

Aalto University  
School of Science  
Master's Programme in Computer, Communication and Information Sciences

Anna Mikhaleva

# Cybersecurity Standard Compliance in Development of Distributed Embedded Systems

Master's Thesis  
Espoo, November 21, 2022

Supervisor: Professor Tuomas Aura, Aalto University  
Advisor: Mika Katara, D.Sc. (Tech.), KONE Corporation

<b>Author:</b>	Anna Mikhaleva	
<b>Title:</b>	Cybersecurity Standard Compliance in Development of Distributed Embedded Systems	
<b>Date:</b>	November 21, 2022	<b>Pages:</b> 71
<b>Major:</b>	Security and Cloud Computing	<b>Code:</b> SCI3084
<b>Supervisor:</b>	Professor Tuomas Aura	
<b>Advisor:</b>	Mika Katara, D.Sc. (Tech.), KONE Corporation	
	<p>In recent years, communication technologies have been actively developed and used in the machinery manufacturing industry. They allow distributed embedded systems to operate more efficiently by remotely interacting with each other and with maintenance systems. However, the ability of machines to communicate through the Internet has increased the number of attack vectors that a potential attacker can utilize. In the lift industry, cybersecurity incidents can lead to a malfunction of lift systems, disruptions to transportation services and irreparable damage to people's lives. The manufacturer can implement security measures from industrial cybersecurity standards to prevent cybersecurity incidents that involve the developed products, to improve security of industrial systems and to ensure safety of their users. Nonetheless, the cybersecurity standards compliance process can be challenging for the product developers. Our intention is to apply this process to the development of distributed embedded systems.</p> <p>In this thesis project, we conducted research on the cybersecurity standards of the IEC 62443 series that are applicable in the lift industry. We analyzed ISO 8102-20 that was published in August 2022 to cover cybersecurity for lifts. We also applied this standard to the development of a prototype of a lift controller in a case study. We document the process of applying ISO 8102-20, present insights into the new standard and underline some areas for improvement.</p>	
<b>Keywords:</b>	ISO 8102-20, IEC 62443-4-1, IEC 62443-4-2, IoT, cybersecurity standards, compliance, certification	
<b>Language:</b>	English	

# Acknowledgements

I wish to sincerely thank Professor Tuomas Aura for supervising the thesis and giving constructive advice and valuable suggestions for improvements.

I would like to express my special gratitude to Mika Katara for providing his constant guidance and feedback throughout my work on this master's thesis. Many thanks to Jussi Valkiainen for reviewing the thesis and Mohit Sethi for the invaluable insight into the IoT security. I also would like to thank my colleagues in KONE cybersecurity team for sharing their extensive knowledge.

I would like to thank my family and friends for their support. I am very grateful to my mother for her endless love and everything she has done for me. I thank my boyfriend for believing in me and his constant help to overcome all problems.

Espoo, November 21, 2022

Anna Mikhaleva

# Abbreviations and Acronyms

4G	Fourth generation wireless
AF	Automation Federation
ANSI	American National Standards Institute
ASCI	Automation Standards Compliance Institute
CA	Conformity assessment
CB	Certification Body
CIA	Confidentiality, integrity, and availability
CBTLs	Certification Body Testing Laboratories
CEN	European Committee for Standardization
CR	Component requirement
CSA	Component Security Assurance
CSF	NIST Cybersecurity Framework
CSMS	Cybersecurity management system
CSRC	Computer Security Resource Center
DevOps	Software development and operations
DM	Defect management
EN	European Standards
EU	European Union
EUC	Equipment under control
FR	Foundational requirement
GSM	Global System for Mobile Communications
IACS	Industrial automation and control systems
IEC	International Electrotechnical Commission
IECEE	IEC System of Conformity Assessment Schemes for Electrotechnical Equipment and Components
IECEX	IEC System for Certification to Standards Relating to Equipment for Use in Explosive Atmospheres
IECQ	IEC Quality Assessment System for Electronic Components

IECRE	IEC System for Certification to Standards Relating to Equipment for Use in Renewable Energy Applications
IIoT	Industrial IoT
ISA	International Society of Automation
ISAGCA	ISA Global Cybersecurity Alliance
ISCI	ISA Security Compliance Institute
ISMS	Information security management system
IoT	Internet of Things
ISO	International Organization for Standardization
IT	Information technology
LAN	Local area network
ML	Maturity level
NCB	National Certification Body
NDR	Network device requirement
NIST	National Institute of Standards and Technology
PESSRAL	Programmable electronic system in safety related applications for lifts
RE	Requirement enhancement
SD	Secure by design
SDL	Secure development lifecycle
SDLA	Security Development Lifecycle Assurance
SDoC	Supplier's declaration of conformity
SG	Security guidelines
SI	Secure implementation
SIL	Safety integrity level
SL	Security level
SL-T	Target security level
SL-C	Capability security level
SL-A	Achieved security level
SM	Security Management
SP	Special Publication
SR	System requirements
SSA	System Security Assurance
SUM	Security update management
SVV	Security verification and validation testing
TC	Technical committee
TR	Technical Report
TS	Technical specification
USB	Universal Serial Bus
VoIP	Voice over Internet Protocol
VPC	Virtual private cloud

# Contents

Abbreviations and Acronyms	4
<b>1 Introduction</b>	<b>8</b>
<b>2 Security standards</b>	<b>11</b>
2.1 International standards . . . . .	11
2.2 Industrial cybersecurity standards . . . . .	14
<b>3 Security standards certification</b>	<b>21</b>
3.1 Standards compliance . . . . .	21
3.2 Limitations of the standards compliance . . . . .	23
3.3 Standards certification schemes . . . . .	23
3.3.1 IECEE . . . . .	23
3.3.2 ISASecure . . . . .	24
3.4 Benefits of certification . . . . .	26
3.5 IEC 62443-4-1 certification . . . . .	27
3.6 IEC 62443-4-2 certification . . . . .	30
<b>4 Safety and security standards for lifts</b>	<b>31</b>
4.1 Safety standards . . . . .	31
4.1.1 EN 81 series . . . . .	32
4.1.2 ISO 12100 . . . . .	32
4.1.3 ISO 8100 . . . . .	34
4.2 Security standards . . . . .	35
4.2.1 IEC 62443-4-1 . . . . .	36
4.2.2 IEC 62443-4-2 . . . . .	38
4.3 ISO 8102-20 . . . . .	40
<b>5 Case study of security certification</b>	<b>43</b>
5.1 Distributed embedded systems and IoT . . . . .	43
5.2 KONE Corporation . . . . .	45

5.3	Product for certification . . . . .	46
<b>6</b>	<b>Implementation</b>	<b>49</b>
6.1	Identification of scope . . . . .	49
6.2	Identification of zones and domains . . . . .	50
6.3	Security requirements creation . . . . .	52
6.4	Security requirements testing . . . . .	55
<b>7</b>	<b>Observations on ISO 8102-20 and evaluation</b>	<b>57</b>
7.1	Contribution of ISO 8102-20 . . . . .	57
7.2	Observations on ISO 8102-20 . . . . .	59
7.3	Evaluation of implementation . . . . .	61
<b>8</b>	<b>Conclusion</b>	<b>64</b>

# Chapter 1

## Introduction

Information technologies are constantly evolving to provide the essentials for the information age and to make people's lives easier. To achieve these results, a lot of attention is paid to the device connectivity and systems communications. The Internet of Things (IoT) is a paradigm that is used to connect distributed embedded systems to large-scale networks [50]. Nowadays, the IoT is widely applied in different areas, such as healthcare, smart cities, smart homes, self-driving cars, and manufacturing industry [45].

Since many components are no longer isolated and are connected to other systems via communication networks, there is an increase in the number of cybersecurity threats and risks [42]. This is especially dangerous for machinery manufactures because cybersecurity incidents affect not only organizational assets and operations, but they can also affect safety of its developed products. For this reason, industrial companies need to establish and apply appropriate security measures to reduce information security risks and to defend themselves and their customers against cybersecurity attacks.

These measures can be found in information security standards that define security controls and requirements for information and cybersecurity in organizations. For instance, the ISO/IEC 27000 series of standards covers different aspects of information security: information security management system, risk management, network security, application security [6]. On the other hand, the IEC 62443 series of standards was developed to address cybersecurity for industrial communications networks and industrial automation and control systems (IACS). Compliance with these international standards increases the security of the organizations and their products against intentional harm from attackers. Moreover, it protects companies and their partners from unpleasant consequences of cyberattacks, such as financial and reputational losses [26].

Furthermore, customers and consumers are concerned about security-

related issues. They need to be confident in the reliability of the purchased products [15]. Problems with the use of these products can also negatively affect their business.

In order to assure customers that the offered product and its development process comply with cybersecurity standards, companies request a certification procedure. During it, the auditor assesses documentation required by the standard, examines its practical application, and, if all the requirements are fulfilled, issues a certificate of compliance. The certificate demonstrates the level of information and cybersecurity measures implemented in the product development process.

Consequently, meeting cybersecurity standards requirements not only minimizes the risks of a successful cyberattack on the organization, but also is a competitive advantage among companies in the market.

It can be a challenge for companies to attest the security of their development processes and products [51]. This is especially the case when the development was started before making a decision to follow the requirements of a particular standard. In this case, the company should study the standard in detail, carefully assess the already implemented processes and security capabilities, and record what is missing and what needs to be improved. The company should also decide who will be responsible for making changes in company's processes, assign roles and tasks, create the required documentation, and resolve how to accomplish all these tasks without business interruption. Additionally, descriptions of some requirements in the standard can be quite vaguely defined or insufficient for new technologies. As a result, separate teams inside of the company can interpret and implement them differently [41].

Furthermore, cybersecurity standards for the industrial product development are relatively new, they are not free to use and can be over the budget for researchers. Additionally, it is not in the interest of companies to publicly share their findings, knowledge, and experience about these standards.

Taking into consideration the above-stated problems, we intend to conduct research on cybersecurity standard compliance in the development of distributed embedded systems. The defined goals of the thesis are:

- survey of cybersecurity standards and certification processes for the development of embedded systems;
- analysis of the relationship between security and safety in the lift industry;
- application of the cybersecurity standard ISO 8102-20:2022 to the development of a lift controller; and

- documenting lessons from the process of preparing for cybersecurity standards compliance certification in distributed embedded systems development.

One research method used in this thesis is based on studying and analyzing the industrial standards. These standards are applicable to the lift industry to ensure safety and security of the product. Each standard is developed by the technical commission of the organizations for standardization and acclaimed by experts in the scope of the standard. Another method is the practical application of the ISO 8102-20 standard in the case study. This cybersecurity standard was published in August 2022. Therefore, it is new for the industry. At the time of writing this thesis, the practical application of the standard has not been studied in academic or professional literature. The case study was conducted as preparation for the ISO 8102-20 compliance and certification process at KONE. The author participated in this ongoing process.

The rest of this thesis is structured as follows. Chapter 2 provides general information about security standards. Chapter 3 presents an overview of security standards compliance and certification process. Chapter 4 surveys essential standards for lifts including cybersecurity standards that are applicable in the development of distributed embedded lift systems. Chapter 5 presents a case study. Chapter 6 provides the practical application of the cybersecurity standard for lifts, escalators and moving walks to the prototype of a lift controller. Chapter 7 discusses ISO 8102-20 and observations made during this process. It also evaluates the application of the standard in the case study. Finally, Chapter 8 provides the summary of this thesis.

## Chapter 2

# Security standards

In this chapter, terms standard and international standard are defined. Then, the chapter describes three standardization bodies that create standards for national and international use: the ISO, IEC and NIST. It also provides detailed description of the IEC 62443 series of standards that was created by IEC to manage cybersecurity of industrial systems. Moreover, the application of the IEC 62443 standards in the product lifecycle for IACS is specified with the definition of the roles involved in it.

### 2.1 International standards

A standard is a document that describes rules, guidelines and characteristics for processes or their products to achieve the optimum level of features, such as safety, security, and quality. The standard also may contain practical information and practices and provide methods of operation and making products in an agreed manner. It is based on the consolidated scientific and technological results, established by consensus among experts and approved by a recognized body [31]. The standard defines acceptance criteria which can be expressed in the form of having a certain activity in the processes.

An international standard is a standard that can be applied globally or be mandatory for compliance in various countries or supranational unions. It may also describe a solution to a global problem or challenges. This document is adopted by an international organization and is available to the public from different countries.

The presence of standards is necessary for various reasons. For example, the standards define non-functional requirements for the product, such as security. Typically, the customer cannot fully test the security of the product and its embedded components before purchasing it. Therefore, understand-

ing what standards the manufactured product meets increases customer trust to the product and improves market efficiency.

There are a lot of different standardization bodies that publish standards for international use. The International Organization for Standardization (ISO) is an independent, non-governmental organization that produces international standards and provides a platform for developing practical tools through general understanding and collaboration with all stakeholders. It sells the standards documents to finance the development of new standards and proper maintenance of already published documents.

The standards that were created by ISO allow manufacturers to produce compatible products. These products can be used in various industry sectors and countries by users with different experience. Moreover, the products can work well together and with products of other manufacturers if they meet the unified standard requirements. The standards also can help to identify quality, safety and security issues of developed products, provided services, and implemented processes. They give ideas for improving production operations, solutions to problems that arise during the operation of a company, codify well-known methods, and best management practices.

ISO has established a lot of widely used standards. The best known among them are management systems standards that address most common and frequent challenges for companies. For example, the ISO 9000 family of standards covers different aspects of quality management with the focus on expectations of customers. It aims to improve the quality of products, services, engagement of employees in business processes and experience of customers.

Another well-known family of management standards is the ISO/IEC 27000. It covers an information security management system (ISMS) and provides requirements for it. ISMS can be implemented in organizations of different sizes and areas of activity and enables them to manage security of their information assets. The assets can be confidential information, such as financial data or employee details, intellectual property, contracts with other companies or documented internal processes.

Ideally, it is possible to have a unified management system that addresses quality and security aspects. For this reason, the ISO 9001 and ISO/IEC 27001 standards that provide requirements for management systems have the same clause structure and the terminology. This not only improves alignment between the standards but also simplifies the creation and efficient development of quality and security management systems in organizations.

International Electrotechnical Commission (IEC) is an international standards organization that creates and publishes standards for electric and electronic technologies. IEC International Standards are the result of the coop-

eration of a lot of technical experts who represent partner countries in the IEC. These standards give rules, instructions, guidelines, terms, and definitions that can be used during the entire lifecycle of electrical and electronic devices and systems. They are important for quality and risk management and let industry companies develop products with reliable performance. IEC standards are not mandatory for companies and are based on knowledge of experts from different countries. They are foundations for testing and certification processes. IEC international standards are frequently adopted by regions and countries that use them for creating their national or regional standards. For instance, almost 80% of electrical and electronic standards in Europe are IEC standards adaptations [11].

