regulation by setting technology-neutral essential requirements; Consistent and coherent legislation; High-quality conformity assessment; Efficient and effective enforcement of legislation and High credibility for CE marking.

The part "**A high level of public interest protection**" in Figure 2 maps all policies, objectives and processes related to the development of product legislation and essential requirements, the development of standardisation requests and the development of harmonised standards.

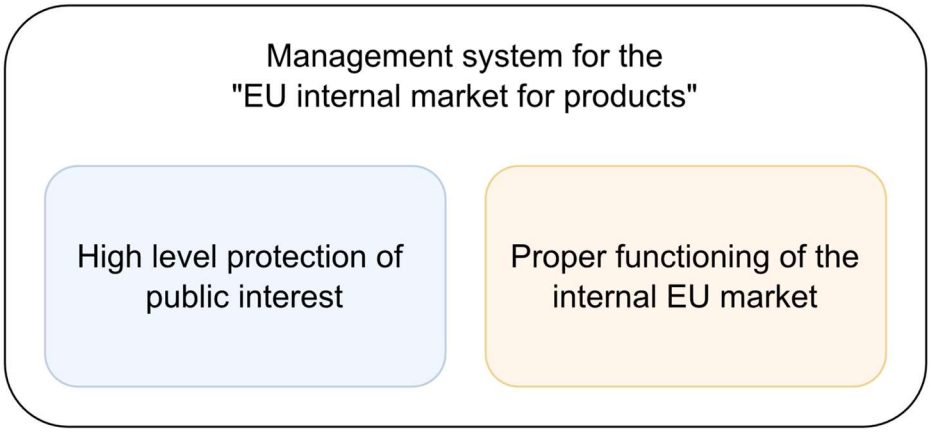

Figure 2: Fictitious management system for the overall EU internal market for products.
All EU policies, objectives and processes for the internal market of products can be mapped in one of these two boxes. The boxes represent the two goals the EU wants to achieve with the internal market of products: A high level of public interest protection and proper functioning of the internal market.

6.2 A management system for the "EU internal market for IoT devices"

In this paragraph, the management system, as discussed in the previous paragraph, is narrowed down to a management system for specifically managing the cyber security risks of IoT devices (via the RED) and the proper functioning of the internal market for IoT devices.

6.2.1 Proper functioning of the internal market of IoT devices

In order to achieve the objective of "A proper functioning of the internal market for IoT devices", the IoT cyber security product legislation should be aligned as closely as possible to the NLF principles leading to coherence and consistency in product legislation (see the right part of Figure 3). According to an EC study [29, p. 213], the RED is highly aligned with the NLF principles. The NLF principles, however, should regularly be updated to remain effective. As discussed in the previous chapters and confirmed by an EC study evaluating the NLF [28], many European product legislation acts align well with the NLF principles. The EC study (see also paragraph 2.4 of this thesis) concludes that the NLF should be modernised to remain effective in a changing environment caused by digitisation, artificial intelligence and the circular economy.

6.2.2 High level protection of public interest (Cyber security)

The objective "A high level protection of public interests" follows from the analysis in Chapter 3 about essential requirements, which shows, in general, that essential requirements in product legislation must offer a high level of protection (section 3.8). This thesis deduces that the essential cyber security requirements from the RED must also provide this high level of protection.

The EC standardization request [17, p. 2] explicitly states that "technical solutions included in the harmonized standards shall be based on *Risk Assesment and Risk Reduction"*. This approach is new under the RED because the Risk Assesment and reduction process is not required for developing standards for non-cyber security-related RED essential requirements. This follows from the EC standardization request that deals with the non-cyber security essential requirements [35].

In order to give these, for RED standardization, new processes of Risk Assesment and Risk Reduction a place in the management system, this thesis chooses to develop the management system from Figure 2 into a three-layer "Risk Management system" in which all RED processes can be mapped. The three layers are Risk Governance, Risk Management and Risk Assesment. These are commonly used layers in managing risks within organizations. In this thesis, these well-known concepts are applied to something new: protecting public interests by managing the cyber security risks of IoT devices in Europe.

The Risk Governance layer maps legislators' processes regulating the cyber risks of IoT devices. The Risk Management layer maps processes that members of standardization organizations perform in the development of RED harmonized standards. The Risk Assesment layer maps the processes for selecting technical solutions for RED harmonized standards.

The following paragraphs of this chapter discuss the three layers in more detail.

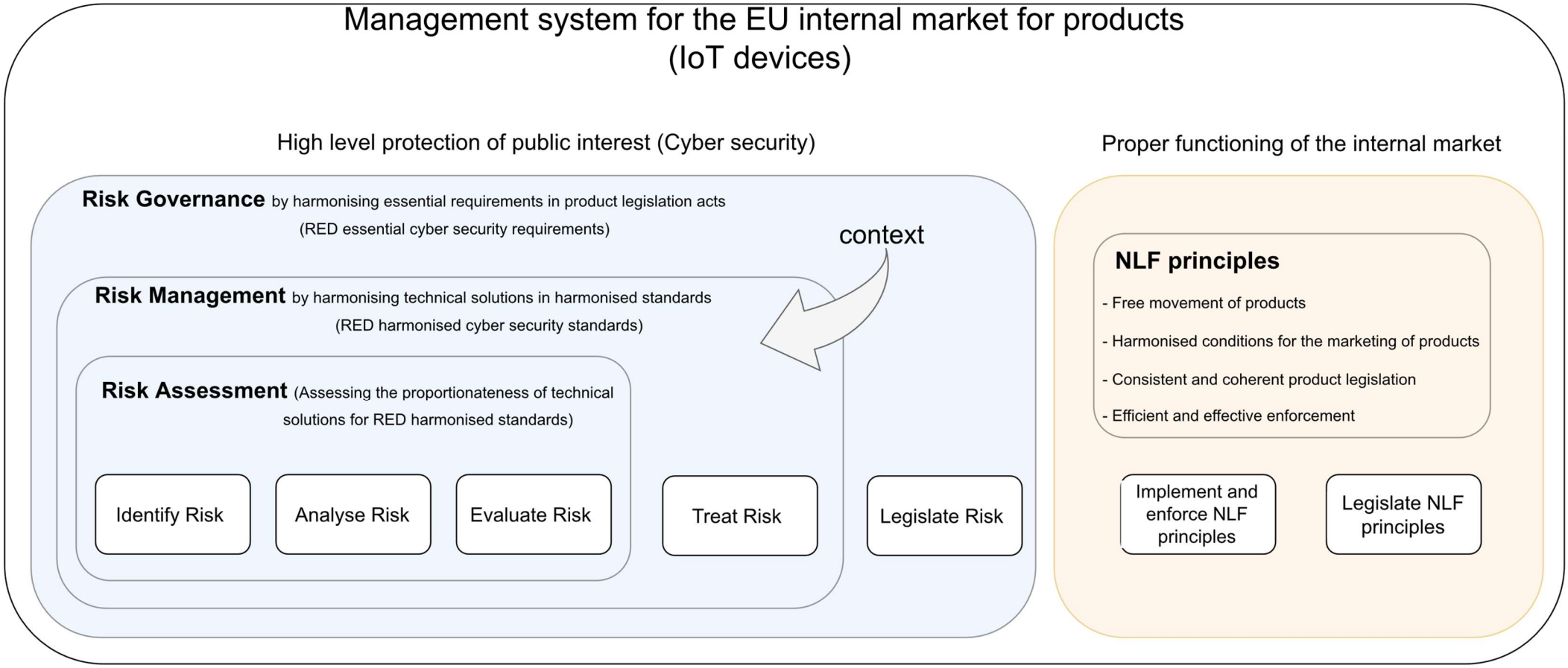

Figure 3: A proposed fictitious management system for the EU internal market of IoT devices. Managing the cybersecurity of IoT devices via the RED is accomplished by the processes of Risk Governance, Risk Management and Risk Assesment.

Risk Governance layer (legislate risk)

The Risk Governance layer contains all the regulatory processes that the legislators (European Commission, European Parliament and European Council) carry out to legislate the cybersecurity of IoT devices to achieve a high level of protection.

Regulators are responsible for establishing the essential cyber security requirements, which is a political process. These essential requirements are obligatory and are harmonized in Europe through the RED and the delegated regulation 2022/30 [11]. The EC standardization request [16] gives additional context and guidance for the standardization process (see paragraph 4.3).

The term "Risk Governance" is used in this thesis as indicated above, with legislators defining public interest protection. In the literature, "Risk Governance" has been used in several ways. For example, as "organizational oversight" [41] or in [42] as "a set of normative principles which can inform all relevant actors of society how to deal responsibly with risks". In [43], "Risk Governance is the application of governance principles to the identification, assessment, management and communication of risk. Governance refers to the actions, processes, traditions and institutions by which authority is exercised and decisions are taken and implemented [43]".

Risk Management layer (treat risk)

In the Risk Management layer, standardisation organisations are responsible for processes converting the essential cyber security requirements into technical specifications (security controls) for IoT devices to be included in harmonised standards. The RED standardisation process is occurring within the CEN/CENELEC committee JTC13-WG8. The deliverables of this Risk Management layer are harmonised standards in which the technical cyber security solutions have been finalised and agreed on, leading to meeting the essential cyber security requirements.

The selection of technical solutions in standards requires a risk-based approach, as stated in the EC standardization request [17, p. 4]

> "The technical solutions laid down in the harmonised standards shall be **proportionate to the risk** that they aim to address. The harmonised standards shall be drafted and revised by applying the **iterative process of Risk Assesment and Risk Reduction"**.

The standardization request, however, provides no information on the Risk Acceptance levels (the levels to which the IoT risk levels shall be reduced) to be applied when creating harmonized standards. This gives the multi-stakeholder standardisation committee freedom to decide on these levels, directly influencing the level of protection that the harmonised standards give.

The unclarity about the Risk Acceptance levels could also lead to (political) discussions in the standardisation committee. The Vademecum on European Standardization states [18, p. 9]:

> "The legal requirements, e.g., essential requirements laid down in legislation and requirements in a standardisation request, should be defined precisely in order to avoid misinterpretation on the part of the ESOs or leaving them to make political choices. This is fundamental to allow those preparing standards in support of Union legislation to provide high-quality specifications, as all political choices are to be made by the legislator".

This thesis argues that according to the Vademecum, more clarity should be given by the Standardisation request on the Risk Acceptance levels.

Section 3.3 of this thesis shows, however, that essential requirements are designed to achieve a high level of protection. It could be deduced from this that the Risk Acceptance level should be regarded as low. This means that only a small residual cyber security risk could be accepted, resulting in a high level of protection.

Risk Assesment layer (identify, analyse and evaluate risk)

Risk Assessments are necessary to support the development of harmonised standards. In order to determine if the technical solutions developed for inclusion in the harmonised standards are adequate and appropriate, a Risk Assesment can show whether the cyber security risks, after the technical solutions are applied to IoT devices, have been sufficiently reduced. By identifying, analysing and evaluating risk, the risk level is assessed, and an evaluation is performed on whether the residual risk level meets the desired level.

7 Risk Management and Risk Assesment frameworks

Chapter 6 discusses the development of a fictitious “EU internal market” management system which maps the relevant RED processes. The management system follows a modular approach, and to be able to use it in practice for the RED standardisation process, the Risk Management and Risk Assesment layers must be completed with practical methodologies.

This chapter examines various Risk Management and Risk Assesment frameworks that can be used to complete the model.

In the conclusion of this chapter, this thesis chooses to incorporate the ISO 27005 [44] Risk Management framework and The Open Fair Risk Assesment method in the fictitious management system of Figure 3 to support the risk-related processes during the development of harmonized standards.

7.1 Risk Management frameworks

7.2 ISO 31000 Risk Management — Guidelines

ISO 31000 defines Risk Management as “coordinated activities to direct and control an organisation with regard to risk” [45].

ISO 31000 [45] is a well-known standard with guidelines for setting up a Risk Management system in an organization. The guidelines apply to all types of organizations and activities and for all types of risks. ISO 31000 is built on three pillars: Risk Management principles, a Risk Management framework and a Risk Management process.

The Risk Management principles concern the properties of an organisation's Risk Management system. It must be an integral part of the organizational activities, structured, proportionate and able to adapt and continuously improve. The second pillar, the Risk Management framework, concerns guidelines for integrating a Risk Management system into the activities and functions of an organization. The third pillar is the Risk Management process. This contains the components: Context, Risk Assesment, Risk Treatment, reporting and communication.

7.2.1 The ISO 27005 Risk Management Framework

ISO 27005 [44] is a standard for Information security Risk Management. It describes the process of information security Risk Management and its activities. It builds on the generic Risk Management process from ISO 31000 [45] but focuses on *information security*.
The risks that can be managed with this standard are risks “which can potentially compromise the organisation's information security” [33]. The ISO 27005 standard applies to all organisations, such as commercial enterprises, government agencies and non-profit organisations [3].

The components of the ISO 27005 Risk Management framework are Context establishment, Risk Assesment, Risk Treatment, and Risk Acceptance. These parts are schematically shown in Figure 4 [44].

Short description of the ISO 27005 Risk Management Process

This section describes the ISO 27005 Risk management process using information from the ISO 27005 standard [44]. The description in this section refers to Figure 4.

In the "Context establishment" phase, necessary information for the Risk Assesment, Risk Treatment and Acceptance are obtained. The context information must concern:

- Purpose of the Risk Management process.
- Scope and boundaries of the Risk Management process.
- Risk Criteria
    - Risk Management approach (which Risk Management methodology to apply)
    - Risk Evaluation criteria (how the level of risk is to be determined)
    - Likelihood criteria (how the likelihood is determined)
    - Impact criteria (criteria to determine the impact of risks)
    - Risk Acceptance criteria (amount and type of risk that the organisation may or may not take)

The risks of the object under investigation (e.g. an IoT device) are identified, analysed, and evaluated in the Risk Assesment process. ISO 27005 does not prescribe a Risk Assesment method and allows it to be determined by the organisation.

If, after having performed the Risk Assesment, it appears that the context information is insufficient to carry out an adequate Risk Assesment, the context will be supplemented or adjusted. After completion of the Risk Assesment, Risk Treatment is applied. ISO 27005 provides four options for Risk Treatment: Risk Modification, Risk Retention, Risk Avoidance and Risk Sharing. Effective Risk treatment results in Risk Reduction. If the residual risk level is acceptably low (lower than the risk acceptance level), the risk treatment is effective, and the remaining risk is accepted. The process is iterative and repeats itself continuously.

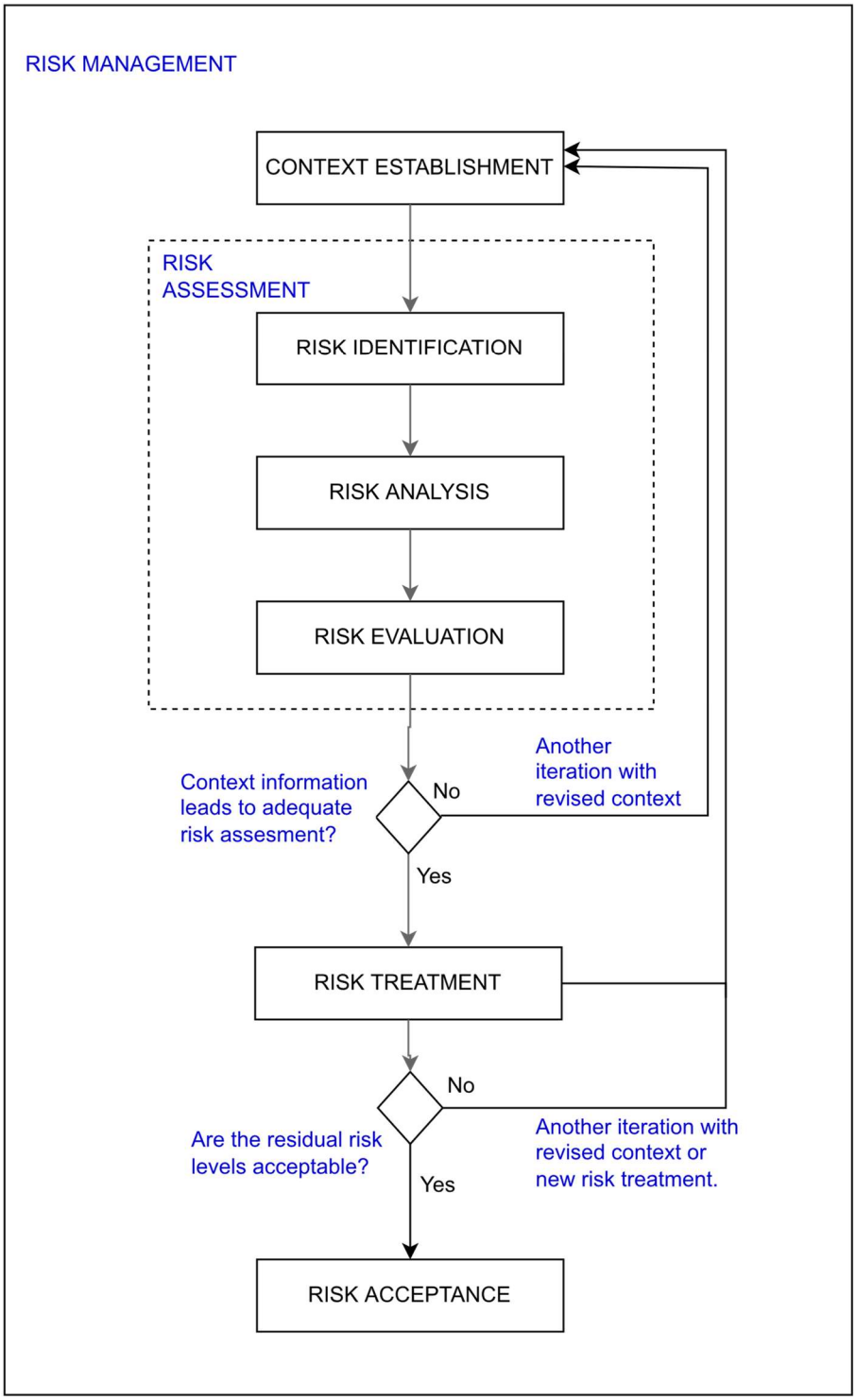

Figure 4 Risk Management process ISO/IEC 27005 [44]

7.2.2 IEC 62443 Risk Management and Risk Assessment framework

Another Risk Management system is described in 62443-3-2 [46]. The IEC 62443 series aims to promote the security of "Industrial Automation and Control Systems" (IACS systems). The standard IEC-62443-3-2 [46] describes a Risk Management and Risk Assesment workflow that must be followed to determine the security risk level of (existing or still to be developed) IACS systems. The workflow has many similarities to the ISO 27005 procedure.

Short description of the IEC-62443-3-2 Risk Management Process [46]

This section describes the IEC-62443-3-2 [46] Risk management process using information from that standard.

The design of an IACS system is an iterative process in which the unmitigated cyber security risk is first determined. Then the cyber risks are reduced to an acceptable level by implementing security controls. If the risk analysis shows that the residual risk is higher than the tolerable risk, then security measures must be implemented. The ultimate goal is that an acceptable risk is realized by implementing adequate security controls. The organization determines the tolerable risk level.

The required security level depends on the complexity of the threat. Table 2 indicates how the security levels of a system correspond to the various threat categories. The necessary security levels (0 to 4) are determined for seven cyber security domains: Identification and authentication control, Use control, System Integrity, Data confidentiality, Restricted data flow, Timely response to events and Resource availability.

The required security level is chosen in such a way that it addresses the expected threat. This required security level is called the target security level. It is expressed as a vector with seven elements representing the seven domains). For each domain, a security level is determined.

Table 2 Security levels as stated in IEC-62443-3-2 [46, p. 27]

Security Level	Protection
0	No security protection necessary.
1	Protection against casual or coincidental violation
2	Protection against intentional violation using simple means with low resources, generic skills and low motivation
3	Protection against intentional violation using sophisticated means with moderate resources, IACS-specific skills and moderate motivation
4	Protection against intentional violation using sophisticated means with extended resources, IACS-specific skills and high motivation

Components and subsystems are used in the design of an industrial control system. These must each at least meet the target security level of the IACS system to be developed.

The corresponding requirements are specified in the standards IEC-62443-3-2 [47] and IEC-62443-3-3 [21]. According to these standards, the components and sub-systems that make up the industrial control system must at least meet the target security level.
Compensating countermeasures are permitted if the individual components or subsystems cannot intrinsically meet the required target security level. These compensating security measures are implemented in combination with the relevant components or subsystems and, in combination with each other, meet the target security level.

7.2.3 The Open FAIR Risk Assesment standard

The Open FAIR Risk Assesment standard [41] describes a model which uses various risk factors to determine the Risk. A technical guide [39] written by the Open FAIR group discusses the integration of FAIR within ISO 27005.

The Open FAIR Risk Assesment model is depicted in Figure 5. The blocks represent Risk factors which determine the Risk. The FAIR model can be applied to a predetermined scenario, e.g. an IoT device in an IoT network, as depicted in Figure 9 on page 52.
In order to reduce the risk, various 'controls' can be chosen to influence the risk factors. A risk factor that applies to devices (like IoT devices) is the “Resistance strength”. Suppose the resistance strength of an IoT device is increased by technical solutions (such as authentication). In that case, it becomes more difficult for a threat agent to perform an action that results in harm. The “susceptibility” for a successful attack is thus lowered.

The Open FAIR method will be further explained in Chapter 10 using an example.