National or regional authorities in countries establish special rules and directives that are called regulations. Most commonly, compliance with regulations is obligatory for companies. Nevertheless, technical regulations can include references to international standards to avoid being overloaded with details and full descriptions. It allows laws and regulations stay up-to-date due to regular renewals of standards.

Another organization that develops different standards is the National Institute of Standards and Technology (NIST). It is part of the United States Department of Commerce and assigned to contribute towards innovation and competitiveness of the United States industry. NIST advances measurement science and technology, develops and promotes standards, and improves quality of life [2].

In the security area, the main goal of NIST is the creation of standards and technologies to protect the United States critical infrastructure. However, NIST works with the private sector and helps organizations to develop their own policies and guidelines. It has widely known security standards, such as NIST SP 800-53 Revision 5 that contains security and privacy controls for federal information systems and organizations. Additionally, NIST developed the internationally recognized NIST Cybersecurity Framework (CSF). This standard is guidance to better understand, manage and reduce cybersecurity risks. It helps to determine the most important activities for service operations and prioritize investments in cybersecurity of an organization. However, there is no possibility of obtaining a certificate of compliance with the CSF. Enterprises can use this framework to reduce security risks but cannot provide proof of its application to their customers.

The organizations described above are not the only organizations that develop and establish international standards. We have mentioned those organizations whose standards will be used for research later in this master's thesis.

## 2.2 Industrial cybersecurity standards

Information security has been initially aimed at achieving three objectives: confidentiality, integrity, and availability, which are usually referred to by the acronym CIA. In a typical information technology (IT) business system, security strategy may prioritize confidentiality and the access control measures that are necessary to achieve it. Integrity and availability might be the second and the third priorities respectively.

Governments and specialized institutions across the world develop security standards and guidelines to meet relevant security objectives and to protect different organizations, infrastructure, and people from malicious actions of attackers. Although a fully secure system is unachievable, these documents attempt to offer stakeholders measures for protecting their system from intentional harm and increasing its security and durability. Generally, security standards and guidelines propose approaches to identify the assets of the organization, to conduct their assessment and to evaluate relevant processes. Moreover, they describe possible countermeasures to improve the current state of security [21].

To address cybersecurity issues in an industrial environment, IEC published the IEC 62443 series of standards. It is intended for the different security actors that take part in the industrial system lifecycle and covers many aspects. At first, the International Society of Automation (ISA) developed the standard under the name ISA 99. ISA started to work on standards in 2002, published the first normative texts in 2004, and the first version of the ANSI/ISA standard was published in cooperation with The American National Standards Institute (ANSI) in 2009. After that, IEC adopted the standard and continued to develop other standards of this series in collaboration with ISA. Thus, a committee of experts with different industry experience and fields of activity began to work on the cybersecurity standards [25].

Although the IEC 62443 standards cover industrial IT systems, they are complementary to the ISO 27000 family that is mainly used for non-industrial IT systems. This series has been developed to be compatible with the ISO 27000 particularly regarding the security management system or the list of measures.

The IEC 62443 series is constantly evolving to be relevant to modern security challenges. For this reason, the standards are regularly reviewed and updated. At the moment, new parts of the series are in development, such as the IEC 62443-1-3 System security conformance metrics.

The structure of the IEC 62443 series is demonstrated in Figure 2.1. Final

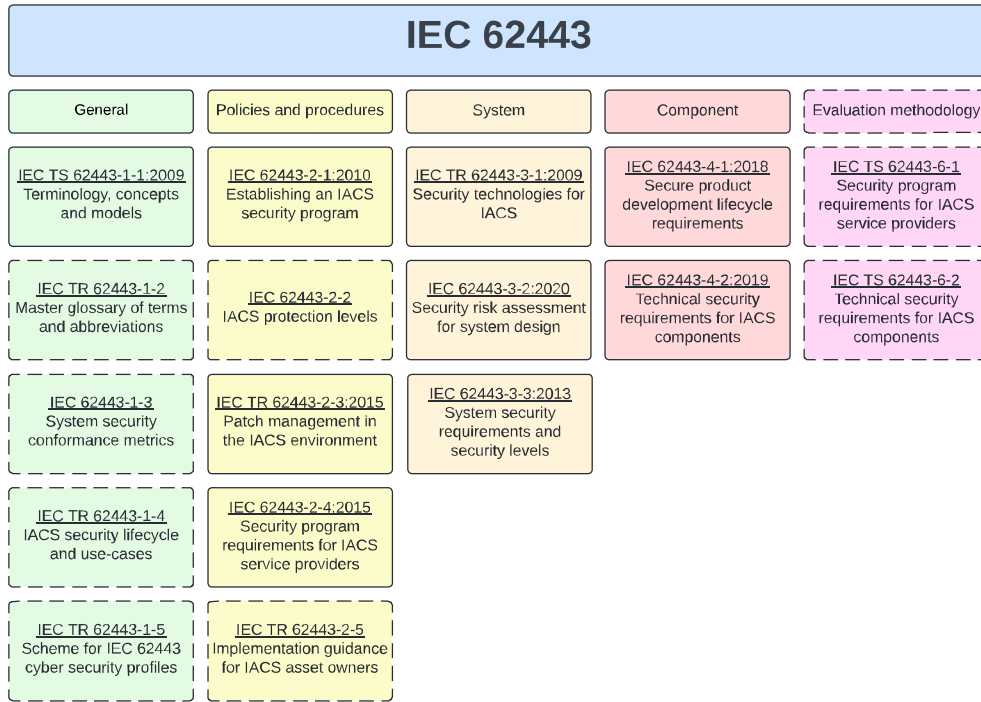


Figure 2.1: Standards of the IEC 62443 series

versions of the standards that are placed in the boxes with the dotted line are in development and have not been published as of this writing. The IEC 62443-4-2 standard provides their titles and affiliation to the whole IEC 62443 series [29]. In addition, information about the planned standards of the series and their development stage can also be found on the web page of the IEC technical committee 65 that develops the standards of the IEC 62443 series [4]. It is important to keep in mind that some of the standards that are under active development might be rejected during the development process and never be published.

The IEC 62443 series consists of different parts that belong to four groups. The first group includes the IEC 62443-1-1:2009 general standard that defines concepts and models used in the series and defines the basis for the series. It describes grouping assets into security zones. It also introduces foundational requirements (FRs) and a concept of security levels to address security for the zone.

The second group of standards relate to the organizational aspects described by policies and procedures. The IEC 62443-2-1:2010 standard defines

the requirements for defining and implementing an effective cybersecurity management system (CSMS). Usually, the standards about management systems describe what a management system should include, but they do not tell how to develop the management system. This standard provides the elements of CSMS and with guidance on developing it for IACS. The main categories of CSMS for IACS are risk analysis, addressing risk, monitoring and improving the management systems. In this standard, the consistency between practices for ISMS taken from the ISO 27001 and the practices to manage cybersecurity of IACS are emphasized.

The IEC 62334-2-3:2015 standard is about secure patch management for IACS. It defines a lifecycle of a software patch that has eleven steps including internal testing and creating a backup version of a system before applying the patch.

The IEC 62443-2-4:2015 document determines requirements for security capabilities for IACS. The target audience includes system integrators and product suppliers of IACS.

The third group of standards is intended for the system level of IACS. The IEC 62443-3-1:2009 standard is a technical report that specifies the application of different cybersecurity tools in an environment of IACS and provides the assessment of them. Since it is the technical report, the standard does not require specific cybersecurity technologies or special mitigation methods. The IEC 62443-3-1 only suggests using them and provides guidance and information that can be useful during development of cybersecurity policies or procedures for the IACS environment.

The IEC 62443-3-2:2020 describes an approach of security risk assessment for system design of IACS. The key concept of this standard is the application of security zones. The standard defines requirements for defining a system under consideration and portioning it into zones and conduits, assessing risk and establishing the target security level for each zone, and documenting these security requirements. This standard is the newest in the series.

The IEC 622443-3-3:2013 standard describes security requirements for IACS in the form of seven foundational requirements that are mentioned in the IEC 62443-1-1. It expands these requirements into a series of system requirements (SRs). Each SR has a baseline requirement and zero or more requirement enhancements (REs) to improve security. Moreover, it describes system security levels (SLs) for it. Security levels are the measure of confidence that a system, component or security zone under consideration functions properly and does not contain security flaws. They are applied in this standard and in the IEC 62443-4-2. The classification of them in terms of the capabilities of the threat actor is the following:

- SL 0. There is no need for specific requirements for establishing security;
- SL 1. Protection is implemented against coincidental or casual violation. It means that there is no system attacker. Low-skilled attackers, also known as *script kiddies*, who can only use scripts made by others without understanding of their work, can be considered in this category. However, there might be somebody who can do something unintentionally wrong;
- SL 2. Protection is implemented against intentional violation by malicious actor with low resources and generic skills. For example, they can be an IACS system attacker who found open-source tools for simple cyberattacks, took them, spent a few days and attacked the system for entertainment. SL 2 also includes the skilled attacker that does not specifically target IACS;
- SL 3. Protection is implemented against more serious intentional violations. In this case, the threat actor is motivated to attack IACS. They have proficient skills and use moderate resources. The attacker can be a real criminal who receives money for attacking the system;
- SL 4. Protection is implemented against the most severe intentional violation. Attackers have extensive resources and advanced skills. They are the best criminals on the market and ready to attack the system with any cost. They can work for a government and participate in a cyber war.

Moreover, there are three types of SLs:

- A target security level (SL-T). It is the desired level of security for the correct operation of a system. Its determination depends on the documented results of the risk assessment.
- A capability security level (SL-C). This level of security is achieved when IACS or their components are properly installed and configured. At this level, the IACS and its components are capable of meeting the SL-T without compensating countermeasures. These countermeasures are used instead of or in addition to existing security capabilities to fulfil one or more security requirements.
- An achieved level (SL-A). It is the actual level of security in the automation solution that is measured after coming into operation.

The main purpose of this standard is to define security capabilities at the system level. It takes into account risk assessment that identifies essential

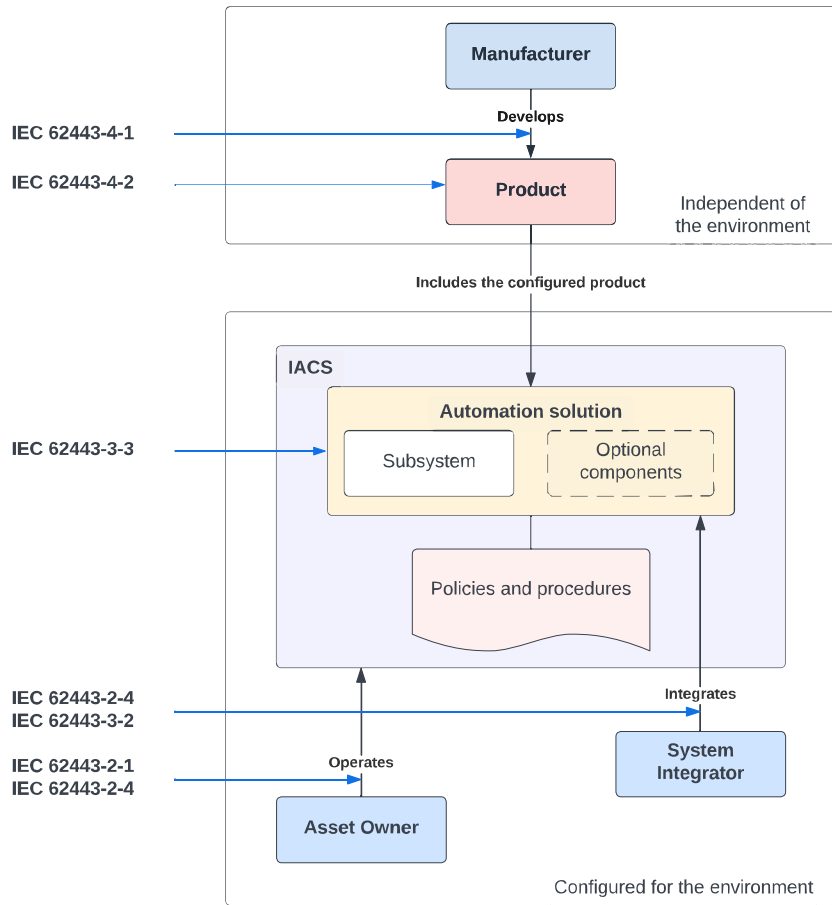


Figure 2.2: General scope of product lifecycle in the IEC 62443 series

services and functions for operations. The key concept of the standard is that security must not endanger availability of the system.

IEC 62443-4-1:2018 defines the requirements for the secure development and continued security of devices, called together the secure development lifecycle (SDL)[28].

The general scope of the product lifecycle that is considered in the IEC 62443 series of standards is illustrated in Figure 2.2. The box with the dotted line in an automation solution indicates optional components that can be another subsystem or hardware and software component.

The manufacturer or the product supplier develops the product according to the IEC 62443-4-1 standard and fulfills its security requirements. The

product can be a component, such as a software application, embedded device, host device or network device, and it meets the requirements of the IEC 62443-4-2 standard. It is possible that the product can be a system or subsystem that includes different components, which work together. The development process is independent of the intended environment.

After development, a system integrator integrates a configured instance of the product into the automation solution. This integration is conducted through processes in accordance with the IEC 62443-2-4 and IEC 62443-3-2 standards. Then the automation solution is installed in the IACS with the consideration of security measures from the IEC 62443-3-3 standard. These measures are implemented and supported in the automation solution as product features or compensating mechanisms. The automation solution can have more than one product. For example, there can be a group of products that is hierarchically brought together. This means that there is an identified dependence of the functioning of one component on the existence of another. After the installation, an asset owner maintains and operates the developed product that has become a part of the IACS according to the IEC 62443-2-1 and IEC 62443-2-4 standards.

The manufacturer or product supplier can act as the system integrator if it not only develops the product but also integrates it into the automation solution. This standard is intended for the product development processes and does not address the automation solution or IACS and their architecture, installation, configuration, and maintenance.

The standard also describes four maturity levels. The maturity level shows the completeness of the requirements fulfillment by the manufacturer. The levels are used to assess the maturity of the implemented security practices during product development. They also help to understand the readiness of the organization, its processes, and procedures to be compliant with the standards requirements. The organization can select the desired maturity level for different sets of requirements that better meet their needs in each case.

However, in order to obtain a certificate of compliance with a certain maturity level, all its requirements must be fulfilled. It means that the manufacturer must have the same maturity level or above it for all the requirements.

The maturity levels for the SDL defined in the IEC 62443-4-1:

- ML 1, initial. Development processes are not planned and not documented;
- ML 2, managed. The manufacturer has documented development processes and is ready to implement them;

- ML 3, defined (practiced). The development processes are practiced according to the documentation, and they are repetitive;
- ML 4, improving. The manufacturer controls the effectiveness and performance of the products and processes. The development processes are continuously improved based on the specific metrics.

The IEC 62443-4-2 standard is aligned with the IEC 62443-3-3 and defines the technical security requirements for a product. In other words, the requirements for the components or devices are obtained from SRs and REs that are described in the standard of the third group. All requirements are grouped by their belonging to foundational requirements. Some of them require stricter security enhancement at the higher security levels. The scope of the standard is one device or component, it does not assess the security of other components of the system. There are four types of components that are used in the standard and several common constraints that can be considered during requirements implementation, such as support of essential functions and compensating countermeasures. For compliance with this standard, the component should comply with hardware requirements and support the implementation of software requirements at the hardware level.

## Chapter 3

# Security standards certification

According to Computer Security Resource Center (CSRC), the certification process is a comprehensive assessment of the management, operational, and technical security controls implemented in an information system, which is done in support of security accreditation, to determine to what extent the controls are implemented correctly, functioning as intended, and give the desired outcome in terms of compliance with the security requirements for the system [44].

The certification process includes various concepts, processes, rules and participants. In this chapter, the cybersecurity standard compliance and certification processes for the IEC 62443 series of standard are analyzed.

### 3.1 Standards compliance

Compliance means fulfillment of all applicable requirements of a standard or another published set of requirements.

In terms of ISO and IEC standards, compliance relates to conformity assessment. Conformity assessment (CA) means any activity of demonstration of fulfillment of the specified requirements by an object of CA, such as a product, service, system, process or people. It includes activities, such as testing, inspection, validation, verification, certification, and accreditation [36]. CA helps to determine that a standard or specification was used in the design, development, installation, and maintenance of the product. It must be conducted according to established rules to ensure consistent results and use a standardized approach. For these purposes, the IEC and ISO have published a series of international standards that specifies how the CA should be done.

The standards organizations distinguish three types of CA. Their descrip-

Type of CA	Description	Level of trustworthiness
First-party	A self-declaration type of CA. The manufacturer declares that a product complies with standards and provides supplier's declaration of conformity (SDoC). This type is usually used for products with low risk. It is the least costly form of CA because its trustworthiness relies on the credibility of the manufacturer.	Low
Second-party	CA is performed by an interested party, typically the customer, that is concerned about the product properties. Customers may conduct CA for products that they intend to purchase. The purpose is to check the first-party CA.	Medium
Third-party	CA is performed by an independent party and called certification. This is the most expensive type of CA for the manufacturer and carried out by for-profit organizations. It can be required by legislation or be applied to improve market positions.	High

Table 3.1: Types of conformity assessment

tions are presented in Table 3.1.

The rules and procedures that describe what can be the object of CA, identify needs or expectations and provide the methodology for performing CA form a conformity assessment scheme. The scheme can be operated at an international, national or industry sector level and is managed by conformity assessment systems which are set of rules and procedures for the management. A certification is a CA scheme performed by third-party bodies.

All CA schemes have an owner whose main responsibilities are the development and maintenance of them and CA systems. The owner does not necessarily perform CA.

## 3.2 Limitations of the standards compliance

The process of compliance with cybersecurity standards requires a considerable amount of time and effort and can incur a high cost for the manufacturer.

Even if a company can afford this process and certification of compliance, there may be no clear understanding what it should exactly do with the information from the standards and how to choose the suitable standards.

Another question that may arise is how to integrate them efficiently into the business processes of the company. It can be insufficient to address this issue with only expert skills because it requires monetary and time resources for evaluating and monitoring the effectiveness of an implemented approach. The integration and evaluations actions need more investments to standards compliance process and good understanding of the desired outcome.

Additionally, there are no generally accepted metrics that can be used during the analysis of theoretically secure systems and their ability to work. Consequently, the compliance with standards can give a false sense of security and be a significant risk for the company [51].

Regulatory authorities may make compliance with a standard mandatory, even though in most cases standards are not regulations and compliance with them is required only by customers. Nonetheless, there is no consensus on the benefits of obligatory regulation and how it will improve security. For example, when security should comply with regulations, companies look for methods to avoid them. The North American Electric Reliability Corporation demonstrated that some companies removed black start capability to restart components of the power system to recover from a blackout just to escape paying for compliance [12]. Hence, overly strict, or difficult-to-manage regulations may force companies to bypass them and may lead to serious consequences that will create new vulnerabilities.

## 3.3 Standards certification schemes

There are two most common certification schemes for IEC 62443 standards: IECEE Industrial Cyber Security Programme and ISASecure certification scheme. However, some certification companies provide their own certification programs based on IEC 62443 series of standards.

### 3.3.1 IECEE

The IEC manages four IEC CA Systems, whose members conduct third-party assessment of standards compliance according to the globally standardized

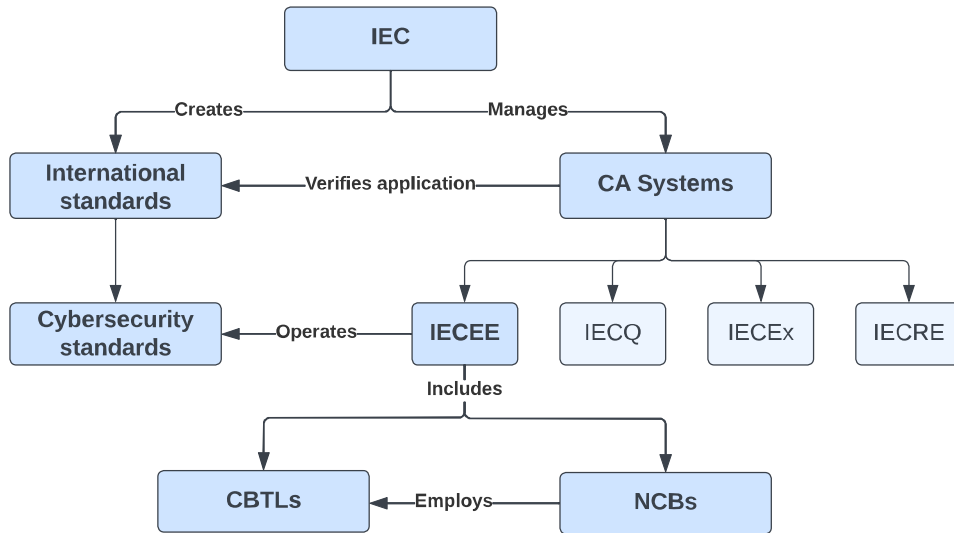


Figure 3.1: IEC standards and CA

approach of CA. IECEE (IEC System of Conformity Assessment Schemes for Electrotechnical Equipment and Components) verifies the proper application of cybersecurity standards through the IECEE Industrial Cyber Security Programme. It includes the National Certification Bodies (NCBs) that conduct assessment processes and issues certificates, and CB Testing Laboratories (CBTLs). NCBs may employ testing laboratories for the certification processes. However, customers can apply only for testing services to CBTLs. In this case the laboratory can issue a test certificate but not a compliance certificate. The connection between IEC standards and CA is demonstrated in Figure 3.1.

IECEE operates the following IEC cybersecurity standards: IEC 62443-2-4, IEC 62443-3-3, IEC 62443-4-1, IEC 62443-4-2.

### 3.3.2 ISASecure

As mentioned before, the original creator of IEC 62443 series of standards is ISA. ISA is a professional engineering society focused on automation engineering. It develops and publishes standards, manages certification and compliance, provides training courses, and organises conferences. This society submits their standards to IEC to make them widely recognized. In the USA, IEC 62443 series is best known under the name ISA/IEC 62443. It is

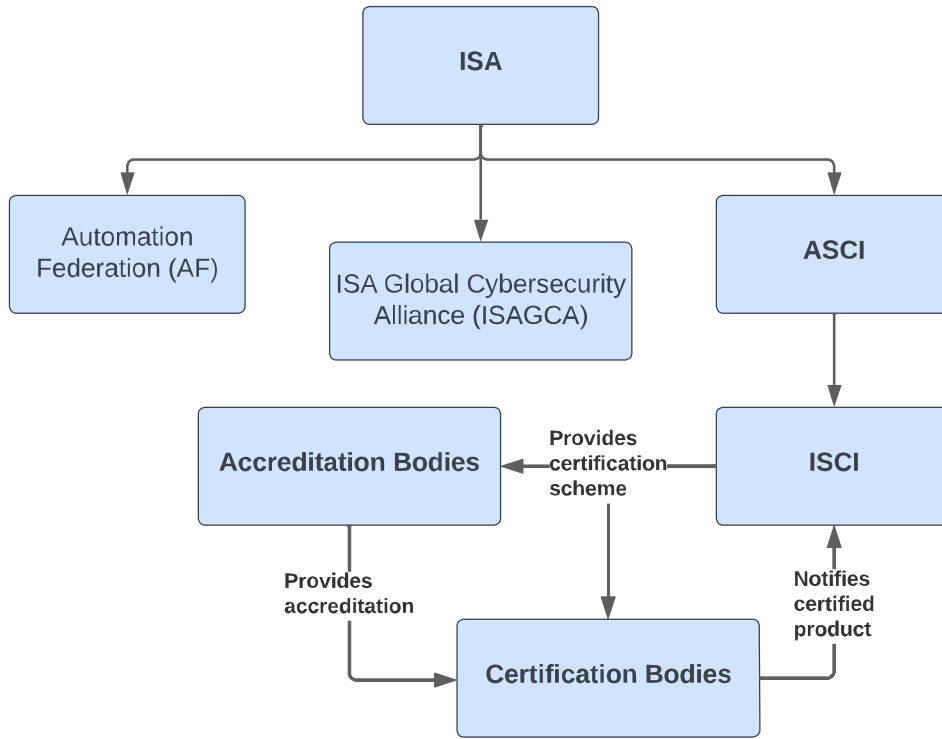


Figure 3.2: ISA and the certification scheme

the most referenced standard in the NIST Cybersecurity Framework.

ISA has the Automation Standards Compliance Institute (ASCI). ASCI includes the ISA Security Compliance Institute (ISCI) that is the developer and owner of the ISASecure certification scheme. The organization structure of ISA that is involved in the certification process is presented in Figure 3.2.

It is important to note that ISCI is a scheme owner and does not operate their own certification body. ISCI has the accreditation requirements and selects accreditation bodies. They can accredit certification bodies to conduct the certification process in accordance with ISASecure. If the CA of the SDL shows meeting all applicable security requirements of ISA/IEC 62443, the certification body issues an ISASecure certificate.

For example, *exida* is the very first certification body under the ISASecure program. This certification company conducts certification on behalf of ISASecure globally. Furthermore, they have their own assessment security programs that they use to certify products or processes in accordance with

IEC 62443 and their additional requirements.

Current ISASecure Certifications [9]:

- Security Development Lifecycle Assurance (SDLA). This scheme includes a process assessment of the SDL practices from ISA/IEC-62443-4-1. It specifies more details and defines additional requirements compared to IEC 62443-4-1 scheme. During the certification process the certification body reviews evidence of execution of the documented processes. If there is insufficient evidence of the fulfillment of the documented requirements, but the readiness to meet them is demonstrated, then the auditor may issue an initial certificate which is valid for 12 months. The final ISASecure SDLA certificate is valid for three years and can be extended after a recertification audit. ISASecure certification scheme does not assess the maturity levels of organizations.
- Component Security Assurance (CSA). It is based on ISA/IEC-62443-4-2 standard. The scheme assesses the SL-C of components. It verifies SDLA certificate, applicability of SDL requirements to the component, and evidence of implementation of that. The certification also examines meeting the requirements of the standard for the specified security level and performs a scanning of component's network interfaces using ISASecure specific policy for the vulnerability assessment tool.
- System Security Assurance (SSA). This certification assesses the SL-C of the IACS system and is based on ISA/IEC-62443-3-3 standard. It also includes checking for the SDLA certificate and evidence of following the SDL process for the system, an assessment of security zones and their security levels in accordance with the standard, and a vulnerability testing of all network interfaces with ISASecure policy. The certificate will demonstrate the SL-C for each security zone.

The SDLA certificate is mandatory for obtaining other certificates, such as SSA and CSA, but it can be used for multiple products.

ISASecure specifications for the certifications schemes are publicly available. Everyone can get acquainted with the certification criteria and their usage for certification of SDL or products.

### 3.4 Benefits of certification

The certification process can be challenging, but as a result, the company will benefit from owning a certificate of compliance. For instance, the certificate of compliance with the IEC 62443-4-1 will ensure customers that the

organization takes security into account at each stage of the product development. In addition to the security department, everyone who is involved in the development is responsible for security of the product. The certificate shows that the organization is able to deal with possible security problems with the product and its maintenance.

In general, benefits of a certification for a company are:

- The result of a certification process is evidence for customers and for original equipment manufacturers that security aspects are a priority for the company.
- To issue a compliance certificate to a company, an independent entity reviews the product, system or development and production processes. After that, the company can use the results of the review to improve its processes and product quality.
- The certificate of compliance with security standards reduces the risk that brand image of the company will be damaged in the future.
- The assurance of security of a product, system or process is increased by a certification.
- It allows customers and consumers to compare security functionalities of similar products from different producers. For example, if companies have identical security standard compliance certificates, customers can make a comparison between products knowing that they are secure according to a single standard.

### 3.5 IEC 62443-4-1 certification

As demonstrated earlier, the IEC 62443-4-1 is the fundamental standard for obtaining certificates of compliance with the IEC 62443 series. It is crucial to organization's project to have SDL because without it a developed solution cannot be considered secure. That is why it is important for organizations that want to receive a certificate of compliance with the IEC 62443-3-3 and IEC 62443-4-2 to understand how the certification process for security management systems including SDL works.