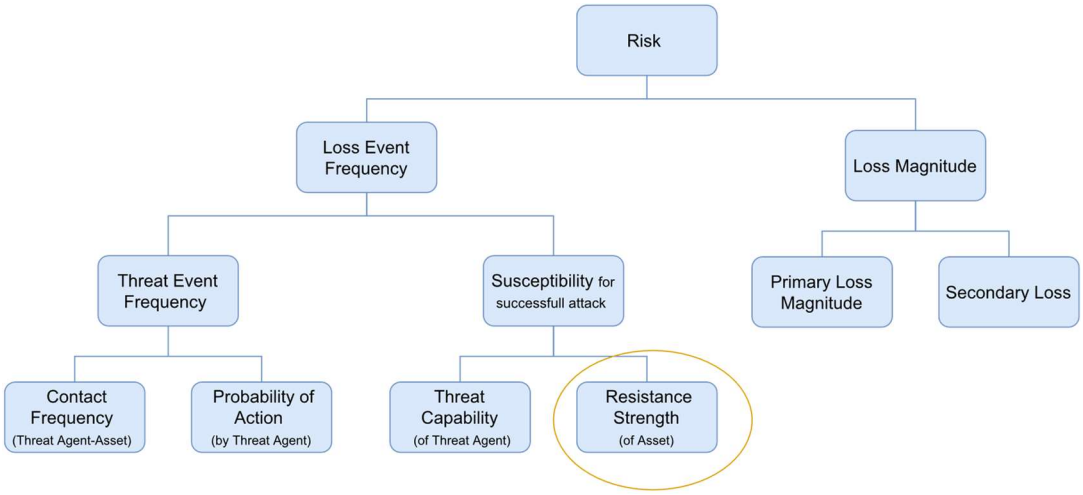

Figure 5 Open FAIR risk taxonomy abstractions [34]. *Appropriate security controls in devices improve their Resistance Strength and lower their susceptibility to successful attacks.*

7.2.4 Other Risk Management frameworks

ENISA (The European Union Agency for Cybersecurity) has investigated the properties of 16 different Risk Management frameworks [48], [49]. The emphasis of the research was on finding the interoperability between the Risk Management frameworks[27]. Interoperability is defined in that study as: "the ability of a Risk Management component or method to reuse information provided by Risk Management components or methods of other frameworks with equal ease and with the same interfaces, towards the same goals [48, p. 31]".
ENISA itself also concludes in the report's Synopsis that the 'scoring' of the degree of 'compatibility' can lead to erroneous conclusions due to the different scopes, goals, methods and detail of the Risk Management frameworks [48].

The author of this thesis notes that the frameworks examined by ENISA are not all Risk Management frameworks. Some involve only a Risk Assesment framework, such as Open Fair (part of a Risk Management framework). Because the goals of Risk Management and Risk Assesment frameworks differ, scoring compatibility is not meaningful.

However, interesting in the ENISA study is the overview of the properties of the different frameworks, which are indicated in Table 3: General aspects, Risk Identification, Risk Assesment and Risk Treatment. The frameworks have many similarities as they all address these properties. The differences mainly lie in the elaboration of the various properties.

Table 3: Risk Management framework characteristics used by ENISA to compare the frameworks [48].

Characteristics Risk Management frameworks	
Generic aspects	Asset-based or risk scenario based
	Quantitative/ Qualitative approach
Risk identification	Asset taxonomy
	Asset valuation
	Threat catalogues
	Vulnerability catalogues
Risk Assesment	Risk calculation method
Risk Treatment	Measure catalogues & calculation of residual risk

7.3 Conclusion

Various Risk Management and Risk Assesment frameworks have been investigated.
The frameworks ISO 31000 [45], ISO 27005 [44], IEC-62443-3-2 [46] and Open FAIR [41] have been examined in more detail.

[27] ENISA investigated: ISO/IEC 27005:2018, NIST SP 800- 37, NIST SP 800- 30, NIST SP 800- 39, BSI standard 200-2, OCTAVE-S, OCTAVE ALLEGRO, OCTAVE FORTE, ETSI TS 102 165-1(TVRA), MONARC, EBIOS Risk Manager (RM), MAGERIT V.3, ITSRM², MEHARI, The open group standard, risk analysis, v2.0, Guidelines on cyber security onboard ships

The research shows that the approach used by many frameworks is similar to the approach in ISO 27005. This also follows from the ENISA study [48], [49] in which the properties of 16 different Risk Management frameworks were investigated.

Because ISO 27005 is a generally accepted standard, this thesis proposes the ISO 27005 framework for incorporation into the management system of Figure 3. The Open FAIR Risk Assesment method has been chosen as the Risk Assesment framework. The Open FAIR method has a clear structure and is well documented. Moreover, it is highly suitable for integration in ISO 27005, as evidenced by an Open Fair technical Guide [50].

The next chapter discusses the proposed “RED cyber security management system” in which ISO27005 and Open FAIR have been integrated. The model can be used in standardization activities for the RED to determine whether technical solutions in harmonised standards for IoT devices are proportionate to the risk they aim to address.

8 Proposed "RED cyber security management system"

The proposed "RED cyber security management system" is shown in Figure 6. The model enables stakeholders participating in the RED standardisation process to determine whether technical solutions in harmonised standards for IoT devices are proportionate to the risk they aim to address.

8.1 Using the proposed model to develop RED standards

According to the proposed model (Figure 6), the phases of Context establishment, Risk Assesment, Risk Reduction, Risk Evaluation and Risk Acceptance must be completed.

Context establishment

The Risk Management process starts with the phase of "context establishment". In this phase, all necessary information is gathered that is needed to complete the Risk Management process correctly. These are (see paragraph 7.2.1) 1. Purpose of the Risk Management process, 2. Scope and boundaries of the Risk Management process, and 3. Risk Criteria. Information about points 1 and 2 can be sufficiently derived from the information from the Risk Governance layer, namely the RED [12] (with the essential cyber security requirements), the delegated regulation 2022/30 [11] and the standardization request [16].

Paragraph 7.2.1 of this thesis mentions a list of Risk criteria that ISO 27005 considers necessary for the implementation of a Risk Management process. This list includes Risk Acceptance levels[28]. As discussed in Chapter 6, the EC Standardization Request provides no information on the Risk Acceptance levels to be applied when creating harmonized standards. This gives the multi-stakeholder standardisation committee freedom to decide on these levels, directly influencing the level of protection that the harmonised standards give.

Section 3.3 of this thesis shows that essential requirements are designed to achieve a high level of protection. It could be deduced from this that the Risk Acceptance level should be regarded as low. In Figure 6, near the arrow, the word Acceptable Risk level has a question mark, indicating that the Acceptable Risk level is not available but could be derived from the assumption that a high level of protection should be achieved.

Risk Assesment phase (see Figure 6)

In this phase, the cyber risk of an IoT device is determined using the proposed FAIR Risk Assesment method. Based on the intended use of the IoT device (to be defined by the manufacturer of the IoT device). FAIR is used to determine the risk of the IoT device in a realistic threat scenario. After an initial attempt to carry out the Risk Assesment, a decision is made on whether the context information is sufficient to continue in the process. If this is not the case, the context information is supplemented or changed, and another Risk Assesment process is completed. The process can be continued if the Risk Assesment can be carried out correctly.

[28] Risk Acceptence level is the Risk level to which the Risk shall be reduced)

Risk Reduction Phase (see Figure 6)
Suppose it is necessary to reduce the risks of an IoT device because the residual risk is higher than the Risk Acceptance level. In that case, technical solutions are devised (e.g. authentication) that are included as draft requirements in harmonized standards. Another Risk Assesment is performed based on the IoT device with the technical solution.

Risk Evaluation phase (see Figure 6)
If it turns out that the risk level is still too high, additional technical solutions are devised, and a Risk Assesment is carried out again. This continues until the risk level is below the Risk Acceptance level. Because the risk acceptance level is not available from the governance layer, it will have to be agreed on by the standardization committee.

Risk Acceptance phase (see Figure 6)
Suppose the Risk Assesment shows that the risk level has become lower than the Risk Acceptance level. In that case, the technical solution is accepted as being adequate and proportionate, and the technical solution is included in the harmonized standard.

8.2 Conclusion on research question 1

Research question 1 reads*: Which criteria and models could be used to determine if technical solutions in the harmonised standards for IoT devices are proportionate to the cyber security risk they aim to address*?

As discussed in the previous section, the "RED cyber security management system", as depicted in Figure 6, can be used to determine if technical solutions in the harmonised standards for IoT devices are proportionate to the cyber security risk they aim to address.

The "RED cyber security management system" consists of a Governance layer, a Risk Management Layer and a Risk Assessment layer and incorporates the Open FAIR and ISO 27005 Risk Management methods. Assessments with the "RED cyber security management system" determine whether the technical solutions for IoT devices have reduced the Risk level to an acceptable level (a level below the Risk Acceptance Level). The technical solutions are proportionate if the Risk Reduction is not unnecessarily high, resulting in a much lower risk level than needed.

As a criterion for this assessment, it is necessary to agree on a Risk Acceptance level. Because the Risk Acceptance level does not result from the legislation, it will have to be determined by the standardization committee.

The above argumentation answers the first research question.

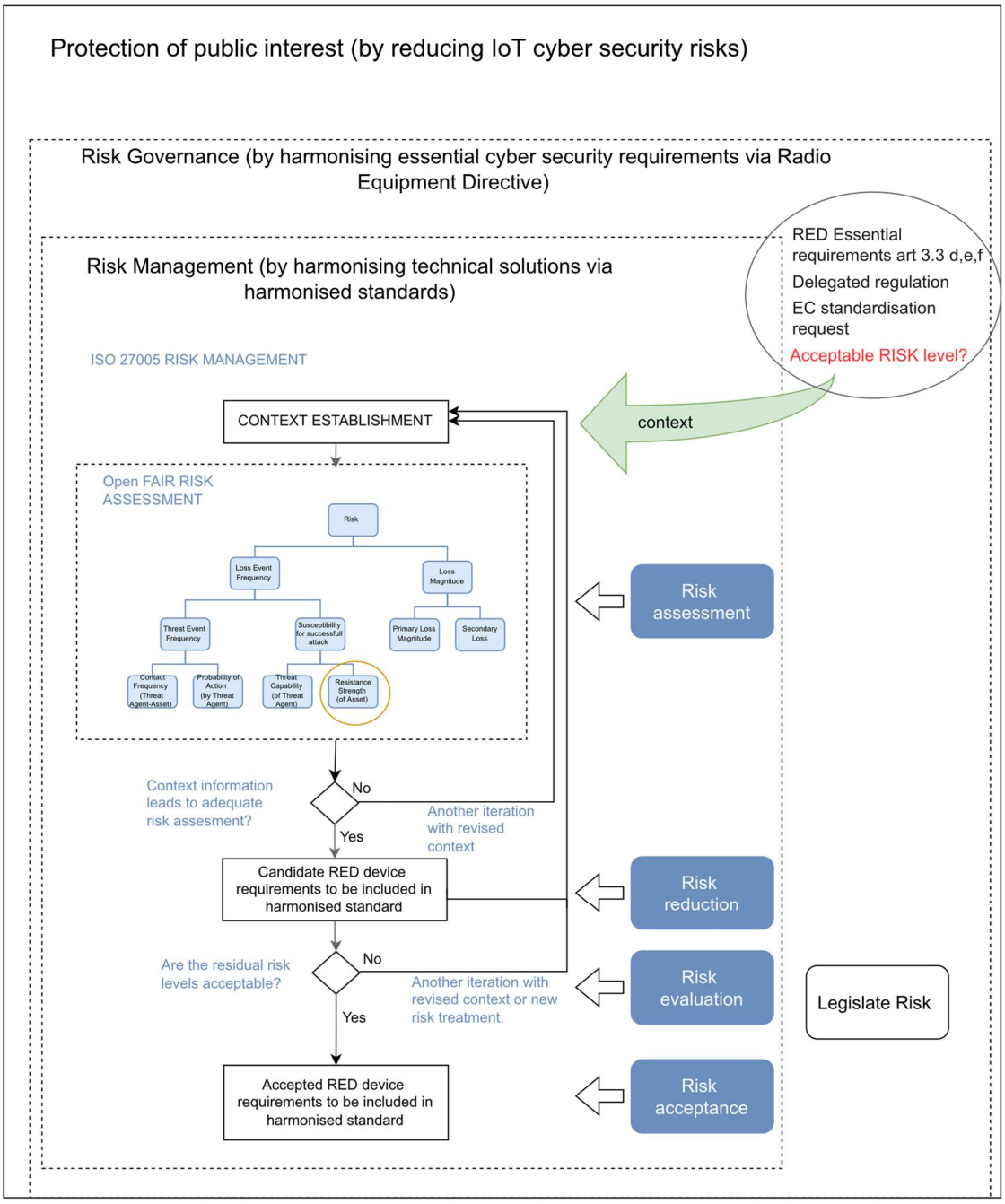

Figure 6 Proposed "RED cyber security management system" to determine the appropriateness of technical solutions in harmonised standards.