The certification processes will be described using the processes of TÜV Rheinland Group. TÜV Rheinland is one of the global leading service certification provider that operates since 1872. The organization acts as an independent third party to assess and certify products and processes inside companies. It also certifies quality and security management systems based on international standards. TÜV Rheinland has a global network of approved

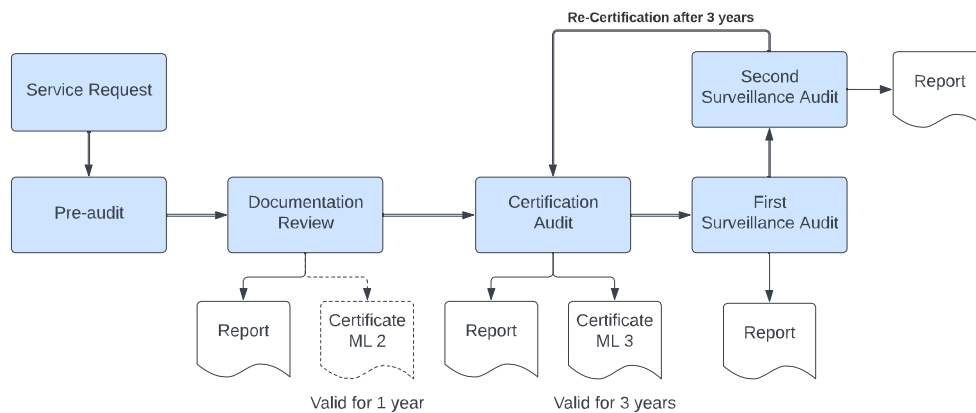


Figure 3.3: General overview of the IEC 62443-4-1 certification process

laboratories and testing centres. Qualified experts work for this certification provider to evaluate and contribute to improvement of the safe and secure product development [10].

General overview of TÜV Rheinland certification process for IEC 62443-4-1 standard is demonstrated in Figure 3.3. The process is based on the ISO/IEC 17021 [5].

The certification process starts when a company that has decided to receive a certificate of compliance makes a service request to NCBs. It includes information about the company, a name of the standard it wants to be certified with, and the project that will be assessed. After that the company with NCBs makes arrangements to conduct a pre-audit, which is the first stage of the certification process.

The pre-audit commonly takes place at an auditee location. According to TÜV Rheinland, it can take two or three days for two auditors to conduct the pre-audit for the company. During this stage evaluation of company's processes occurs to identify possible deviations from standards requirements. The auditor checks that all responsible roles and their expertise are identified. At this stage the company should have defined processes that are able to fulfill the requirements. Also, the auditor inspects the company's location, for example, an office-building or a testing laboratory, and evaluates site-specific conditions that may have an impact on the project and meeting requirements. After the pre-audit the company receives a list of identified gaps that the company should eliminate before the next stage of the certification process.

The documentation review comes after the pre-audit. An important dif-

ference between them is that the auditor can review company's documentation online at auditor's office. It means that the company, for instance, can provide the access to their documents on cloud via shared link or send them through email to the auditor. One auditor is able to evaluate all documented processes and their versions. They check organization charts, procedures, work instructions, templates, and forms for writing documentation. If the auditor decides that all documented processes are well-defined and the organization has provided all the required documentation, they issue a certificate of maturity level 2 with an audit report after reviewing the documented process. This certificate is optional and valid for one year.

The main stage of the certification process is the initial certification audit that as pre-audit takes place at an auditee location. The organization should show that the documented processes have been improved, all gaps defined during documentation review have been eliminated and at least one project has been completed according to the reviewed documentation. Moreover, the organization should show evidence that all requirements from the standard have been followed for the project during the whole product development lifecycle. If the provided evidence proves that all processes documented according to the standard are functioning, the auditor will assign a certificate of maturity level 3 and give a report of the conducted audit. The certificate is valid for three years. With the consent of the company, the certificate can be uploaded to an online auditor's database accessible to any user. This allows potential customers and consumers to verify the authenticity of the issued certificate.

The next stage of the certification process is an annual surveillance audit that takes place at the auditee location. One auditor checks that the organization uses the created documentation and evaluates an application of the defined processes in daily operations. The auditor can selectively check compliance with the requirements of the standard, for example, select only a part of the required practices without warning about their choice.

It is possible to say that the certification process is a cyclical procedure repeated every three years. The last stage of the cycle is the re-certification audit. The main idea of it is to confirm that the effectiveness of the complete management processes. The auditor reviews applicable processes and measures that have been changed. They issue a new certificate of maturity level 3 if the provided evidence confirms the application of documented processes. Furthermore, the auditor evaluates improvements that have been made in three years and depending on their significance, they can issue a certificate of maturity level 4.

There are no strict deadlines in the certification procedure for conducting the next audit after receiving a certificate of any maturity level. For example,

the certificate of maturity level 2 is valid for one year. However, this does not mean that the company is obliged to obtain a maturity level 3 certificate within one year. The company can conduct the certification audit after two years and provide an expired certificate of maturity level 2. This does not affect the maturity level 3 certificate.

### **3.6 IEC 62443-4-2 certification**

Detailed information on the certification procedure for verification of compliance with the IEC 62443-4-2 standard requirements is not publicly accessible.

However, there are situations when the manufacturer or an independent researcher wants to understand how the components are validated during the IEC 62443-4-2 certification. In this case, it is possible to get acquainted with the ISASecure documents that are freely available on the website for registered users [3]. The documents have a description of validation activities that must be performed for common component security constraints and each component requirement from IEC 62443-4-2 during the evaluation audit. Moreover, they contain the identical description of requirements from IEC 62443-4-2 and the same additional information on each requirement from sub clause "Rationale and supplemental guidance" in IEC 62443-4-2 [18]. It is worth mentioning that access to the IEC standards is not free, unlike these documents. The registration on the website does not require membership in the organization.

Additionally, these documents contain ISASecure certification requirements. According to them, the manufacturer shall specify the maximum SL-C for which they would like to receive a certificate when they apply for the certification of a component.

## Chapter 4

# Safety and security standards for lifts

In the modern world, security and safety are inextricably linked. It is impossible to ensure complete safety of products for transporting people or goods, such as lift, without taking into account potential security aspects.

In this chapter we will review the most important standards for safety and security that are applicable to a lift domain and will be needed for the case study in Chapter 5. Additionally, we will analyse the relationship between security and safety. Furthermore, we will survey a new cybersecurity standard for lifts that includes safety and security aspects.

### 4.1 Safety standards

The most influential standardization organizations for the lift industry are CEN and ISO [13]. CEN stands for the European Committee for Standardization. This association coordinates the work of 34 National Standardization Bodies in the developing of European Standards (EN) and other types of technical documents. It covers different fields and sectors, such as construction, defence and security, health and safety, machinery, transport [1].

A published European Standard must become the national standard in all CEN member countries. These countries are also obliged to withdraw any conflicting national standards.

The Vienna Agreement is a treaty for technical cooperation between CEN and ISO. It was created to prevent duplication of standards. The agreement allows technical committees to develop standards that can be recognized across the world. Therefore, new standards projects are planned by CEN and ISO together. Moreover, ISO standards meet European legislative

requirements and non-European organizations fulfil international and European requirements concurrently. It is planned that ISO standards will replace European standards in the future. This can help to reduce worldwide trade barriers.

#### 4.1.1 EN 81 series

CEN has developed the EN 81 series of standards for safety of the construction and installation of lifts. At the moment the series does not cover the process of mounting and erection of lifts. The word "installation" implies a piece of equipment, machinery or a complete system that has been installed ready for use [16].

In 2014 the EN 81-20 and EN 81-50 standards for the design and manufacturing of lifts were published to provide considerable accessibility and safety benefits to passengers and installers. They replaced EN 81-1 and EN 81-2 standards that were introduced in 1998.

EN 81-20:2014 contained safety requirements for the construction and installation of lifts, while EN 81-50:2014 specified the testing and inspection requirements for certain components of the lift.

All lifts that have been produced after 31 August 2017 must comply with the requirements of these standards.

CEN made a revision of EN 81-20 and EN 81-50 standards and published them in 2020. The new versions of them supersede the previous ones, although they do not contain technical changes. EN 81-20:2020 and EN 81-50:2020 have dated normative references. These standards cite editions of the referenced documents that were published in a specific year. If a normative reference does not have a date, the standards cite the latest version of the document. Furthermore, they have a new informative annex about the relationship between the standard and the requirements of Directive 2014/33/EU [22, 24].

CEN has been reviewed other standards of the EN 81 series. For example, a revision of EN 81-28 was published in June 2022. The organization also continues developing new versions of documents related to lifts safety, such as EN 81-76 that is about the evacuation of persons with disabilities using lifts. This standard is planned to be published in 2022.

#### 4.1.2 ISO 12100

ISO 12100 standard provides guidance for the development of machinery, methodology to design safe to use machines, and principles of the assessment and reduction of risks associated with machinery. It also describes procedures

for identifying and eliminating hazards and for working with risks during the machine lifecycle. Moreover, the standard provides a strategy for the preparation of safety standards [32].

ISO 12100 forms the basis for standards which has the structure:

- Type-A standards that are basic safety standards. They provide basic concepts, principals for design and general aspects for machinery. ISO 12100 is a type-A standard.
- Type-B standards or generic safety standards consider one safety aspect or one type of safeguard that can be used across a wide range of machinery. Type-B1 standards are about particular safety aspects. For instance, safety distances or noise. Type-B2 standards cover protective devices, such as interlocking devices or guards.
- Type-C standards are machine safety standards that deal with detailed safety requirements for a particular machine, for example a lift, or group of machines. If a type-C standards deviates from one or more technical provisions described in a type-A standard or type-B standard, the type-C standard has priority.

The purpose of the structure of type-A, type-B and type-C standards is to give one method for manufacturers to develop machinery that can be used to attain tolerable risk by adequate risk reduction.

According to the ISO 12100 standard, the risk is associated with a hazardous situation and depends on a severity of harm that can result from the considered hazard and the probability of occurrence of the harm.

ISO/TR 22100-1 provides explanations of the general principles of ISO 12100. This technical report helps the manufacturer of machinery and its components to understand the different types of ISO machinery safety standards. It also elaborates how this type-A standard is used for practical cases in combination with type-B and type-C machinery safety standards [38].

ISO 12100 was published in 2010. At that time, cybersecurity was not given as much attention as it is nowadays. During the time after the publication of the standard, it became clear that cybersecurity attacks are becoming a real threat to the safety of machinery. Remote interactions with machinery provide benefits of a simplified operating process but also increases attack surface.

To address the situations when cybersecurity attacks can affect safety of machinery, ISO/TR 22100-4 was published in 2018. This technical report provides guidance on relations between security aspects and safety of machinery. It gives basic information on identification and addressing cyber threats which can affect safety [39].

The document compares the principle objectives and conditions of safety of machinery and cybersecurity. For instance, the main goal of safety of machinery is to prevent accidents, health harm and injuries. However, as mentioned earlier, CIA forms the main objective of cybersecurity. Moreover, cybersecurity field is developing very fast together with methods of cyberattacks implementation. Safety of machinery is a more static field where it is possible to foresee a misuse of a machine.

The elements of risk also change in cybersecurity. The risk is related to the considered threat and depends on possible negative impact of the threat and the probability of that impact when this threat can exploit existing vulnerabilities.

The relationship between safety of machinery and cybersecurity according to ISO/TR 22100-4 is presented in Figure 4.1. The figure shows that cybersecurity incidents can lead to failures of the machine and cause serious damage to human safety.

### 4.1.3 ISO 8100

The ISO 8100 family of standards is intended as a replacement for EN and ISO standards related to lifts. This is done to create the series of international standards specific to the lift domain and to improve coherence between them.

ISO 8100-1 standard contains the content of EN 81-20:2014 and some minor editorial changes. It is a type C standard that defines safety rules for passenger and goods passenger lifts [33].

The standard defines the safety integrity level (SIL) that is a separate level for specifying the safety integrity requirements of the safety functions allocated to the programmable electronic system in safety related applications for lifts (PESSRAL). This system is designed to control, protect or monitor lift functions. It uses one or more programmable electronic devices, such as input devices, communication paths, output devices. The standard provides rules for PESSRAL design and the list of the electric safety devices with the minimum SIL for each of them. SIL 3 has the highest level of safety integrity and SIL 1 has the lowest.

The minimum design requirements for relevant SIL for PESSRAL are presented in ISO 8100-2 standard. This standard replaces EN 81-50:2014 and contains the same content with some updates. The standard specify design rules, calculations, examinations and tests of lifts components. Additionally, the standard provides with specific measures for each SIL [34].

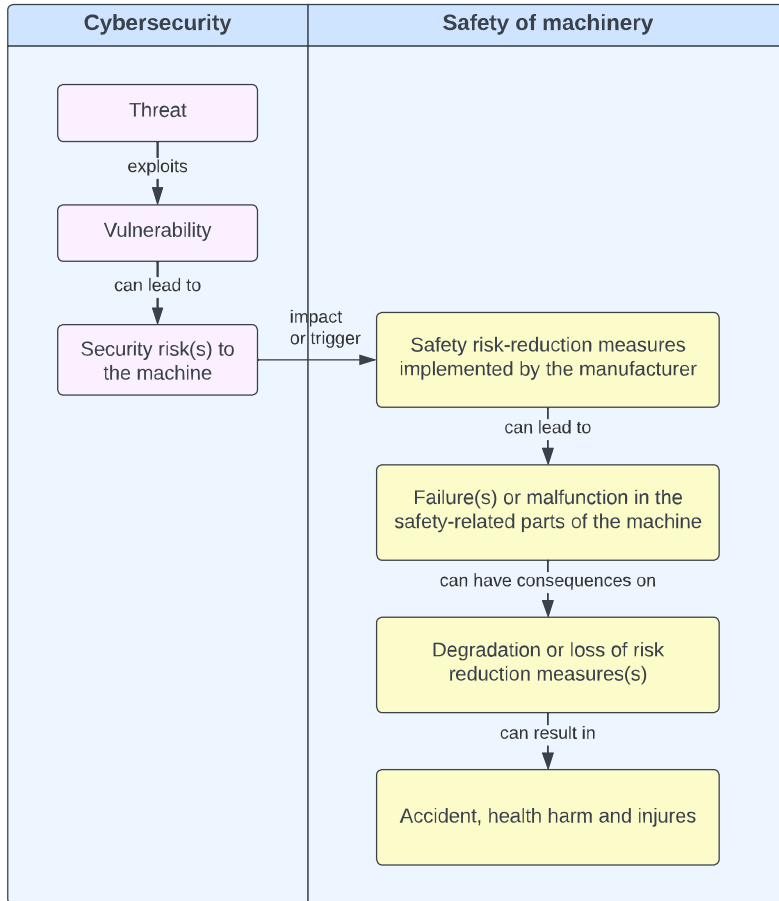


Figure 4.1: Relation between safety and security

## 4.2 Security standards

Worldwide product development can be under intense short-term pressure for maximizing efficiency and minimizing cost. In addition, quality is another challenge for the development that is based on safety and security. Cybersecurity is obligatory to guarantee trusted connectivity of distributed services. It should be especially considered in the development of embedded systems. They could be a target for a cyberattack by hackers since they perform critical functions for products [47].

When a disturbance occurs in traditional systems connected via the Internet, problems arise in the digital world which indirectly affect the physical

world. For example, hijacking of a user account could lead to disclosure of confidential information or to financial losses. Incidents in the IoT world may have direct physical impact on the real world. For instance, a hacker can unlock a lift door, alter settings of critical systems, or break a vehicle and kill its passengers. For these reasons, security issues in the IoT environment have significant impact on safety and security of the physical product [52]. Thus, security of the developed product should have high priority starting from the early stages of its development. To improve this process, the fourth part of IEC 62443 cybersecurity standard series has been developed.

In Chapter 2 we provided general information about each standard of IEC 62443 series. Nonetheless, in the following sections, we will focus in more detail on the standards that are important for the lift domain. These standards are also used during the case study.

#### 4.2.1 IEC 62443-4-1

The IEC 62443-4-1:2018 includes the requirements for managing development security, implementing security from threat model to release, and maintaining products in a secure manner. These requirements are for developers of any automation and control systems and components where security is essential. This standard presents eight practice requirements for SDL:

1. Security Management (SM). The fundamental practice that is a consistent process and covers essential activities for SDL, such as planning and documentation. During this practice responsible roles, their responsibilities, security requirements for the development environment and for external components should be identified.
2. Specification of security requirements (SR). Includes threat modeling, after which security requirements are specified. It is a direct part of the development process that evaluates system's properties, identifies threats using threat modelling and security controls that should be implemented. In case of lift's embedded systems these security controls and requirements should target security levels from IEC 62443-4-2 standard. All of them should be reviewed before applying to the development process.
3. Secure by design (SD). This development practice contributes to a defence in depth approach. Defence in depth aims to defend the system against any cyberattack using different independent methods. It has several layers of security protection and is ready to maintain a high level of defence even if one layer is defeated. A vulnerability from one layer can be successfully mitigated by activities of other layers. However, all

layers are autonomous and do not have the same functionalities and failure modes. That is why the secure design of the system is an important practice and should have multiple levels of defence. The good design of the system reduces the attack surface and allows the reuse of components in a secure way.

4. Secure implementation (SI). The practice ensures that the system defined in previous practices has been developed securely and has all essential security capabilities.
5. Security verification and validation testing (SVV). Testing activities verify the design and that the security requirements have been implemented correctly. This practice tests security capabilities and checks treat mitigation and that there are no other security problems.
6. Security defect management (DM). The post release practice that is part of SDL that is responsible for maintenance process. It is about how to handle security-related issues and vulnerabilities. Security researchers can start to investigate the system at this stage of SDL.
7. Security update management (SUM). Another post release practice that includes verification of updates and their compatibility. It also covers requirements for description of updates and their delivery to the system.
8. Security guidelines (SG). It covers documentation process that is required for continuous security operations of the system after release. All documentation should specify security features and their configurations, security assumptions that are related to installation and maintenance processes of the system and all other activities of SDL that have impacted the system's operations. During this practice the development team produces documentation that is intended for an end user, such as guidelines for secure configuration and maintenance of the product.

The purpose of defined SDL is to develop and maintain secure products using described above practices. SDL according to IEC 62443-4-1 is demonstrated in Figure 4.2.

There is no need to create new processes, since the requirements of the standards can be applied not only to new processes for developing and maintaining products, but also to existing ones. Also, they can be applied to hardware, software, firmware of new or already developed products. For example, the SG practice can be used as guidance on how to create comprehensive user documentation for a product that has not been developed in accordance with IEC 62443-4-1.

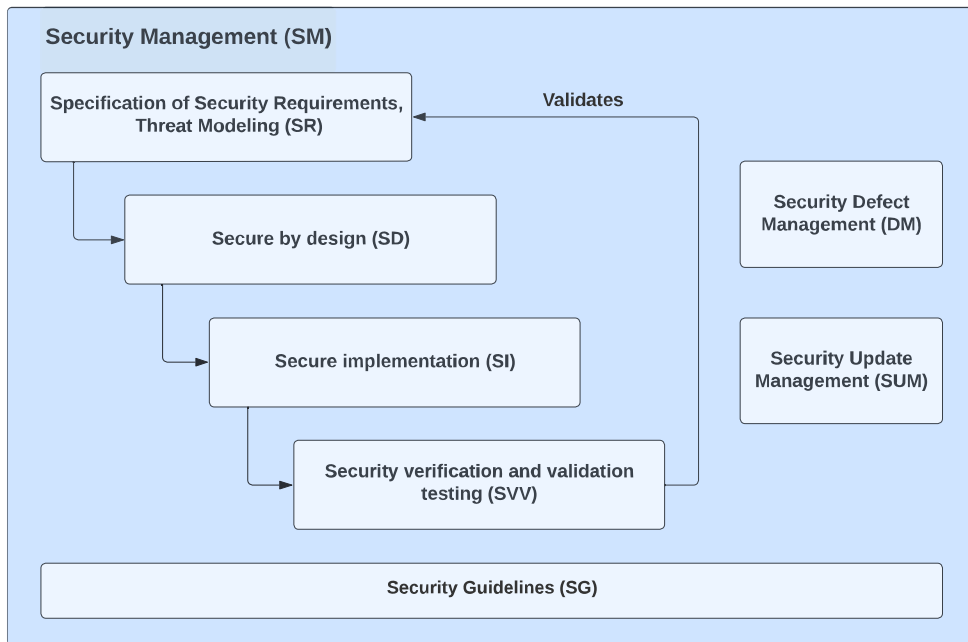


Figure 4.2: Security development lifecycle

The standard is intended for developers and maintainers of the product and do not cover the integrator or an asset owner of the product.

#### 4.2.2 IEC 62443-4-2

IEC 62443-4-2 is the second standard of the fourth group that is applied to IACS at a component level. It defines cybersecurity technical requirements for components, such as host devices, embedded devices, software applications and network devices. The requirements can be applicable to all mentioned types of components or to be specific to some of them.

According to the standard, the product may have characteristics of one or more of a component type. It may combine different features of an embedded, host, network device or software application and cannot be defined only as a one type of device. In this case the product should meet all requirements provided for each applicable component type. The standard provides definitions of the components and their examples with typical attributes. However, there is no guidance on how to determine what component or components the product belongs to.

The goal of the standard is to describe security capabilities that help mitigate threats for a certain SL without using compensating countermeasures grouped by seven foundational requirements. These groups are:

1. Identification and authentication control. A capability of a component to identify and authenticate people, software processes and devices with granting them access to the system. It covers passwords, keys, their quality and storage. This requirement is very important for a lift controller because a maintenance person should be able to interact with it.
2. Use control. Provision of the assigned privileges of authenticated users to perform actions with the system. Monitoring users' activity and the use of the privileges. This requirement covers wireless, portable and mobile devices use control. Embedded component's test and diagnostic interfaces for developers should be protected.
3. System integrity. Protection of the component's integrity against illegitimate manipulation including malicious code and physical tamper. It covers provisioning roots of trust and correct error handling. Software of embedded components should be verified and protected against execution malicious code.
4. Data confidentiality. The information transferred through communication channels remains confidential. Data in storage repositories is protected against disclosure. It covers use of cryptography and information persistence.
5. Restricted data flow. The system is segmented into zones and conduits to avoid the unnecessary flows of information. General purpose communication through industrial networks should not be allowed.
6. Timely response to events. In case of an incident or any other security violations the system is able to respond to it, report and take mitigation actions during a defined time period. This requirement covers audit logs accessibility and continuous monitoring.
7. Resource availability. The component is protected against degradation or denial of services. There are system backups, recovery management and a principle of least functionality.

The standard also defines several common constraints that should be considered during components implementation:

- Support of essential functions. Security controls and methods should not interfere with essential operations of the component.

- Compensating countermeasures. Some of the component requirements might be fulfilled by external factors, for example, physical security. Compensating countermeasures can help to reach a high level of security when it is already difficult to fulfill the requirements of the standard or there is a ready product that was developed before compliance with the standard. It can be useful when there are some functionalities dictated by other regulations or there is a need to secure legacy functionalities or protocols. For instance, insecure protocols can be secured by countermeasures, such as traffic segregation or physical isolation of hardware.
- Following the principle of least privilege when it is appropriate. The granularity of permissions and flexible mapping of them to identified roles should be provided. The information of that should be documented.
- Software development process. All components should be developed in accordance with IEC 62443-4-1 standard. The SDL practices should be used.

The company cannot be certified in accordance with the IEC 62443-4-2 standard if its development lifecycle does not comply with the requirements of IEC 62443-4-1. However, it does not mean that without a certificate of maturity level 3 for SDL the company cannot receive a certificate of compliance with IEC 62443-4-2. In this case, the company must provide all evidence that the product has been fully developed in accordance with the requirements of IEC 62443-4-1. Nevertheless, if it is necessary to certify several products, then the company has to provide all evidence of compliance with each IEC 62443-4-1 requirement for each product. The possession of the certificate of maturity level 3 for SDL allows the company not to provide evidence for compliance with some practices requirements.

### 4.3 ISO 8102-20

ISO 8102-20 is a new cybersecurity standard for lifts, escalators and moving walks. It was published in August 2022 as a response to the lift and escalator industry request to set a baseline for cybersecurity in the domain.

The scope of the standard are lift, escalators and moving walks with equipment and systems that support connectivity. It means that these systems are installed and maintained on the customer side and capable to connect to other external systems. For example, a lift can have a permanent connection to building networks or cloud services. Additionally, it is able to

temporarily connect to service tools brought to the site during maintenance or other activities. Interfaces of lift systems and equipment are also in the scope of the ISO 8102-20 standard. However, it should be noted that the requirements of this standard are not applicable to lift and escalator equipment installed before the publication of the standard [35].

Compliance with this standard is crucial for vendors of the lifts and escalators domain. It is possible that when a new edition of the Machinery Directive is published, ISO 8102-20 will become obligatory for all lifts providers in the European Union. Although manufacturers will have 3 to 5 years to adapt to the new regulation, it is in the interests of lift manufacturers to meet all requirements as soon as possible. Moreover, a new version of EN 81-76 standard will also require compliance with ISO 8102-20 for a remote assisted evacuation feature in the products. In addition to that, possibly new national standards will refer to requirements of IEC 62443 or ISO 8102-20.

Nevertheless, even if ISO 8102-20 is not mandatory yet, it is expected that cybersecurity aware customers will demand following the requirements of this standard for products intended for buildings of critical infrastructure, such as airports and public transportation systems. They probably have already demanded meeting the requirements of IEC 62443 and asked for the certificate of compliance.

ISO 8102-20 considers lift, escalators and moving walks as the equipment under control (EUC). The assets of the EUC are its components with functional capabilities.

The standard mainly takes requirements from IEC 62443 industrial standards and applies them to the product lifecycle of lifts, escalators and moving walks designed in accordance with ISO 8100 series of standards. The product lifecycle includes the development process, manufacturing, installation, maintenance and decommissioning activities. Security requirements are also applied to the product under development.

The standard uses IEC 62443-4-1 requirements for SDL. However, some of them have additional specifications on applying the requirements to the lift domain in the new standard.

The security requirements of the ISO 8102-20 standard are based on the foundational requirements of IEC 62443 series that are described in IEC 62443-3-3 and IEC 62443-4-2 standards. The common component security constraints are also taken from these standards.

The standard specifies the following functionality-based security domains:

- The safety domain includes safety related control functions. As an example it can be a SIL-rated electric safety device. It is important to understand that every domain is responsible for safety of people

who use the equipment. The scope of the safety domain are only the SIL-rated control functions.

- The essential domain covers functions and capabilities that are required to ensure the lift or escalator availability and its compliance with safety normative documents. It has functions that are not in the Safety or Alarm domains. The essential functions for the lift, for instance, are car and landing indicators, access, door and load control, remote monitoring and interaction, and fire service operation.
- The alarm domain contains devices that are used in case of entrapment. They can be applicable for entrapment verification, calling for help and rescue activities. Examples of them are alarm, intercom and video devices, emergency supply and evacuation device.
- The other domain includes additional functions that cannot be covered by safety, essential or alarm domains. In most cases, devices for entertaining the passengers are related to this domain. For example, displays that show advertisements or music devices.

Each security domain except "other" domain has its own SL-T vector. The mapping of domains to SL-T is demonstrated in Table 4.1. The vectors in the table can be presented in the vector format. For instance, the security vector for the safety domain is  $SL-T(\text{Safety}) = \{3\ 2\ 2\ 2\ 1\ 1\ 2\}$ .

Before the selection of security controls from IEC 62443-3-3 and IEC 62443-4-2 standards for the equipment, it should be determined which components and functions belong to which domain. The requirements of the standards are selected according to the security vector.

In addition, ISO 8100-1 requires presence of alarm function in lifts. In accordance with ISO 8102-20, availability of them is considered more important than confidentiality.

Foundational requirement	Security level		
	Alarm	Essential	Safety
Identification and authentication control (FR 1)	1	2	3
Use control (FR 2)	1	2	2
System integrity (FR 3)	1	2	2
Data confidentiality (FR 4)	1	2	2
Restricted data flow (FR 5)	1	1	1
Timely response to events (FR 6)	1	1	1
Resource availability (FR 7)	1	2	2

Table 4.1: Target security level vectors

## Chapter 5

# Case study of security certification

This chapter provides the analysis of the relation between distributed embedded systems and the IoT. It also introduces the case study of the IoT system that includes a lift controller as an embedded system. The lift controller is a simplified prototype that has some similarities to the real developed solution by KONE Corporation. In addition, the chapter presents this corporation with a description of its main activities and their achievements in the area of cybersecurity.

### 5.1 Distributed embedded systems and IoT

There is no exact definition for an embedded system. Generally, it means a computer system that is designed with a special purpose to control or support operations of a larger technical system with mechanical components in which this embedded system is integrated. An embedded system differs from a computer in performance of tasks. In most cases, it does a limited number of predefined functions and works with limited or no human interaction by using sensors and actuators. Furthermore, this system operates under real time constraints and handles service requests within certain time intervals [17].

In recent years, there has been a drastic rise in the number of the IoT concept implementations. IoT is created for the deployment of smart objects that can sense the surrounding environment, for transmission and processing of data acquired by these objects, and for sending their feedback to the environment. A connection of objects to the Internet is able to improve key values of industries such as sustainability and safety. In addition, it allows

the physical and digital world to efficiently interact with each other. The IoT is considered a disruptive technology that is aimed at solving modern societal issues [49].

The IoT is inextricably linked with embedded systems. However, the relationship between these terms is not clearly defined in scientific literature. For instance, some researchers consider that the IoT is an example of embedded systems. They also explain that innovative development of industry, medical and automotive applications cause IT to converge with embedded systems. Besides, industries that develop embedded systems evolve their processes toward IT using cloud solutions and automatic scaling services [19].

Nevertheless, there is another opinion that distributed embedded systems are part of the IoT where the embedded systems are designed to complete predefined tasks, such as collecting information from sensors and delivering control signals to actuators or processing audio and video signals. These tasks are distributed among several devices that differ from each other in their functional capabilities and characteristics. The researchers also define the IoT as a system that consists of interrelated objects, devices, machines, people with unique identifiers that can transfer data through a network without human interaction. Thus, a distributed embedded system combines different devices to complete a shared task [48].