9 IoT device and IoT system descriptions

This chapter researches methods to describe IoT devices and systems. The goal is that these descriptions can be used for performing cyber security assessments of IoT devices in IoT systems. Such a description can be used as a basis for performing cyber security risk analyses with Open Fair in the Risk Assesment layer of the RED cyber security management system from Figure 6. To this end, this chapter discusses a literature study into the functional components of an IoT device, conceptual models of IoT networks and IoT reference architectures.

Furthermore, this chapter identifies IoT application domains of IoT systems. The application domain in which IoT devices are used can influence the "impact" of a successful cyber security attack. The intended use of an IoT device in a specific IoT application domain can therefore influence the outcome of the cyber security Risk Assesment.

9.1 Internet of Things devices

Many definitions of the Internet of Things can be found in the literature. The definitions differ depending on the underlying visions of the IoT paradigm [51].

The definition used by the ITU-T [52] for "Device", "Internet of Things", and "Thing" are:

> **Device**: "With regard to the Internet of things, this is a piece of equipment with the mandatory capabilities of communication and the optional capabilities of sensing, actuation, data capture, data storage and data processing" [52].
>
> **Internet of things (IoT)**: "A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies. Note 1 – Through the exploitation of identification, data capture, processing and communication capabilities, the IoT makes full use of things to offer services to all kinds of applications whilst ensuring that security and privacy requirements are fulfilled. Note 2 – From a broader perspective, the IoT can be perceived as a vision with technological and societal implications" [52].
>
> **Thing**: "With regard to the Internet of things, this is an object of the physical world (physical things) or the information world (virtual things), which is capable of being identified and integrated into communication networks" [52].

According to [53], the primary purpose of an IoT system is "to collect real-world status data and make them available to services and applications that create insights and act upon them by affecting the physical system under observation in some way. Implementing those functions requires an infrastructure to run them and control functions to keep the IoT system secure and operational".

The functional elements, "data collection", "data processing", "data storage", and "acting", as indicated in Figure 8, can be present in one device but can also be separated from each other

and distributed over different devices on different locations which are connected via the IoT network (consisting of one or more networks including the Internet).
As shown in Figure 7, this thesis extends the ITU-T model by adding “IoT device service” as an optional component of an IoT device. An “IoT device service” provides capabilities to other entities at their request. The IoT device acts, in such a case, as a server. An IoT device service can, for example, give a user access to data or to the settings of the IoT device via a web interface. The capability to provide a service to other entities is an important element in IoT security. The Mirai botnet, for example, could spread because IoT devices were accessible via Telnet ports with standard passwords [54].

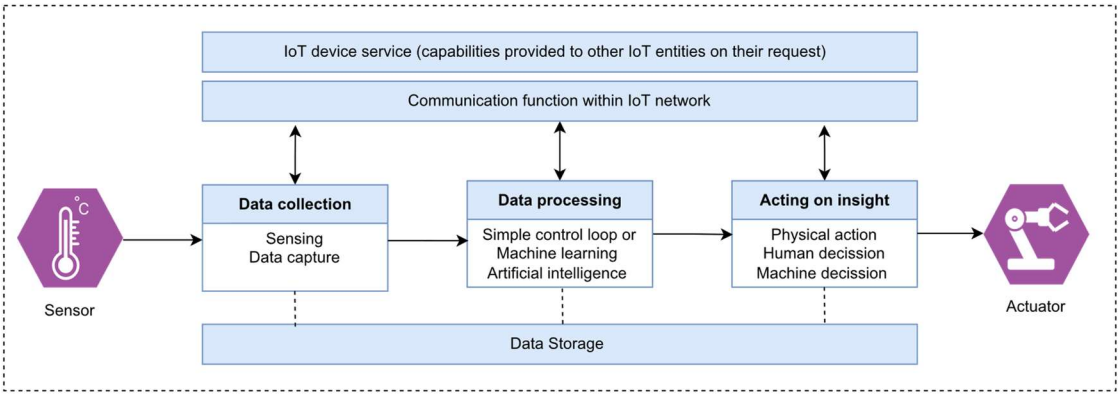

Figure 7 Components of an IoT device based on the definition in ITU-T [52] *but expanded by this thesis with “IoT device service”. All components are optional except for the capability to communicate and to be identified within the IoT network* [52].

IoT devices are part of an IoT system. A well-known example is an IoT surveillance system in which image information is collected via a surveillance camera (sensor). The image information obtained is processed in the device or by a cloud service. If the data processing shows that the image information contains a person, this is signalled and passed on to the device itself or another device within the IoT network. The device can take action directly or indirectly through human action, such as sounding an alarm or sending a message to an app on a mobile phone.

The following sections take a closer look at the three primary goals of an IoT device or system: data collection, data processing and acting on insights.

Data collection

Collecting data can be performed with sensors. This allows environmental parameters such as sound, image (camera), temperature and humidity to be registered. Analog to digital converters digitize the data and make it suitable for transmission to other devices, services and applications (whether or not to the cloud) [55].

Examples of sensors are light sensors, audio and microphone sensors, accelerometer sensors

location sensors, touch, temperature, pressure, medical, neural, environmental, and chemical sensors mobile phone-based sensors. The field of application is vast: Sensors can be used for environmental monitoring, disaster management, domestic purposes, human health, public security, and early warning systems in the domains of smart cities (waste management, air quality, traffic management, smart grids), medical and health care applications, agricultural applications, smart home, smart manufacturing systems, Internet of robotics and oil and gas [55].

Data processing

Data processing is applied to the data collected by sensors. The data processing can be performed on the device or another device if more computing power is required (for example, via a cloud service). The purpose of the data processing can be a simple control loop or a complex analysis using machine learning algorithms. Depending on the required computing power, complex analyses usually occur in the system hierarchy's higher levels [55].

Acting upon insights

Acting refers to taking action based on insights obtained from data processing. This action can be, for example, an action affecting the physical world (with an actuator) or making a decision (by a human or a machine) [53].

9.2 IoT application domains

According to [56], IoT can be regarded as an umbrella covering different technologies in various application domains. The ISO/IEC 30141 standard [38] contains a list of key properties for IoT systems. Different "key properties" may apply to different IoT applications. The main properties identified by this standard are "system trustworthiness characteristics" and "IoT system architecture characteristics".

Borgia [51] describes three main IoT application areas: The Smart city domain, the Industrial domain and the Health and Well-being domain. These are shown in Figure 8 and are summarised below:

In the Industrial Domain, IoT can be used for *logistics and lifetime management*, where objects (goods and materials) are provided with Radio Frequency Identification (RFID) tags. These tags can identify and monitor objects throughout their entire supply chain. By using IoT, cost reductions can be achieved through an increase in the efficiency of production processes. In *Agriculture and Breeding*, IoT is used for animal monitoring, including location tracking and health monitoring. Furthermore, in *Industrial Processes*, IoT can be used, for example, for real-time vehicle diagnostics and monitoring of industrial processes [51].

In the Smart City Domain, IoT applications can be used for *Smart Mobility* (e.g. sensors generating traffic information) that help, for example, to regulate traffic or find parking spaces. An important application area is *Smart Grid.* In this subdomain, IoT devices perform monitoring

and control functions to manage electrical distribution systems connected to consumers who use and generate energy. The *Smart Home, Smart Building* domain involves all applications used in a domestic environment or a building. Examples are multimedia distribution in the house, a smart refrigerator, or video surveillance. IoT applications interacting with the smart grid are also included in this category. *Public Safety and Environmental Monitoring* aim to promote safety in society by detecting and resolving emergencies [51].

In the Health and Well-being domain, IoT applications are used for *medical and healthcare* purposes where IoT devices, for example, monitor medical parameters or identify medical instrumentations. In addition, IoT in this domain can contribute to *Independent living for ageing or disabled people* by, for example monitoring the condition and status of the elderly and setting medical alarms [51].

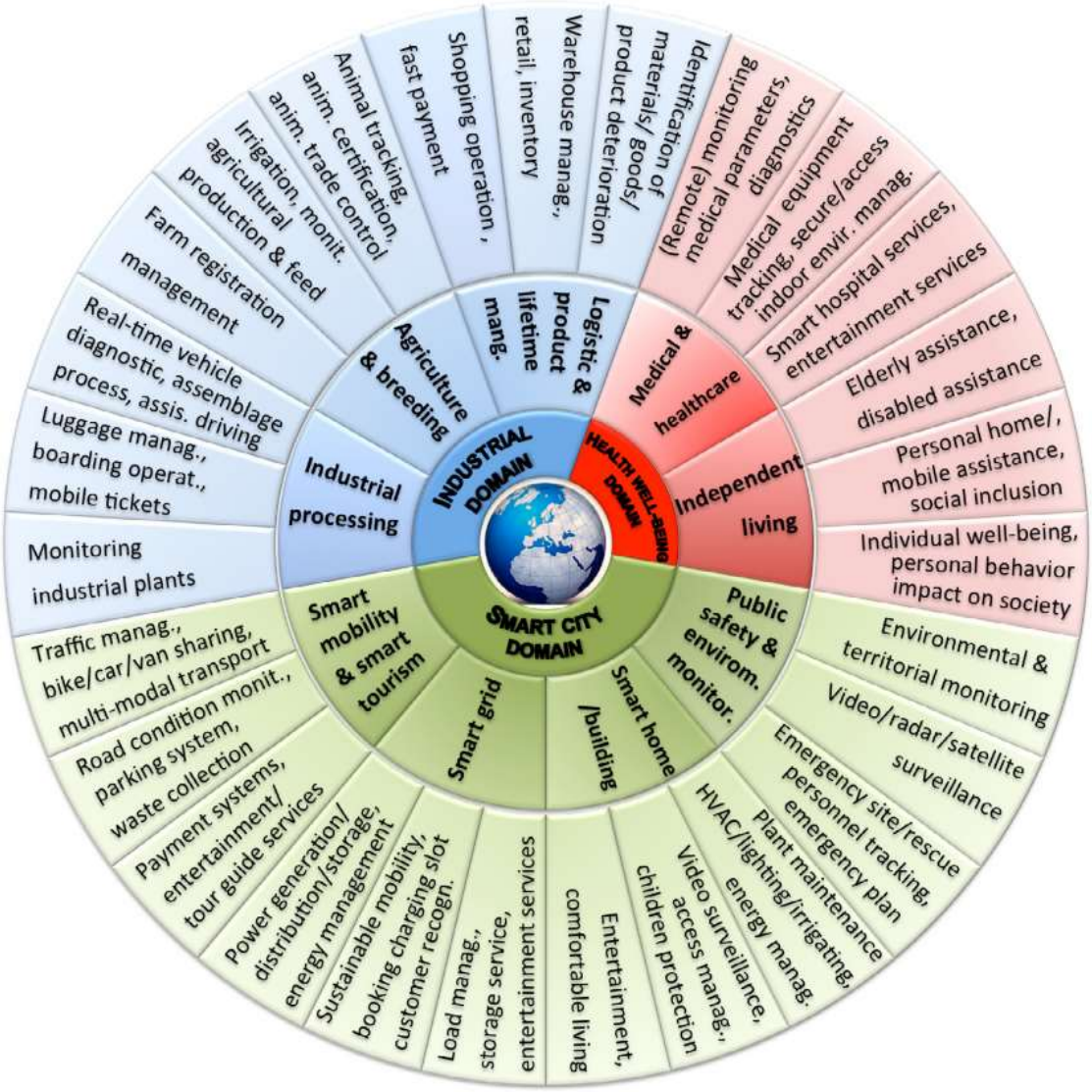

Figure 8 IoT application domains and related applications [51]