Moreover, other researchers define embedded systems as cyber-physical systems that combine software and hardware and the capability to interact with the physical world through their components. The embedded systems are part of the IoT and can be considered as IoT devices with the requirement of being connected to the Internet [20].

According to the ISO/IEC 20924 international standard, the IoT represents infrastructure of interconnected entities, systems, information resources and people in conjunction with services which processes and reacts to information gained from the physical and virtual world. The standard also defines IoT system as a system that provides functionalities of the IoT and can include IoT devices, IoT gateways, sensors, and actuators [37].

In the case study a prototype of a lift controller is considered as an embedded system. The case study included in this thesis is based on a simplified version of a real lift controller that can be developed and produced by lift manufacturer, such as KONE Corporation. The controller together with sensors and gateway compose the IoT system.

## 5.2 KONE Corporation

KONE Corporation is a well-known manufacturer of lift and escalators. The company is a world leader in this industry. In addition to lifts and escalators, KONE produces automatic building doors and solutions for maintenance of released products. The company has approximately 550,000 customers in the world and almost 1,5 million equipment in maintenance [8].

KONE focuses on developing smart, connected and sustainable products that are able to adapt to evolving technologies and to the needs of customers and partners.

KONE is an innovator in the lift industry. The corporation has been developing the first digital lift series KONE DX Class that combines digitization of services and built-in connectivity.

KONE has an international reputation for quality of provided products and services. Any problems that impact the reputation could badly affect company's business operations and financial aspects. They can happen due to safety, cybersecurity or non-compliance incidents [7].

To improve security of operations and developed products, KONE collaborates with trusted third-party security service providers to manage security risks and solve security problems. KONE conducts tests, audits and maturity assessments to ensure security on a regular basis. The company measures its improvement in cybersecurity using the NIST CSF.

The corporation constantly invests in its cybersecurity. KONE has developed and established security policies to define security controls for protecting the confidential data and information systems. The protection concerns systems that are under development and already in operation. KONE security controls can detect and timely respond to cybersecurity incidents and allow fast recovery of systems in case of a cybersecurity issue.

In July 2022, KONE received a certificate of compliance with IEC 62443-4-1 standard at ML 3. The certificate was awarded by TÜV Rheinland to demonstrate that SDL processes of the company are properly applied to the development of new solutions, such as KONE DX Class lifts, and fulfill all requirements of the standard. The case study presented in this thesis was conducted using findings from the IEC 62443-4-1 compliance and certification process.

In addition, KONE participates in the cybersecurity standardization initiatives in lift and escalator industry. The company develops solutions to be compliant with the industry cybersecurity standards requirements, such as IEC 62443 and ISO 8102-20.

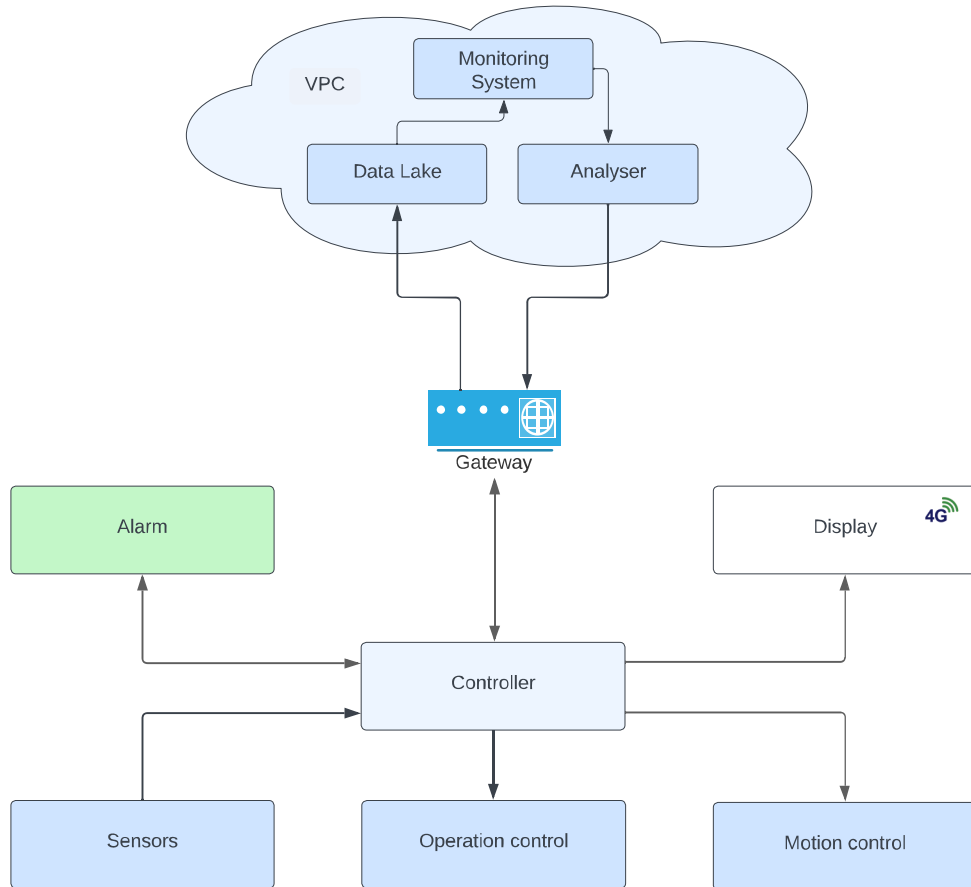


Figure 5.1: Lift controller architecture, simplified example

### 5.3 Product for certification

A prototype of the lift controller used in the case study is presented in Figure 5.1. It has built-in communication functionality for transmitting and receiving information from virtual private cloud (VPC), for normal functioning of the alarm system, and for connecting to the lift system that oversees several lifts. For clarity, the main functions of the controller are represented as components of the controller.

Motion control is an essential capability of the controller that controls the motor of the lift. It allows the controller to use special commands for a lift drive to move the car of the lift and control its speed. The controller uses

the serial bus to communicate with the drive that does not support remote access. Feature wise, the drive is intentionally kept basic to lower risks as it is the most essential part of the lift system. As a result, communication between the controller and the drive is unidirectional. Since the drive cannot hold state, the controller must maintain real-time information of the car position, direction and speed.

The lift is equipped with sensors that send the raw data about speed, load, temperature and landing to the controller that relay this data to the VPC through a local gateway. Once the data is in the cloud, it is stored in a data lake. This storage is massive in size and has low write latency, which is suitable for storing data from many sensors of different lifts in real-time. The raw data is processed into structured information, which is consumed by applications, such as a monitoring system and an analyzer, that monitor and analyze the information respectively. Based on the received information, the analyzer can send commands to the controller, for example, to slow down the car or to go to the particular floor. Furthermore, if the analyzer detects anomalies in the lift data or behaviour, it can contact the personnel responsible for maintenance. The controller also communicates with the VPC to receive commands for upgrading software or to provide debug information.

Through the gateway, the controller is able to communicate with connected devices in the lift car and cloud services, authenticate, route and filter the car network. Single point of entry to the data flow reduces the attack surface and minimizes efforts required to secure the system.

Moreover, the controller supports service tools for maintenance operations provided by the manufacturer. They can be connected to the controller through USB interface or Ethernet port with LAN connection. The communication functionality also uses the USB interfaces for connection to a cellular modem.

The operation control component includes several essential functions of the controller:

- Normal control that is responsible for the overall operation of the lift and controls its functioning.
- Access control that manages access rights of passengers. For example, a person can go to the particular floor only after successful authentication that can be done, for example, with a key or password.
- Door control together with the protective devices and re-opening of the doors capability.

The lift controller supports an alarm functionality comprised of three main parts: a siren, intercom and emergency dialer. The siren is placed both

in the lift car as well as the exterior of the shaft, which alerts people in case of entrapment and gives audio cues about the position of the lift in the shaft.

The intercom allows two-way voice communication between the lift car and the call center. Additionally, by utilizing VoIP of the building network or GSM, lift car is able to communicate directly with a remote operator or emergency service, which is required by the EN 81-28 standard. In cases of emergency, the lift car can dial and alert emergency services such as fire department or hospitals for immediate assistance. The alarm phone regularly makes automatic call to the call services to check if the alarm system is still able to operate normally [23].

The alarm functionality can work autonomously without any user intervention, but it also allow passengers to trigger it manually using buttons inside the lift. One downside of allowing manual alarm system triggers is that bad actors can use them to disturb normal lift service.

Display functionality, not to be confused with floor or direction indicators, is considered to be non essential. Modern lifts can be equipped with high-definition media displays that show advertisements, weather and play music. The display system is equipped with 4G modems that provide Internet connection for its functions. However, the communication is only one way. In case of display malfunction, the function of the lift is not affected. Additionally, displays do not disclose any confidential data, such as parameters of the controller. Thus, any of the displayed information cannot be used for the disruption of lift services.

The controller is placed in a physically secure machine room or a cabinet with restricted access. In the lift industry, it is a generally accepted practice. Moreover, there can be a physical lock that will prevent an unauthorized person from tampering configurations and values of the controller.

## Chapter 6

# Implementation

In this chapter, we apply the ISO 8102-20 standard to the development of the lift controller in the case study.

### 6.1 Identification of scope

Before applying any standard, it is crucial to study its scope. In the case of ISO 8102-20, it is important to understand that the standard is applicable to products that support communication and are capable of connectivity to networks. Accordingly, if a lift and its components do not possess this capability, then the requirements of this standard are not mandatory.

In the case study the lift controller supports connectivity due to the built-in communication functionality. Therefore, the requirements of ISO 8102-20 are applicable to it.

The lift is a system that has multiple components that function as one. For the integration of the components to the lift system, each component should be specified in the context of the system. This means that the component types must be defined in accordance with the IEC 62443-4-2 standard. Moreover, it is required to determine which components belong to which security domains, zones and conduits.

There are examples describing devices that belong to a different component type in IEC 62443-4-2. The Annex A of the standard can help in determining of a component type.

In the case study we consider the lift controller and the devices that it controls or from which it receives data for normal operation as the assets of the EUC. However, cloud services are considered as external services. For this reason, they are not included in the EUC.

We define the lift controller as an embedded device. This is done for the

following reasons:

- Firstly, it fits the definition of the embedded device given in the standard. The lift controller is designed to directly control and monitor the operation of the lift, it has an embedded operating system and supports a limited number of exposed services.
- Secondly, as an example of the embedded device, the standard provides a programmable logic controller that has some similar functionalities with the case study lift controller.

In addition to that, the lift controller has communication function, through which it can transmit data to the VPC and provide functionalities of the IoT. In this case the lift controller has functions of a network device.

Therefore, component requirements from IEC 62443-4-2 for embedded and network devices are applicable to the lift controller. These requirements are security requirements from ISO 8102-20. In addition, the SDL is applicable to the entire lift controller, not just to some parts of it.

The described above actions relate to the requirements *4.2.3 Identification of applicability* and *4.2.5 Process scoping* of the ISO 8102-20 standard.

## 6.2 Identification of zones and domains

As described earlier, the lift controller should be installed in a physical secure location with access control. In the case study, the controller is placed in the machine room that can be accessed through a maintenance cabinet by authorised install and maintenance personnel. The controller can also be placed in the maintenance access panel if it is used for a machine-room-less lift.

The lift controller can be also accessed via the Internet and a building network. The network connection is conducted through the gateway and is used for alarm phone functions, for the management systems controlled by customers and for sending data to the VPC and receiving commands back. The controller supports a cellular modem that is used for secure connection to the VPC. The lift controller also receives the data from sensors.

The identified assets of the EUC are classified into the corresponding security domains:

- The alarm functionality of the controller is under the domain "Alarm".
- Sensors, operation and motion control functions, and gateway that is responsible for the remote interaction with the lift controller form the

domain "Essential". The controller as an asset of the EUC has the essential role. It also does not have SIL-rated functions to perform. That is why it is also included in the "Essential" domain.

- The display is designed to show informative and entertaining content for the passengers. It takes information from the Internet using the built-in 4G modem. It does not send any information to the controller and does not relate to alarm, essential, and safety domains. Therefore, it is under the domain "Other".

We have grouped the assets of the EUC into four zones based on their operation functions. One zone consists of one essential domain and includes the gateway. There is another zone that includes only the essential functions: sensors, operation control, and motion control. We have not combined these zones together because of the trust boundary. Other zones are a zone with the alarm functionality and a zone that includes the display functionality.

The trust boundaries and zones with security domains for the EUC are presented in Figure 6.1.

In the case study, the lift controller has different functionalities including the essential functions. Moreover, these functions have the highest SL-vector requirements for each FR. Thus, the lift controller regardless of its supported functionalities must meet at least the requirements that belong to the essential SL-vector:  $SL-T(\text{Essential}) = \{2\ 2\ 2\ 2\ 1\ 1\ 2\}$ .

The ISO 8102-20 standard provides the minimum SL-vector for each security domain. However, the manufacturer should set the minimum SL for the EUC assets based on the results of threat modelling and risk assessment processes. It should be analysed if the minimum SL from the standard is enough for ensuring security of the developed product. If the standard SL-vector for some functions is not sufficient, the manufacturer must aim for a higher SL.

The standard does not clearly specify how the manufacturer should identify the target SL for the product. Thus, it is possible to decide it based on the expected attacker profile. However, the assumption should be verified by risk assessment.

In the case study, the threat modelling and risk assessment were performed. As a result, we have determined that the SL-C for the lift controller corresponds to the SL-T (Essential) from ISO 8102-20.

Therefore, the controller must meet the SL 2 requirements for the identification and authentication control, use control, system integrity, data confidentiality, resource availability, and the SL 1 requirements for the timely response to events and resource availability. All these requirements are FRs from IEC 62443-4-2.