9.3 Conceptual model of an IoT network

Figure 10 shows a conceptual IoT model based on the ISO/IEC 30141 standard [45]. In the "conceptual model", the structure and (logical) relationships between the entities of an IoT system are represented. Explanations of these entities are shown in the boxes. This thesis proposes to use the (adapted) ISO/IEC 30141 model to describe IoT devices in IoT systems in a standardised way using standardised entity relationships and definitions. IoT system descriptions are necessary for performing cyber security assessments (like threat analysis) of IoT devices in IoT systems. They should also be used as a basis for performing cyber security risk analyses with Open Fair in the Risk Assesment layer of the RED cyber security management system from Figure 6.

The original model ISO/IEC 30141 is extensive. In order to be able to use the model optimally for the above purpose, the model has been simplified and slightly modified. The (adapted) model is first described below, and then the differences with ISO/IEC 30141 are discussed.

According to the model, an IoT system consists of entities, as shown in figure 8. The possible entities are Human IoT Users, Digital IoT users, IoT devices, IoT clients, IoT system servers, networks, IoT gateways, routers and switches. Digital entities have a computational or data element. All entities from Figure 8 are digital entities except the Human IoT User.

According to the conceptual model, an IoT system can have two types of IoT users: **Human IoT Users** and **Digital IoT Users** (machine). They have access to the IoT system via an **IoT client device**. An IoT client device can be, for example, a mobile phone with an IoT app or a Web Browser that provides access to the IoT system. An **IoT system server** provides a "set of distinct capabilities" to entities in the IoT system. Examples include data storage (local or in the cloud) or data processing. The composite IoT model from Figure 7 is used as an IoT device in the conceptual model. Data communication between entities happens via so-called "**endpoints**". An endpoint implements a communication interface on a network. Communication is possible between endpoints in the same network (via **switches**) or via a **gateway** or **router** between endpoints on different networks. IoT devices can interact with other IoT devices, and IoT system servers can interact with other IoT system servers.

The model in Figure 8 differs from the ISO/IEC 30141 standard [45]. Not all entities from ISO/IEC 30141 are used. The IoT client device entity has been added to better address how an IoT user accesses the IoT system. The entity IoT system server has been added instead of the entity "service", which is used by the ISO standard. Although the same definition has been used, the adapted model refers to the hardware (server instead of service). Finally, the adapted model uses the composite IoT model from Figure 7 as an IoT device.

Example of a simple IoT system

Figure 9 shows an example of an IoT network consisting of a smart camera that connects via WIFI to an IoT gateway, which makes the connection via the local network to the Internet network to connect to a Cloud Server where the camera images are saved. The cloud server can be accessed via the Internet network with the mobile phone of the IoT User. The User can

access the device settings of the camera via the local network. To this end, the IoT device has a Web Interface (called IoT device service in Figure 7)

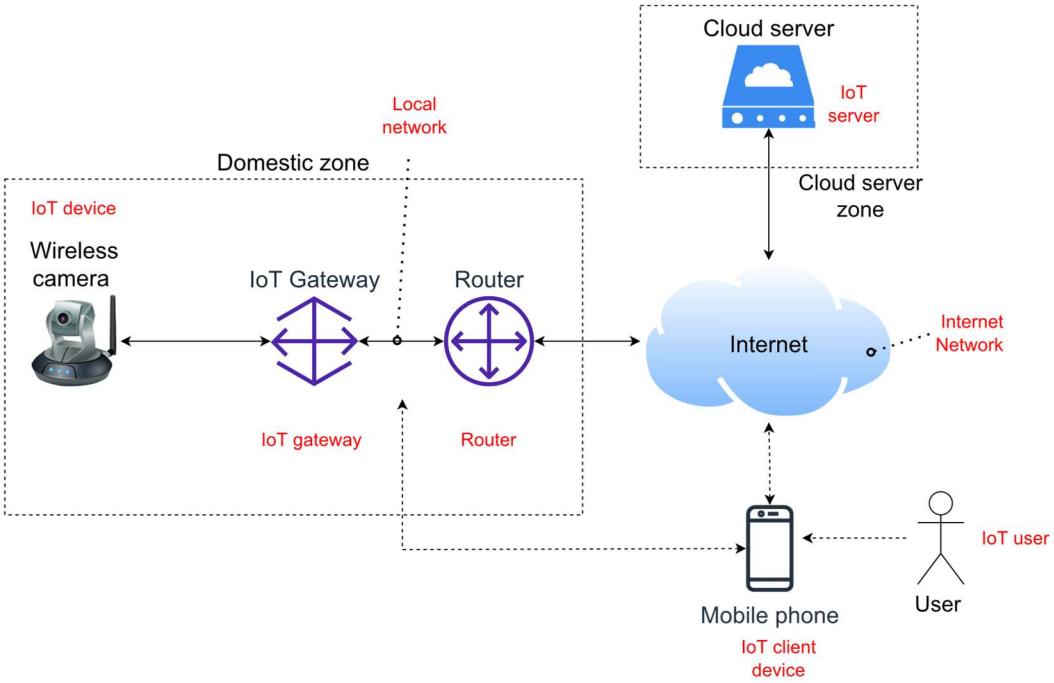

Figure 9 Example of a simple IoT network. Definitions and relationships between entities are in accordance with the conceptual IoT model of Figure 10.

The following (not complete, but as an example) analysis can be made using the terminology and conventions of the conceptual model:

The **IoT device** (wireless camera) interacts with the **IoT Server** (Cloud server) through the **internet network** to store camera recordings on the Cloud server. The IoT device and the IoT server both expose an **endpoint** on the internet network to enable data transfer on request of the IoT device. The IoT's endpoint is used to connect to the IoT server. The IoT server's endpoint is used to be evoked by other entities on the Internet network.

The **IoT device** (wireless camera) and **IoT client device** (mobile phone) interact via **the local network** to allow the IoT client device to change the IoT device's settings. The IoT device and the IoT client device both expose an **endpoint** on the local network to enable data transfer on request of the IoT client device. The IoT device's endpoint is used to be evoked by other entities on the local network. The IoT client device's endpoint is used to connect to the IoT device.

The **IoT client device** (mobile phone) and **IoT server** (Cloud server) interact with each other via **the Internet network** to download the stored data from the IoT server. The IoT client device and the IoT server both expose an **endpoint** on the Internet network to enable data transfer on request of the IoT client device. The IoT Server's endpoint is used to be evoked by other entities on the internet. The IoT Client Device's endpoint is used to connect to the IoT Server.

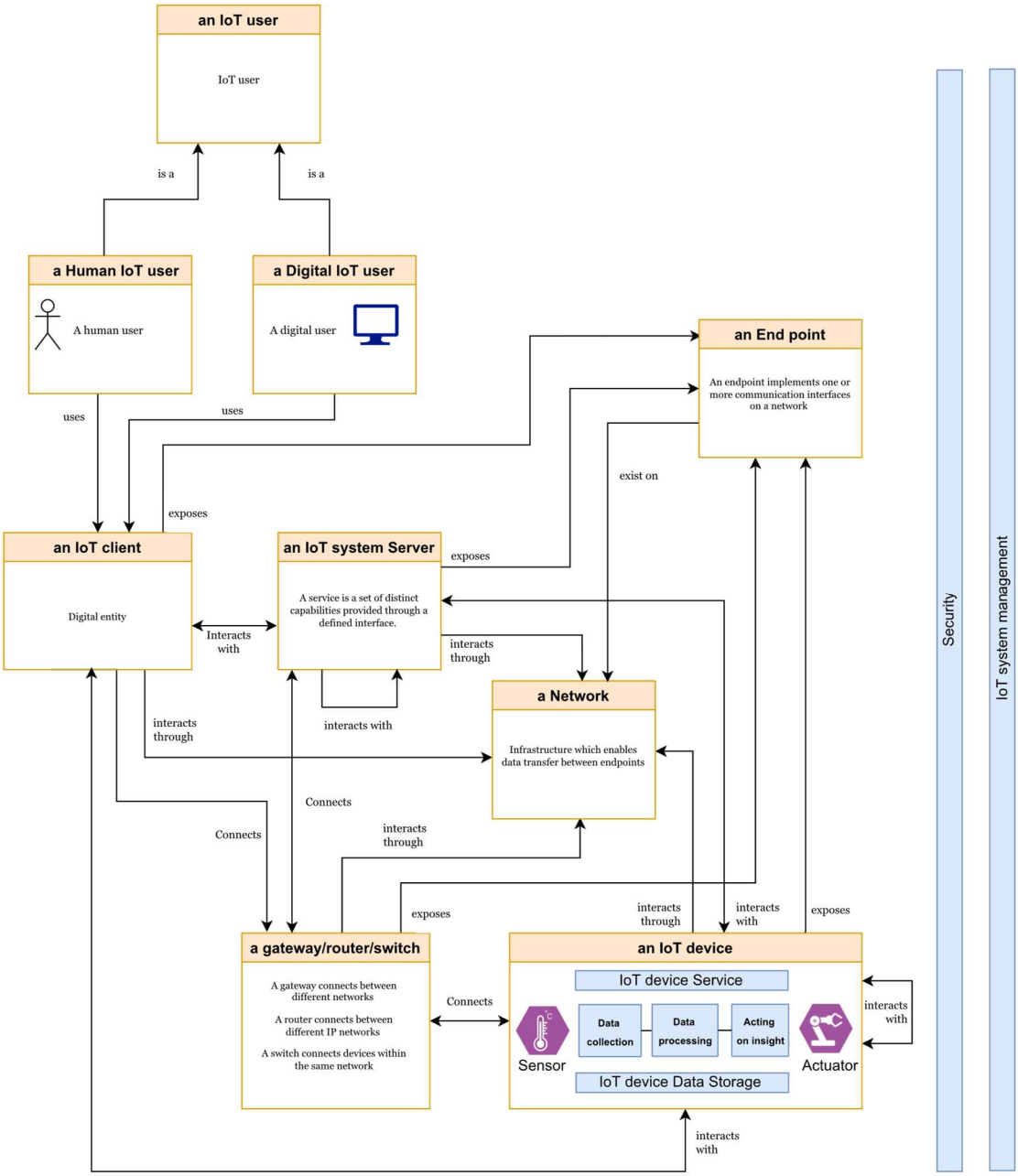

Figure 10 Conceptual IoT system, based on ISO/IEC 30141 [57] *and ITU* [52] *and Figure 7.*

9.4 Reference architectures

According to [56], a reference architecture "provides a template solution for an architecture for a particular domain. It also provides a common vocabulary with which to discuss implementations, often with the aim to stress commonality."

In [39], different IoT reference models are compared. Some reference models are included in standards in ITU-T [35] and ISO [38]. Vendor-specific reference architectures are also discussed (Microsoft, Intel, SAP WS2o). The vendors' architectures are all based on using (their own) cloud services. ITU-T and ISO are formulated more generally and do not explicitly mention the role of cloud services, which offers room for local solutions.

Figure 11 describes the four-layer ITU-T reference model [52]. The four layers of the model are the application layer, the service support and application support layer, the network layer and the device layer. The layers are distinguished from each other by the capabilities that are offered. The application layer contains the IoT applications. The service support and application support layer contain generic (for all IoT applications) and specific (for certain IoT applications) support capabilities like data storage and data processing. The network layer concerns networking and transport capabilities, and the device layer contains the device and gateway capabilities. In all layers, capabilities to manage and secure the IoT network apply.

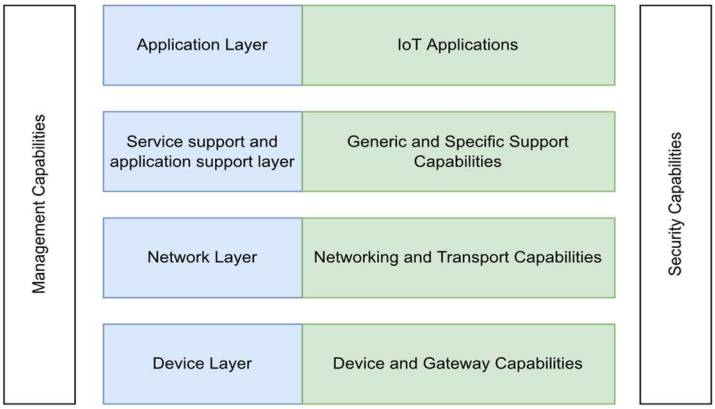

Figure 11 IoT reference model according to ITU-T [52]

9.5 Conclusion

This chapter constructs a conceptual model of an IoT system based on models from ISO/IEC 30141 [57] and ITU [52]. The model defines all entities in an IoT system and their (logical) relationships within the IoT system.

This thesis proposes to use this model when describing IoT devices and systems for performing cyber security risk analyses with Open Fair in the Risk Assesment layer of the “RED cyber security management system” from Figure 6.

10 Applicable and appropriate “authentication and access control requirements”

The first research question reads: *Which criteria and models could be used to determine if technical solutions in the harmonized standards for IoT devices are proportional to the cyber security risk they aim to address*?

In this context, the proposed “RED cyber security management system” model from Figure 6 has been developed and is described in Chapter 8.

The second research question is related and reads: *Could the criteria and models identified in research question 1 be used to determine the applicability of authentication and access control mechanism requirements for IoT devices? and to determine the appropriateness of specific authentication and access control mechanisms for particular IoT devices?*

This chapter answers this second research question by going through the Risk Assesment, Risk Reduction, Risk Evaluation and Acceptance processes from Figure 6. Interpretations of the terms “applicable” and “appropriate” are given.

10.1 Interpretation of “applicable” and “appropriate”

The developed “RED cyber security management system” from Figure 6 can be used to determine which security requirements are needed to reduce the cybersecurity risk of IoT devices to a predetermined Risk Acceptance level. This level should meet the cyber security protection objectives set by the RED's essential cyber security requirements.

In this section, the model from Figure 6 is applied to help select adequate “authentication and access control” requirements for IoT devices. The proposed approach is as follows:

As a first step, the conceptual model from Figure 10 is used to represent the IoT device in the intended IoT installation.

Subsequently, in the Risk Assesment phase, it is determined whether the risk of the IoT device without added “authentication and access controls” is below the Risk Acceptance level. In Figure 13, several options influencing the risk factors are added to the FAIR Risk Assesment model. This thesis uses information from the standards IEC 62443-3-3, ETSI 303645 [22] and NIST IR 8425 [23] for the authentication controls. Information from IEC 62443-3-3 [24] is used for the threat actor categories.

Suppose the risk analysis shows that without authentication and access controls, the IoT device (in its intended environment) presents a lower risk than the acceptable risk. In that case, it can be argued that technical specifications in a standard are not applicable to this device. However,

if the risk of the IoT device is higher than the Risk Acceptance level, then additional requirements are applicable.

If additional requirements are necessary, adequate “authentication and access controls” are selected in the Risk Reduction process of Figure 6 to ensure that the risk is sufficiently reduced. This is assessed in the Risk Evaluation process by performing a Risk Assesment based on the IoT device equipped with the selected “authentication and access controls”.
Suppose the risk has been reduced to the Risk Acceptance level. In that case, the selected "authentication and access controls" in the harmonized standard are made mandatory for the relevant IoT device in the Risk Acceptance process.

Suppose the technical specifications in the standard reduce the risk of the IoT device beyond the “Risk Acceptance level”. In that case, the requirements go too far and can be considered not “proportionate” and therefore “not appropriate”.

The processes of Risk Assesment, Risk Reduction and Risk Evaluation are repeated as often as necessary to achieve the desired Risk Reduction.

10.2 Example of IoT configuration facing Mirai bot threats

In this example, the Open FAIR Risk Assessment method [41] estimates the cyber security risk based on a scenario with a wireless IoT camera (with weak passwords) and Mirai bots [54] as threat actors. Figure 12 shows the fictitious scenario with an IoT device (wireless camera) connected to the Internet. According to the camera's intended use, the camera provides access to users from the Internet. Via a password (weak and not unique per device), access can be gained to stored camera images (privileged data) and device settings (privileged functions).

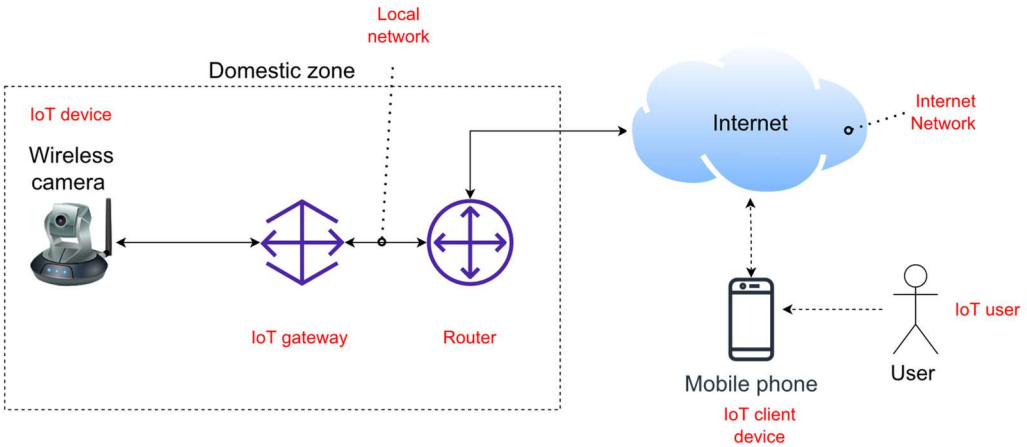

Figure 12 Example of an IoT configuration with a wireless camera.

A short description based on the conceptual model of Figure 10 on page 53 results in the following:

The **IoT client** device (mobile phone) and **IoT device** (wireless camera) interact via the **Internet network** to allow the IoT client device to change the IoT device's settings and download camera recordings. The IoT device and the IoT client device both expose an **endpoint** on the Internet network to enable data transfer on request of the IoT client device. The IoT device's endpoint is used to be evoked by other entities on the Internet network. The IoT client device's endpoint is used to connect to the IoT device.

An important detail is that the wireless camera exposes an endpoint on the Internet that can be evoked via the Internet by any entity.

Calculating the Threat Event Frequency by determining the Contact Frequency and the Probability of Action

The contact frequency is defined as the expected number of times per unit of time (e.g. per year) that the threat actor comes into contact with the asset. This contact can be physical or logical [58]. Although the IoT device is located in a trusted environment (home environment), an invokable endpoint is present on the Internet. A large number of individual Mirai bots are each able to search the internet for vulnerable devices. So the contact frequency can be regarded as "**high**".

The probability of action concerns the probability that the threat actors will attempt (regardless of whether the attempt is successful or not) to take a malicious action if he/she comes into contact with the Asset [58]. The Threat actors are the bots of the Mirai botnet trying to recruit new bots. These bots are programmed to always attempt to take malicious action. So the probability of action can be regarded as "**high**".

The Threat Event Frequency is determined by the Contact Frequency and the Probability of Action. It is defined as "the probable frequency, within a given time frame, that a Threat Agent will attempt to take a malicious action against an Asset" [58]. This is not necessarily a successful attack. The Threat Event Frequency is "**high**".

Calculating the Susceptibility by determining the Threat Capability and the Resistance Strength

The Threat Capability is the "probable level of force that a Threat Agent can apply against an Asset" [58]. The threat capability of a Mirai bot could be estimated as: "Intentional violation using simple means with low resources, generic skills and low motivation."[29] The Threat Capability is "**moderate**".

[29] Threat actor categories from IEC-62443-3-2 [46, p. 27] are used, which are also stated in Table 2 of this thesis.

Resistance strength is defined as “The strength of a Control as compared to the probable force that a Threat Agent is capable of applying against an Asset” [58]. As a first step, we assume that the wireless camera has a weak authentication and control mechanism with a default password. The Resistance Strength is “**low**”.

The Susceptibility is the probability that the “threat capability is greater than the resistance strength” [58]. This value will be high because the Mirai bot can most likely beat the resistance strength of the weak authentication mechanism. The Susceptibility is “**high**”.

Calculating the Risk by determining the Loss Event Frequency and the Loss Magnitude

Loss Event Frequency is defined as: “frequency within a given time frame that a Threat Agent will inflict harm upon an asset” [58]. Due to the high threat event frequency and high susceptibility, this Loss Event Frequency will be “**high**”.

Loss Magnitude is “the probable magnitude of loss resulting from a Loss Event” [58]. The primary Loss concerns unauthorized access to privileged device functions and unauthorized access to privileged data. Secondary losses could occur due to the botnet's malicious control over the device. The effects could vary from safety consequences to damage caused by DDoS attacks. The Loss Magnitude can be regarded as “**moderate**”.

The risk can be estimated as high because the Loss Event Frequency is “high” and the Loss Magnitude is “moderate”.