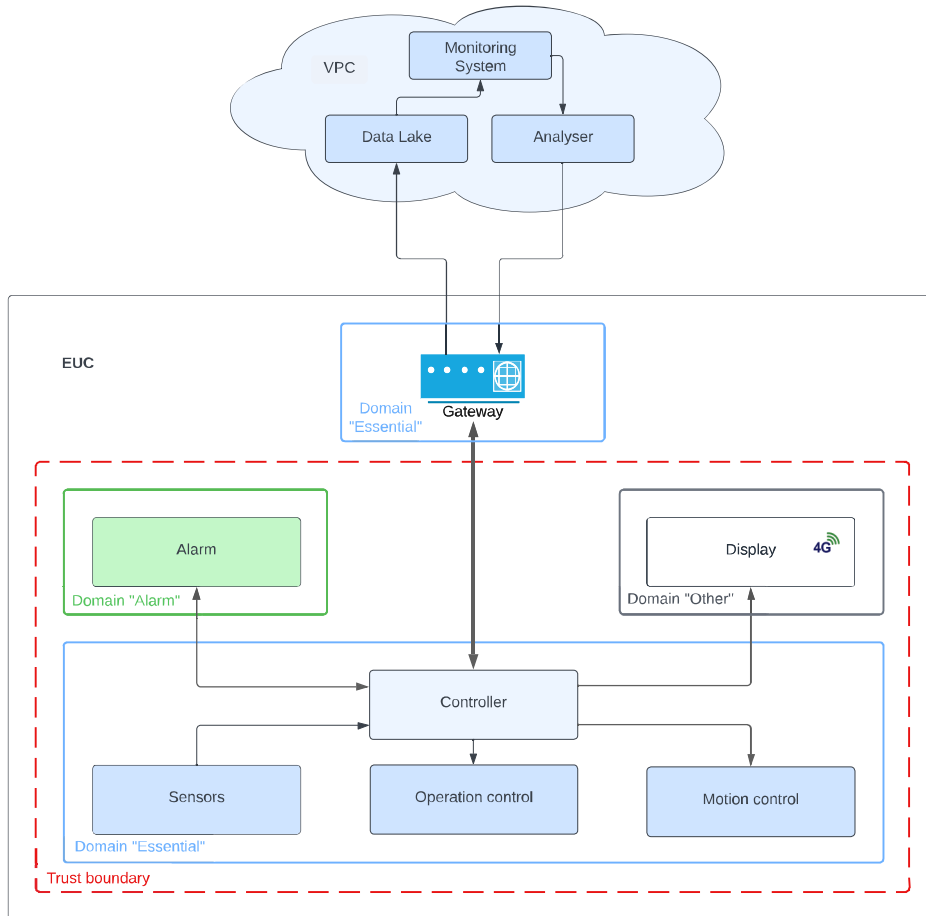


Figure 6.1: Lift controller with defined function domains and zones

The described above actions relate to the requirements *4.3.1 Product security context* and *4.3.2 Threat model* of ISO 8102-20.

### 6.3 Security requirements creation

After identification of zones and required capability SL of the controller, we need to define security requirements based on the IEC 62443-4-2 standard. The requirements must be applied not only to the product under development but also to its lifecycle: to installation, operation, maintenance, and decommissioning processes.

During the security requirements creation, defined zones and SL-C must

Attack vector	Mitigation	Security requirement
Unnecessary ports are open	<ul style="list-style-type: none"> <li>• Unnecessary ports are closed</li> <li>• Firewall controls access to network ports</li> </ul>	CR 7.7 Least functionality

Table 6.1: Example of relation between identified attack vector and security requirement

be considered. The security requirements must be aligned with the threat model, documented, reviewed, updated, and verified.

As an example, we will show the connection between one of the identified attack vectors from the threat model and the security requirement of the IEC 62443-4-2 standard. The described relation is demonstrated in Table 6.1.

The lift controller has ports that are not necessary for the normal operation of the lift. For example, some ports are intended for connection with external systems, such as access control systems. The customer may not use these systems. The mitigation measures are closing unnecessary ports and checking the use of network ports by the firewall. The ports for additional systems can be open by the manufacturer or maintenance service only if the customer uses them.

The security requirement from IEC 62443-4-2 that covers the use of unnecessary ports is *CR 7.7 - Least functionality*. The requirement satisfies the SL 1 and SL 2. Based on this requirement of the standard, we have created a security requirement for the lift controller, which is documented as follows: Only ports for functions that are required for the essential operation of the lift shall be open by default. The controller shall automatically close all unnecessary ports that are not in use for a defined period of time.

In the case study, we use a requirements management software for creation and management of the SDL and security requirements. This software is used for compliance with requirements of various standards. It contains product requirements, security requirements, test plans and test cases for their testing, test results and software defects. The software also supports the review process that is very important for creating high-quality requirements. The requirement management software does not store all information about the product but has links to sources where other details can be found depending on the access restrictions. For example, additional information on the security architecture can be placed in the internal wiki.

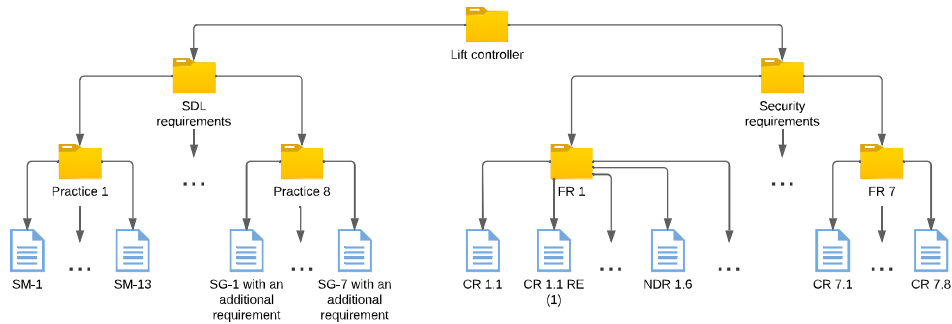


Figure 6.2: SDL and security requirements management structure

The software can generate reports that have all information about requirements or test cases. These reports can also be used as evidence for the auditor.

For the lift controller, there is one folder in the software that is divided into different subfolders with all applicable requirements. The simplified folder structure that we developed to manage SDL and security requirements for the lift controller is demonstrated in Figure 6.2.

The IEC 62443-4-2 standard has Annex B with the table that indicates which component security requirements apply to which FRs for a given SL-C. It is convenient to use this table during the addition of security requirements to the requirements management tool.

Each requirement has a specific description and a status that allows people involved in the development process to trace the current state of the requirement. Moreover, each requirement is linked to the corresponding test cases.

In the requirements management software, we created 47 SDL requirements for the secure development process of the lift controller, 16 of which contain additional requirements according to ISO 8102-20. We also created 76 security requirements in accordance with component requirements for embedded and network devices that are applicable to the controller. Furthermore, we developed the tooling guideline for the ISO 8102-20 compliance that is used by software developers and security specialists at KONE. This guideline explains necessary processes for compliance with the standard, such as creating and managing SDL and security requirements.

Additionally, to visualize the progress of compliance with the requirements, we developed a tool that uses different graphs to represent the current state of this process. For example, it shows the number of fulfilled security

requirements based on their tests results.

The described above actions relate to the requirements *4.3.3 Product security requirements*, *4.3.4 Product security requirements content*, and *4.3.5 Security requirements review* of the ISO 8102-20 standard.

## 6.4 Security requirements testing

A crucial part of any compliance process is the verification and validation testing of security capabilities of the product. The security testing activities ensure that all security requirements have been met.

The ISO 8102-20 standard as well as the IEC 62443-4-1 standard has requirements related to testing the developed product. All security tests should be planned, documented, reviewed and conducted.

In the case study, we defined and documented test types and methods, testing environments and examples of tools in the lift controller security testing plan. It also has descriptions of roles involved in the testing activities and assigned responsibilities in order to ensure the independence of testers.

We created tests cases for security requirements in the requirements management software based on the security testing plan, threat model, default system configuration and defined security requirements. It is important to note that test cases for the product cannot be based only on the clauses of security standards. Therefore, the translation of the high-level security requirements to more detailed technical ones is a crucial part of the compliance process.

For the security requirement that was given as an example in the previous section, we created three test cases in the requirements management software:

- One test case verifies that the product fulfils the security requirement *CR 7.7 - Least functionality* and does not have ports for inessential functionality opened by default.
- Another test case checks that the controller automatically closes unnecessary ports that are not used for a defined period of time.
- The third test case verifies existence of the firewall rules that do not allow access through unnecessary network ports.

All conducted tests must be marked as *passed*. If some tests are not passed, then in addition to the documented results, a defect must be logged into the requirements management software.

The security testing plan, content of the test cases and tests results must be provided to the auditor as evidence of compliance. If the provided evidence is insufficient, the auditor ask the manufacturer to provide additional

documents to clarify or confirm the test results. They also can ask to create additional test cases to test different system configuration.

The described above actions relate to the requirements *4.6.1 Security requirements testing*, *4.6.2 Threat mitigation testing* and *4.7.1 Receiving notifications of security-related issues* of ISO 8102-20.

## Chapter 7

# Observations on ISO 8102-20 and evaluation

In this chapter, we will discuss observations on ISO 8102-20. The observations were made during development of this thesis. Moreover, we will evaluate the results of the application of ISO 8102-20 to the prototype of a lift controller.

### 7.1 Contribution of ISO 8102-20

The publication of the ISO 8102-20 standard is an important milestone in the development of communication technologies, such as the IoT, which can be implemented in the lift and escalator industry. Compliance with requirements of the standard minimizes the risk of a malicious intruder entering the system to cause a disruption of the lift services.

The standard provides unified requirements and methods for all lift manufactures to secure connection between the lift products and external environment. The requirements not only help to improve the efficiency of the lift operations but also allow the manufacturer to ensure safety of personnel and passengers of lifts [40].

Moreover, ISO 8102-20 helps the manufacturer to build the efficient and secure products that support updating the lift remotely. This feature of the modern lift systems provides prompt response to possible lift malfunctions and allows to eliminate the problem as soon as possible. In addition, connecting the lift to the monitoring system via the Internet reduces the workload of the maintenance personnel and the number of their physical interaction with lift systems.

Additionally, the standard helps the manufacturer to protect the systems

from different types of malware. For example, the most dangerous type of malware for organizations at the moment is a ransomware. A malicious actor infects systems with ransomware that restricts access to data or a system for legitimate users. Then, the attacker requests to be paid some amount of money to return access or decrypt files.

The frequency of occurrences of ransomware attacks, has dramatically increased in recent years. The attacks have been targeting mostly computer systems of different organizations including governments, health services and manufactures. Ransomware attacks on distributed embedded systems in IACS are not prevalent right now. However, it is expected that attackers will start actively targeting the IoT systems used in the industry in the near future [46]. For this reason, manufacturers of lifts capable of communicating through the Internet must take care of cybersecurity, which forms the foundation for safety.

Besides, there has already been a case when a successful severe ransomware attack on a large European hotel chain disrupted its business operations and shut down a lift system. As a result, the attackers gained access to a confidential data and were able to disable lifts in hotels of the chain [14].

The ISO 8102-20 as well as standards of the IEC 62443 series does not explicitly define methods of mitigation of ransomware attacks and protection against them. Nonetheless, if the manufacturer meets all SDL and security requirements of ISO 8102-20, it is much more difficult for an attacker to implement a successful ransomware attack on the developed systems.

As described earlier, ISO 8102-20 is based on requirements of IEC 62443-3-3, IEC 62443-4-1, and IEC 62443-4-2. Unlike the listed standards, the ISO 8102-20 standard additionally specifies the information for use as a part of certain requirements. This information for use is intended to provide description of how to achieve, configure and maintain security of the EUC.

In addition, the ISO 8102-20 has the informative Annex A that specifies some aspects of SDL practices for lifts in more detail. For example, it lists SDL documentation that is typically produced during compliance with the SDL requirements. Moreover, it gives an example of identifying specific assets of the lift and includes information about identification of the relevant attacker types or attacker profiles. According to the standard, the threat modeling and risk analysis should start from this identification. Types of attacker profiles can be more than the number of SLs. The profiles may include an incompetent developer, an insider or an unauthorised penetration tester.

Furthermore, the Annex A has some guidance on performing a risk assessment. It provides considerations that should be taken into account during the initial risk assessment and examples of questions that can be used when

developing the documentation. Additionally, the Annex B of the standard provides information on how to apply the risk assessment methods and examples of using risk matrices.

## 7.2 Observations on ISO 8102-20

The ISO 8102-20 standard can be confusing for users who apply it to the EUC. The user can think that only the domain "Safety" and the safety level vector covers the safety functions of a lift. But in reality, the SL vector for the essential domain also includes functionalities related to safety. For instance, the control of the car doors, including protective mechanisms for locking and emergency unlocking of them, relates to ensuring the safety of passengers and maintenance personnel. However, the standard refers the door control including its protective devices to the domain of essential functions. The alarm initiation device is related to safety functionalities and belongs to the domain "Alarm".

Therefore, it is recommended to think that all domains specified in ISO 8102-20 are responsible for safety operations of the EUC. The safety domain exclusively covers the SIL-related functions.

Additionally, the relationship between the terms *EUC* and *IACS* is not clearly defined in the ISO 8102-20 standard. As described previously, the standard is based on the requirements of the IEC 62443-4 standards. The scope of those standards are IACS. However, ISO 8102-20 uses only the EUC term. It may cause readers of the standard to question why the IACS term is not used in the standard and how the EUC relates to that.

The concept of the EUC has been used in the IEC 62443 series before the publication of ISO 8102-20. According to IEC 62443-1-1, the equipment under control is an equipment, machinery, apparatus or plant used for manufacturing, process, transportation, medical or other activities [30]. Thus, the EUC from ISO 8102-20 is included in the concept of the equipment under control from the IEC 62443 series.

It can be concluded that the EUC is the process equipment controlled by the IACS. In the case of lifts, the EUC is a lift system that is controlled by a lift controller and can be divided into different assets. Not all of these assets are controlled by the controller. However, the functions of the controller, such as alarm and safety functions, are assets of the EUC.

As mentioned earlier, the requirements of standards are often described vaguely. They do not have the specific details necessary to implement the requirement and test it. For example, the IEC 62443-4-2 standard has the requirement for validation of input data — *CR 3.5 - Input validation*. One of

the methods to test this requirement is to use fuzzing. Fuzzing or fuzz testing consists in automatically providing random and invalid values as input. The standard does not specify any testing details, such as the types of input values and the duration of the testing. These details should be identified by the manufacturer using a threat model.

Another example of the security requirement from the standard where duration affect the final testing results is *CR 7.1 - Denial of service protection*. The values used for the denial of service testing also should be taken based on the threat model. However, the standard does not provide examples of how long the testing should take and how it should be done.

The lack of detailed instructions can lead to uncertainty for the manufacturer to understand whether the testing was performed correctly and its results reflect the actual security of the product. In order to avoid misunderstanding of how testing activities must be carried out, the manufacturer should prepare testing plans for each component by describing the every step in detail.

It should be noted that the Annex A of the ISO 8102-20 standard contains some information on the performance of fuzz testing and details of a fuzz testing plan. The plan should include listed components for fuzzing, description of the testing process, type of fuzzing, and the pass criteria for the tests.

It is also unclear what criteria the auditor uses to verify the results of testing the implementation of the requirements. Therefore, the product can have the *passed* testing result that is satisfactory for developers but not sufficient for the auditor.