Risk reduction

However, the risk can be reduced by requiring in the harmonised standard for IoT devices that IoT devices having similar intended use as the example shall have a human user authentication mechanism and a unique per-device password when placed on the marked.

If the risk assessment is performed again, the Risk value will be greatly reduced because the Susceptibility has been lowered by increasing the Resutence strength of the IoT device.

10.3 Conclusion

The “RED cyber security management system” from Figure 6 is beneficial for linking technical requirements to IoT devices through Risk Assesment, Risk Reduction, Risk Evaluation and Risk Acceptance processes, with which the risk can be reduced to an acceptable level.

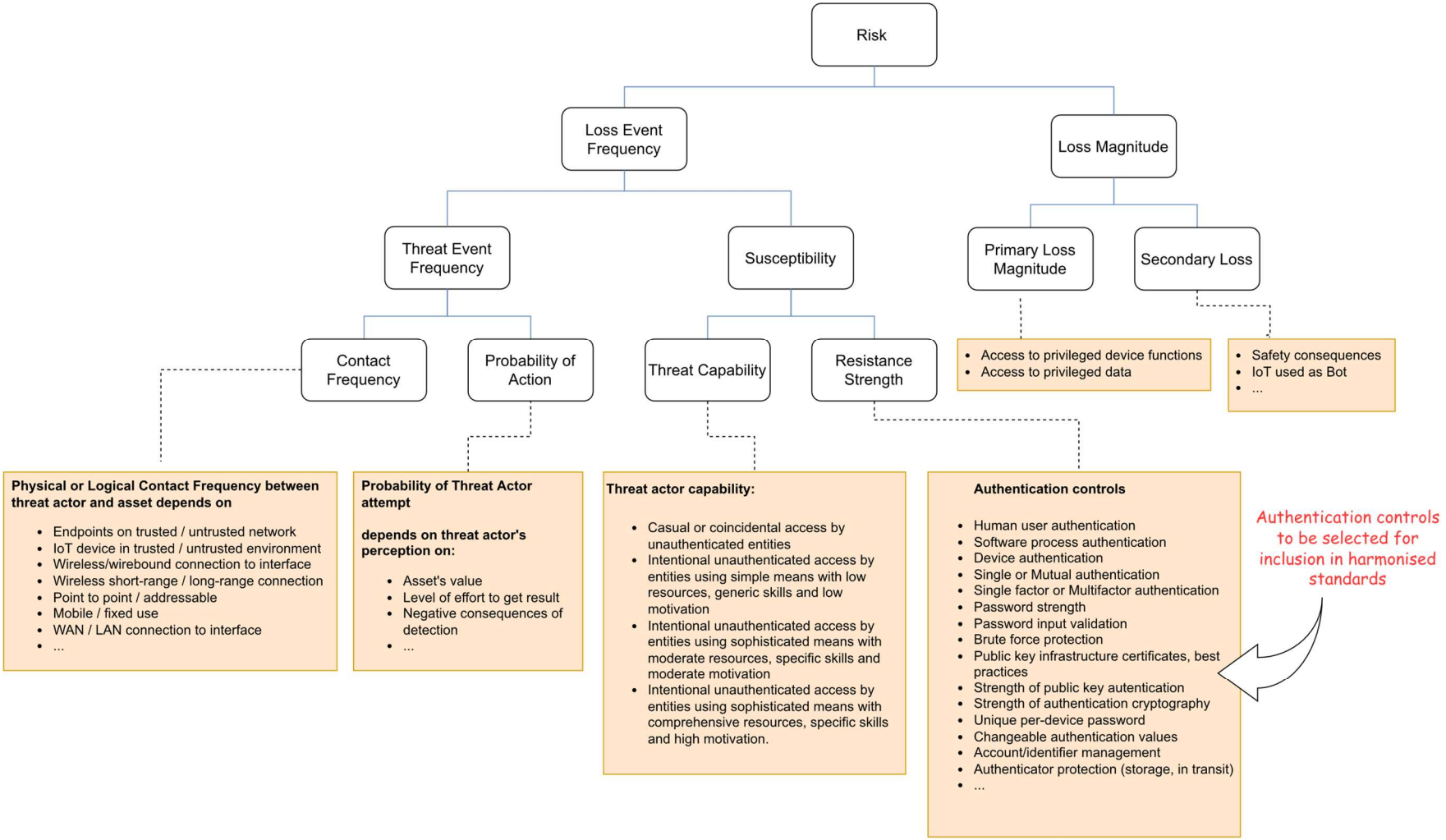

Figure 13 Open FAIR model. The orange boxes are added for the purpose of this thesis.

11 Conclusion

11.1 Summary

On 29 October 2021, the EC adopted a Delegated Regulation under the Radio Equipment Directive, extending the existing radio equipment requirements with “cybersecurity by design” requirements. Wireless internet-connected devices must comply with these cyber security requirements from August 2024 as a precondition for placing on the market IoT devices in the EU.

The RED essential cyber security requirements set “goals” but do not give technical solutions to fulfil these “essential requirements”. A formal standardisation process exists in which the essential requirements are elaborated in technical specifications to be included in harmonised standards. Via a so-called “EC standardisation request” [16], the EC has requested CEN/CENELEC to develop these harmonised standards.

The EC standardization request [17, p. 2] explicitly states that “technical solutions included in the harmonized standards shall be based on ***Risk Assesment*** *and* ***Risk Reduction****”* and that “the technical solutions laid down in the harmonised standards shall be **proportionate to the risk** that they aim to address.”

This risk-based approach is new under the RED because the Risk Assesment and reduction process is not required for developing standards for non-cyber security-related RED essential requirements. The EC standardisation request does not provide information on how to implement the Risk assessment and risk reduction processes. Moreover, there is currently no harmonised standard available for the cyber security of products that can serve as an example for the harmonised standards to be developed in support of the RED cyber security essential requirements.

This thesis develops a model that can be used in standardization activities for the RED to determine whether technical solutions in harmonised standards for IoT devices are proportionate to the risk they aim to address. The developed model is referred to as the “RED cyber security management system” The model maps the RED processes in three layers. The Risk Governance layer maps the legislators' processes regulating the cyber risks of IoT devices. The Risk Management layer maps processes that members of standardization organizations perform in the development of RED harmonized standards. The Risk Assesment layer maps the processes for selecting technical solutions for RED harmonized standards. This thesis proposes to incorporate the ISO 27005 Risk Management framework and the Open FAIR Risk Assesment framework in the “RED cyber security management system”.

The developed “RED cyber security management system” has shown to be beneficial for linking technical requirements to IoT devices. In a simple IoT scenario, It was shown that the model could be used to determine the applicability of authentication and access control mechanism requirements for IoT devices

11.2 Open directions and follow-up research

Using the RED cyber security management system

The author of this thesis participates in the CEN/CENELEC standardization committee JTC13-WG8 that deals with the harmonized standards for the RED and has already taken the first steps to gain support for the application of the "RED cyber security management system" in developing harmonized standards.

The "RED cyber security management system" has a modular structure and can be used with a Risk management framework other than ISO 27005 or a Risk assessment framework other than Open Fair. The governance layer (which is now focused on the RED legislation) can also be adapted to other NLF product legislation acts, such as the future Cyber Resilience Act.

In particular, much practical experience will have to be gained about how a cyber security standardization process can best be implemented.

Cyber Security Risk Acceptance Level: Who should set this level?

A critical input parameter of the "RED cyber security management system" is the Risk Acceptance level. According to the "RED cyber security management system", the technical IoT requirements (to be included in the harmonised standards) shall reduce the IoT risk to the Risk Acceptance level. If, by applying technical solutions to the IoT device, the risk level becomes lower than the Risk Acceptance Level, then the technical solutions are adequate and will be accepted for inclusion in the harmonised standard in the Risk Acceptance phase. The Risk Acceptance level determines the level of cyber security protection the harmonised standard shall achieve.

If the legislators would determine and provide the Risk Acceptance level, then the standardisation organisation has clarity on the level of protection that the harmonised standards shall achieve. Suppose the Risk Acceptance level is not set by the legislators (which is the case for the RED), then the standardisation organisation should determine the Risk Acceptance level itself. However, this could result in political discussions between stakeholders, which should be avoided according to The Vademecum on European Standardization [18]–[20].

Follow-up research could reveal whether future cyber security product legislation (like the CRA) should leave the decision on Risk Acceptance levels at the standardization organisations or whether the legislators should provide and impose this level.

Reproducibility of results obtained with the "RED cyber security management system"

With the "RED cyber security management system", it can be determined whether technical solutions in harmonized standards for IoT devices are proportional to the risk they aim to address. In future research, the reproducibility of the results obtained with the "RED cyber security management system" could be investigated: To what extent are the outcomes identical if different independent parties use the model?

ANNEX 1

— The restriction of the use of certain hazardous substances in electrical and electronic equipment (Directive 2011/65/EU)

— Appliances burning gaseous fuels (Regulation (EU) 2016/426)

— Ecodesign requirements for energy-related products (Directive 2009/125/EC and all implementing Regulations for specific product groups that have been adopted under this Framework Directive)

— Simple pressure vessels (Directive 2014/29/EU)

— Toys' safety (Directive 2009/48/EC)

— Electrical equipment designed for use within certain voltage limits (Directive 2014/35/EU)

— Machinery (Directive 2006/42/EC)

— Electromagnetic compatibility (Directive 2014/30/EU)

— Measuring instruments (Directive 2014/32/EU)

— Non-automatic weighing instruments (Directive 2014/31/EU)

— Cableway installations (Regulation (EU) 2016/424)

— Radio equipment (Directive 2014/53/EU)

— Medical devices (Regulation (EU) 2017/745, replacing Directives 90/385/EEC and 93/42/EEC as of 26 May 2021)

— *In vitro* diagnostic medical devices (Directive 98/79/EC to be replaced by Regulation (EU) 2017/746 as of 26 May 2022)

— Pressure equipment (Directive 2014/68/EU)

— Transportable Pressure equipment (Directive 2010/35/EU)

— Aerosol Dispensers (Directive 75/324/EEC as amended)

— Lifts (Directive 2014/33/EU)

— Recreational craft (Directive 2013/53/EU)

— Equipment and protective systems intended for use in potentially explosive atmospheres (Directive 2014/34/EU)

— Explosives for civil uses (Directive 2014/28/EU)

— Pyrotechnics (Directive 2013/29/EU)

— Regulation on the Labelling of Tyres (Regulation (EU) No 2020/740)

— Personal protective equipment (Regulation (EU) 2016/425)

— Marine equipment (Directive 2014/90/EU)

— Noise emission in the environment by equipment for use outdoors (Directive 2000/14/EC)

— Emissions from non-road mobile machinery (Regulation (EU) 2016/1628)

— Energy labelling (Regulation (EU) 2017/1369 and all delegated Regulations for specific product groups that have been adopted under this Framework Regulation and those adopted under Directive 2010/30/EU, the predecessor of Regulation 2017/1369)

— Fertilising Products (Regulation (EU) 2019/1009)

— Unmanned aircraft systems (drones) (Commission Delegated Regulation (EU) 2019/945)

Figure 14: Harmonised product legislation for different categories of products [27]

[1] STRICT, “Report on IoT Device Security,” 2019. https://www.agentschaptelecom.nl/documenten/rapporten/2019/09/25/rapport-digitale-veiligheid-van-iot-apparatuur (accessed Nov. 18, 2022).
[2] ANEC, “Cybersecurity for Connected Products,” 2018, Accessed: Nov. 21, 2022. [Online]. Available: www.beuc.eu.
[3] European Commission, “IMPACT ASSESSMENT REPORT Accompanying the document Commission Delegated Regulation supplementing Directive 2014/53/EU of the European Parliament and of the Council with regard to the application of the essential requirements referred to in Article 3(3), p,” 2021.
[4] Cisco, “Cisco: 2020 CISO Benchmark Report,” *Comput. Fraud Secur.*, vol. 2020, no. 3, pp. 4–4, 2020, doi: 10.1016/s1361-3723(20)30026-9.
[5] European Commission, “Annexes to the Impact Assessment Report Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020,” 2022.
[6] The European Parliament and the Council of the European Union, “GDPR: REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (Gene,” *OJEU*. 2016, doi: 10.1308/rcsfdj.2018.54.
[7] The European Parliament and the Council of the European Union, “NIS Directive: DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.” 2016.
[8] The European Parliament and the Council of the European Union, *Cyber Security Act: Regulation (EU) 2019/881 of the European Parliament and of the Council on ENISA and on Information and Communications Technology Cybersecurity Certification and Repealing Regulation*, vol. 2019, no. L151/15. 2019.
[9] The Netherlands; Ministry of Economic Affairs and Climate Policy, “EG RE (02)05r02 Cyber security Baseline Requirements IoT.” https://circabc.europa.eu/ui/group/43315f45-aaa7-44dc-9405-a86f639003fe/library/b4016779-5e33-4298-b64e-a2cce6f4dba2/details (accessed Nov. 20, 2022).
[10] European Commission, “The EU’s Cybersecurity Strategy for the Digital Decade EN,” 2020, [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020JC0018&from=EN.
[11] European Commission, “COMMISSION DELEGATED REGULATION (EU) 2022/30 of 29 October 2021 supplementing Directive 2014/53/EU of the European Parliament and of the Council with regard to the application of the essential requirements referred to in Article 3(3), points (d), (e) and,” 2021, doi: 10.4324/9781849776110-28.
[12] The European Parliament and the Council of the European Union, *Radio Equipment Directive: Directive 2014/53/EU of the European Parliament and of the Council - of 16 April 2014 - on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Direct*. 2014.
[13] European Commission, “CRA: Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020,” 2022, [Online]. Available: https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act.
[14] European Commission, “Commission strengthens cybersecurity of wireless devices.” https://ec.europa.eu/commission/presscorner/detail/en/ip_21_5634 (accessed May 08, 2022).
[15] European Union, “Regulation (EU) No 1025/2012 of the European Parliament and of the

Council of 25 October 2012 on European standardisation." https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32012R1025 (accessed Sep. 03, 2022).
[16] European Commission, "COMMISSION IMPLEMENTING DECISION on a standardisation request to the European Committee for Standardisation and the European Committee for Electrotechnical Standardisation as regards radio equipment in support of Directive 2014/53/EU of the European Parli," 2022, [Online]. Available: https://ec.europa.eu/transparency/documents-register/detail?ref=C(2022)5637&lang=en.
[17] European Commission, "ANNEXES to the Commission Implementing Decision on a standardisation request to the European Committee for Standardisation and the European Committee for Electrotechnical Standardisation as regards radio equipment in support of Directive 2014/53/EU of the," 2022, [Online]. Available: https://ec.europa.eu/transparency/documents-register/detail?ref=C(2022)5637&lang=en.
[18] European Commission, "Vademecum on European Standardisation in support of Union Legislation and policies PART I Role of the Commission's Standardisation requests to the European standardisation organisations," 2015, [Online]. Available: https://ec.europa.eu/docsroom/documents/13507/attachments/1/translations.
[19] European Commission, "Vademecum on European standardisation in support of Union legislation and policies PART II Preparation and adoption of the Commission's standardisation requests to the European standardisation organisations," 2015, [Online]. Available: https://ec.europa.eu/docsroom/documents/13508/attachments/1/translations.
[20] European Commission, "Vademecum on European standardisation in support of Union legislation and policies PART III Guidelines for the execution of standardisation requests EN," 2015, [Online]. Available: https://ec.europa.eu/docsroom/documents/13509/attachments/1/translations.
[21] IEC, "IEC 62443-3-3 Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels," 2013.
[22] ETSI, *ETSI EN 303 645. CYBER; Cyber Security for Consumer Internet of Things*, vol. 1. 2019.
[23] M. Fagan, B. Cuthill, M. Fagan, and K. N. Megas, "NIST Internal Report Profile of the IoT Core Baseline for Consumer IoT Products NIST IR 8425 Profile of the IoT Core Baseline for Consumer IoT Products."
[24] The European Parliament and the Council of the European Union, "Decision 768/2008/EC: common framework for the marketing of products," *Official Journal of the European Union*. p. 768/2008/EC, 2008.
[25] the Council of the European Union, "REGULATION (EC) No 765/2008 Requirements for accreditation and market surveillance relating to the marketing of products," 2008, [Online]. Available: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:218:0030:0047:en:PDF.
[26] the Council of the European Union, "REGULATION (EU) 2019/ 1020 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL- of 20 June 2019 - on market surveillance and compliance of products and amending Directive 2004/ 42/ EC and Regulations (EC) No 765/ 2008 and (EU) No 305/ 2011," vol. 2019, no. June, 2019, [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019R1020&qid=1652431784207.
[27] European Commission, "The 'Blue Guide' on the implementation of EU product rules 2022," 2022. Accessed: Sep. 03, 2022. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:C:2022:247:TOC.
[28] European Commission, "Evalation of the New Legislative Framework," 2022, [Online]. Available: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12654-Industrial-products-evaluation-of-the-new-legislative-framework_en.
[29] European Commission, *Supporting Study for the evaluation of certain aspects of the New Legislative Framework*. 2022.
[30] European Commission, "General framework of European standardisation policy." https://single-market-economy.ec.europa.eu/single-market/european-

standards/standardisation-policy/general-framework-european-standardisation-policy_en (accessed Oct. 12, 2022).
[31] The Council of the European Union, “The Treaty on the Functioning of the European Union (consolidated version).” doi: 10.1080/03235408.2013.817161.
[32] European Commission, “Decision No 768/2008/EC of the European Parliament and of th... - EUR-Lex.” https://eur-lex.europa.eu/legal-content/EN/LSU/?uri=CELEX%3A32008D0768 (accessed Oct. 30, 2022).
[33] European Commission, “Supplementary Guidance on the LVD/EMCD/RED,” 2018.
[34] European Commission, “EG RE (06)06 - Preliminary Q&As on certain issues arising in relation to the security of products (connected products) as well as software.” 2020, [Online]. Available: Preliminary Q&As on certain issues arising in relation to the security of products (connected products) as well as software.
[35] European Commission, “COMMISSION IMPLEMENTING DECISION of 4.8.2015 on a standardisation request to the European Committee for Electrotechnical Standardisation and to the European Telecommunications Standards Institute as regards radio equipment in support of Directive 2014/53/,” 2015, [Online]. Available: https://ec.europa.eu/transparency/documents-register/detail?ref=C(2015)5376&lang=en.
[36] European Commission, “An EU Strategy on Standardisation - Setting global standards in support of a resilient, green and digital EU single market.” https://ec.europa.eu/docsroom/documents/48598 (accessed Sep. 03, 2022).
[37] The European Parliament and the Council of the European Union, “Medical Device Regulation: REGULATION (EU) 2017/745 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directi.”
[38] The European Parliament and the Council of the European Union, “Regulation (EU) 2017/746 of the European parliament and of the council on in vitro diagnostic medical devices,” *Official Journal of the European Union*, vol. 5, no. 5. pp. 117–176, 2017.
[39] ISO, “ISO IEC 27000 Information technology — Security techniques — Information security management systems — Overview and vocabulary,” 2018.
[40] European Commission, “Single Market for Goods,” 2023. https://single-market-economy.ec.europa.eu/single-market/goods_en (accessed Jan. 07, 2023).
[41] The Open Group, “The Open Group Risk Analysis (O-RA),” 2021, [Online]. Available: www.opengroup.org/legal/licensing.
[42] M. B. A. van Asselt and O. Renn, “Risk governance,” *J. Risk Res.*, vol. 14, no. 4, pp. 431–449, 2011, doi: 10.1080/13669877.2011.553730.
[43] Terje Aven, *The Science of Risk Analysis*. 2020.
[44] ISO, “ISO/IEC 27005 Information technology — Security techniques — Information security risk management,” 2018.
[45] ISO, “ISO 31000:2018, Risk management - Guidelines,” 2018.
[46] IEC, “IEC 62443-3-2 Security for industrial automation and control systems - Part 3-2: Security risk assessment for system design,” 2020.
[47] IEC, “IEC 62443-4-2 Security for industrial automation and control systems - Part 4-2: Technical security requirements for IACS components,” 2019.
[48] ENISA, *INTEROPERABLE EU RISK Methodology for and assessment of interoperability*, no. January. 2022.
[49] ENISA, *COMPENDIUM of risk management frameworks with potential interoperability*, no. January. 2022.
[50] The Open Group, *FAIR – ISO / IEC 27005 Cookbook*. 2010.
[51] E. Borgia, “The Internet of Things vision: Key features, applications and open issues,” *Comput. Commun.*, vol. 54, pp. 1–31, 2014, doi: 10.1016/j.comcom.2014.09.008.
[52] International Telecommunication Union (ITU-T), “Overview of the Internet of things,” no. Y.2060, 2012.

[53] M. Milenkovic, “Internet of Things: System Reference Architecture,” 2022.
[54] Manos Antonakakis *et al.*, “Understanding the Mirai Botnet,” *Proc. 26th USENIX Secur. Symp.*, pp. 1–19, 2017, [Online]. Available: https://www.usenix.org/system/files/conference/usenixsecurity17/sec17-antonakakis.pdf.
[55] W. Kassab and K. A. Darabkh, “A–Z survey of Internet of Things: Architectures, protocols, applications, recent advances, future directions and recommendations,” *Journal of network and computer applications*, 2020. .
[56] B. Di Martino, M. Rak, M. Ficco, A. Esposito, S. A. Maisto, and S. Nacchia, “Internet of things reference architectures, security and interoperability: A survey,” *Internet of Things*, vol. 1–2, pp. 99–112, 2018, doi: 10.1016/j.iot.2018.08.008.
[57] ISO/IEC, “ISO/IEC 30141 Internet of Things (IoT) – Reference architecture.” 2018.
[58] The Open Group, “Risk Taxonomy (O-RT).” 2021, [Online]. Available: https://publications.opengroup.org/downloadable/download/link/id/MC43Nzg0NzcwMCAxNjY0OTU3MDQyMTY1NzU1NjE2OTQ2OTMxMjc4/.
[59] European Commission, *Europeans’ attitudes towards Internet security Fieldwork, Special Eurobarometer 480 Report European*. 2019.
[60] European Commission, “Single market for goods.” https://single-market-economy.ec.europa.eu/single-market/goods_en (accessed Oct. 15, 2022).