Furthermore, it is quite possible that the manufacturer intentionally does not consider one of the identified threats and does not document it in the threat model. It can be done in order to avoid increasing SL for the product, compliance with more requirements and the implementation of additional security capabilities for the product for the certification. The manufacturer also can accidentally miss one threat that is applicable to the product during the threat modeling process. For both cases, it is not clear whether the auditor can identify the missed threat, or whether the auditor creates their own threat model for the product based on the received evidence.

Another thing to consider is skills and actions of people who install the developed product on the customer site. The manufacturer can follow all recommendations and meet all requirements for SDL, implement all security capabilities required for the highest SL. But it is still challenging to eliminate the risk of human error during installation of the product. The ISO 8102-20 and the IEC 62443-4-1 standards require security guidelines creation for the product that supports installation and gives guidance on hardening

the product during this process. However, the guidelines requirements do not demand the addition of a minimum level of personnel expertise to the guidelines. The IEC 62443-4-1 standard has one *SM-4 - Security expertise* requirement that is about availability of security training and assessment programs for personnel to improve their security expertise. ISO 8102-20 contains the additional requirement to *SM-4* that requires training programmes to include EUC-specific safety expertise.

Nevertheless, this requirement mentions the importance of security awareness training for people involved in SDL. There is no information about how important it is for safety and security that installation personnel have the necessary knowledge and skills to install the developed solutions. Therefore, the manufacturer should provide a secure out-of-the-box product to avoid security problems caused by possible improper installation.

In the lift industry, it is not mandatory for the maintenance company to belong to the lift manufacturer. For example, the manufacturer cannot require customers to use only manufacturer's maintenance services when it has a dominating market position. Thus, in case of changing the maintenance provider, the skills of the maintenance personnel and their actions can cause security problems with a lift. The manufacturer does not know how this company performs lift maintenance. However, if a problem with the lift arise, including security issues, then it may cause the reputational losses for the manufacturer that has a certificate of compliance with cybersecurity standards.

### 7.3 Evaluation of implementation

The practical application of the ISO 8102-20 standard is an important contribution of this thesis to the cybersecurity standards compliance in the lift industry. Chapter 6 can be used as an auxiliary material in preparation for compliance by people involved in this process.

We explained on what grounds and how the type of device for the lift controller was chosen. This explanation can help developers to comply with the standard, as they need to determine the type of device themselves.

Besides, we described in detail the process of identification of zones and domains. This process is crucial for the application of ISO 8102-20. Although the standard has the informative Annex D that contains the guidance for application of zones and conduits, it does not provide examples with system architecture.

Additionally, this annex defines a zone as a group of cyber assets that share the same SL for each FR. In the case study, we have two zones with

the same SL-vectors. According to the IEC 62443-3-2 standard, a zone can be grouped based upon risk and other criteria, such as operation function and physical or logical location [27]. Due to the trust boundary, we have two zones where assets have the essential SL-vector.

Based on the IEC 62443-3-2 and ISO 8102-20 standards, the manufacturer has many options for identifying zones. In our case study, it would be possible to define, for example, only two zones based on the trust boundary. Thus, in one zone there would be only the gateway belonging to the essential domain. In the other zone, there would be alarm functionalities, the lift controller with operation control and motion control, sensors, and the display. However, in this case, it would be required that all elements of one zone share one essential SL-vector, which is the highest in the zone. This is not reasonable because the alarm functionalities can comply with requirements of SL 1. Also, the display does not have functionality that must meet the requirements of the standard. And if these assets are in the same zone with the essential domain, then they must also meet the requirements of SL-T(Essential) that contains requirements of SL 2.

Therefore, in the case study, based on the risk assessment and threat model for assets, four zones were created. We believe that in this case, such identification of zones is the most rational.

To simplify the demonstration of the application of ISO 8102-20 in the case study, PESSRAL is not considered as a subcomponent of the lift controller and not considered as an asset of the EUC. Hence, the SIL-rated functions that form the safety domain are out of scope of the case study. That is why the lift controller interacts with only two security domains in accordance with the standard. The presence of the third domain may complicate the process of applying the standard, especially if several zones and sub-zones are defined.

In the implementation part of our case study, we demonstrated the relation between the identified attack vector from the threat model, security requirements creation and security requirements testing using the example with unnecessary ports. This example can be used to organize activities related to specification of security requirements and their testing. The threat modeling process was carried out without using threat model platforms or software. The process was based on sessions with security experts and established internal policies. To manage the SDL and security requirements of the standard, we used the requirements management software that has been already used by developers to manage functional requirements. This made it possible to reduce the resource costs of implementing a new tool for managing security requirements.

Furthermore, we have provided the names of the SDL requirements, which

correspond to the processes described in the application of the standard. However, some requirements of the SDL practices are out of scope and have not been mentioned. For instance, we assume that the lift controller is implemented according to the defense in depth strategy with using secure by design principles and secure coding standards. Management of security defects and security update management are not in the scope because these practices are often established in the organization for the development process of various products and do not specifically apply only to the lift controller.

In addition, the creation of security guidelines for the end user of the controller is out of scope of the case study because all information that should be in them is described in the requirements of the standards. There are no requirements for the design or structure of these guidelines, so the manufacturer can create them in a free form based on the internal rules. The form of the guidelines is specific to each organization. Nevertheless, we can give one recommendation for creating the guidelines: End users should not need to know all risks and security aspects of the product. They should be aware only about risks that are associated with configuration, installation, and maintenance.

## Chapter 8

# Conclusion

Communication technologies are developing rapidly. They are already actively involved in the machinery manufacturing industry. The ability of machines to interact with each other and remote monitoring systems through networks improves their efficiency.

In the lift industry, distributed embedded systems connected to the Internet allow lifts to support remote services, such as predictive maintenance. For instance, the manufacturer is able to implement remote monitoring of lift systems that can ensure their correct functioning and can immediately notify about an out-of-service lift. Moreover, the manufacturer can perform remote software updates for lifts that have the connectivity capability.

However, the interaction of components of the machinery with the Internet increases the number of cybersecurity threats and risks. Cybersecurity incidents can jeopardise the safety of the machinery and its users. For example, if malicious actors gain control of the lift system, they can disrupt its functioning and cause damage to passengers or maintenance personnel. Therefore, safety of modern lifts that supports connectivity features depends on their security.

To help manufactures with the implementation of cybersecurity measures for the machinery, the industrial cybersecurity standards have been published. In this thesis, we conducted research on the standards of the IEC 62443 series that are applied during the development of distributed embedded systems.

Furthermore, we analyzed ISO 8102-20 — a new cybersecurity standard for lifts, escalators and moving walks. The standard describes SDL requirements, security requirements and methods for securing lift systems and their communication with the external environment, such as a remote monitoring system in the cloud. The observations on the standard are presented in Chapter 7. Besides, we applied the ISO 8102-20 to the development of a

prototype of a lift controller. To the best of author's knowledge, this thesis is the first published work with the evaluation of this standard from a practical point of view. The ISO 8102-20 is based on the IEC 62443 standards, such as IEC 62443-4-1 and IEC 62443-4-2. For this reason, the implementation part also covers requirements from these standards.

To confirm compliance with requirements of standards, manufactures have a certification audit to receive a certificate of compliance. If the manufacturer's development process and products are certified in accordance with cybersecurity standards, such as IEC 62443-4-1 and IEC 62443-4-2, customers and consumers can be confident at security aspects of the developed products. Besides, the certificate allows manufacturers to gain competitive advantage in the market.

We analyzed the cybersecurity standards compliance certification process for IEC 62443-4-1 and IEC 62443-4-2 to improve the preparation for it. At the time of writing, there is no certification programs for the ISO 8102-20 standard. Thus, manufacturers cannot be certified in compliance with the standard. Nonetheless, it is highly probable that certification providers will start to conduct an audit of compliance with this standard in the near future. It is quite possible that the certification audit will be based on certification programs for the IEC 62443-3-3, IEC 62443-4-1 and IEC 62443-4-2 standards.

As future work, the following items can be considered:

- Apply the ISO 8102-20 standard to the component that supports SIL-rated functions and evaluate the results.
- Investigate possible methods to automate implementation of SDL requirements and security requirements, the threat modeling process and testing activities.
- Implement and evaluate the proposed approach of the integration of IEC 62443-4-1 into DevOps pipelines [43]. Propose a solution for integration of security activities in accordance with ISO 8102-20 into DevOps pipelines.
- Study whether the process of meeting the requirements of IEC 62443 or ISO 8102-20 interferes with the compliance process for ISO/IEC 27001.
- Conduct research on the Industrial IoT (IIoT) and its role in the cybersecurity standards compliance process.

This thesis work provides insights into cybersecurity standards compliance process and demonstrates a practical application of the newest cybersecurity standard in the lift industry.

The author participated in the successful certification process of compliance with the IEC 62443-4-1 standard and in the ongoing IEC 62443-4-2 certification process at KONE. After the publication of ISO 8102-20, the author was involved in the process of compliance with this standard and preparation for the certification. The case study presented in this thesis was conducted during these processes. It was updated based on the lessons learned from the certification processes of compliance with IEC 62443-4-1 and IEC 62443-4-2 for use as a simplified example in this thesis.

# Bibliography

- [1] About CEN. <https://www.cencenelec.eu/about-cen/>. Accessed: 2022-09-07.
- [2] About NIST. <https://www.nist.gov/about-nist>. Publication date: 2022-01-11.
- [3] IEC 62443 — CSA Certification. <https://isasecure.org/en-US/Certification/IEC-62443-CSA-Certification>. Accessed: 2022-10-02.
- [4] IEC Technical Committee 65: Industrial-process measurement, control and automation. Dashboard. [https://www.iec.ch/dyn/www/f?p=103:23:6807418416600::::FSP\\_ORG\\_ID,FSP\\_LANG\\_ID:1250,25](https://www.iec.ch/dyn/www/f?p=103:23:6807418416600::::FSP_ORG_ID,FSP_LANG_ID:1250,25). Accessed: 2022-08-29.
- [5] ISA/IEC 62443-4-1: Audit and certification process overview. Webinar. <https://www.isasecure.org/en-US/Learning-Center/Webinars/ISA-IEC-62443-4-1-Audit-and-Certification-Process>. Accessed: 2022-05-09.
- [6] ISO/IEC 27000 Overview. <https://www.isms.online/iso-27000/>. Accessed: 2022-04-27.
- [7] KONE annual review 2021. [https://www.kone.com/en/Images/KONE\\_Annual%20Review%202021\\_tcm17-112892.pdf](https://www.kone.com/en/Images/KONE_Annual%20Review%202021_tcm17-112892.pdf).
- [8] KONE sustainability report 2021. [https://www.kone.com/en/Images/KONE\\_Sustainability\\_Report\\_2021\\_tcm17-115554.pdf](https://www.kone.com/en/Images/KONE_Sustainability_Report_2021_tcm17-115554.pdf).
- [9] Quick start guide: An overview of ISASecure certification. <https://www.isasecure.org/en-US/Documents/0920-ISASecure-QuickStart-Guide-FINAL>. White paper. Accessed: 2022-09-11.
- [10] TÜV Rheinland. About us. <https://www.tuv.com/world/en/about-us/>. Accessed: 2022-09-03.

- [11] Understanding standards. <https://www.iec.ch/understanding-standards>. Accessed: 2022-04-27.
- [12] ANDERSON, R., AND FULORIA, S. Security economics and critical national infrastructure. In *Economics of information security and privacy*. Springer, 2010, pp. 55–66.
- [13] BARNEY, G., Ed. *Guide D: Transportation systems in buildings*. CIBSE, 2020.
- [14] BIJL, P. Case study: Ransomware attack against Nordic Choice Hotels. <https://www.visma.com/blog/case-study-ransomware-attack-against-nordic-choice-hotels/>. Publication date: 2022-10-26.
- [15] BRANDAO FILHO, S. B., AND CESAR, C. D. A. C. A secure method for industrial IoT development. *SN Computer Science* 3, 2 (2022), 1–12.
- [16] CEN/TR 81-10:2008, Safety rules for the construction and installation of lifts — Basics and interpretations — Part 10: System of the EN 81 series of standards. Technical report, CEN, 2008.
- [17] COLNARIČ, M., VERBER, D., AND HALANG, W. A. *Distributed embedded control systems: improving dependability with coherent design*. Springer, 2008.
- [18] CSA-311 Component Security Assurance - Functional security assessment for components. Certification requirements specifications for CSA, ASCI - Automation Standards Compliance Institute, 2019. Version 1.11.
- [19] EBERT, C., AND DUBEY, A. Convergence of enterprise IT and embedded systems. *IEEE Software* 36, 3 (2019), 92–97.
- [20] ECEIZA, M., FLORES, J. L., AND ITURBE, M. Fuzzing the internet of things: A review on the techniques and challenges for efficient vulnerability discovery in embedded systems. *IEEE Internet of Things Journal* 8, 13 (2021), 10390–10411.
- [21] EHRLICH, M., TRSEK, H., WISNIEWSKI, L., AND JASPERNEITE, J. Survey of security standards for an automated Industrie 4.0 compatible manufacturing. In *IECON 2019-45th Annual Conference of the IEEE Industrial Electronics Society* (2019), vol. 1, IEEE, pp. 2849–2854.
- [22] EN 81-20:2020, Safety rules for the construction and installation of lifts — Lifts for the transport of persons and goods — Part 20: Passenger and goods passenger lifts. European standard, CEN, 2020.

- [23] EN 81-28:2022, Safety rules for the construction and installation of lifts — Lifts for the transport of persons and goods — Part 28: Remote alarm on passenger and goods passenger lifts. European standard, CEN, 2022.
- [24] EN 81-50:2020, Safety rules for the construction and installation of lifts — Examinations and tests — Part 50: Design rules, calculations, examinations and tests of lift components. European standard, CEN, 2020.
- [25] FLAUS, J.-M. *Cybersecurity of industrial systems*. John Wiley & Sons, 2019.
- [26] IEC. Understanding IEC 62443. <https://www.iec.ch/blog/understanding-iec-62443>. Publication date: 2021-02-26.
- [27] IEC 62443-3-2:2020, Security for industrial automation and control systems — Part 3-2: Security risk assessment for system design. International standard, IEC, 2020.
- [28] IEC 62443-4-1:2018, Security for industrial automation and control systems — Part 4-1: Secure product development lifecycle requirements. International standard, IEC, 2018.
- [29] IEC 62443-4-2:2019, Security for industrial automation and control systems, Part 4-2: Technical security requirements for IACS components. International standard, IEC, 2019.
- [30] IEC TS 62443-1-1:2009, Industrial communication networks — Network and system security — Part 1-1: Terminology, concepts and models. International standard, IEC, 2009.
- [31] ISO 10241-2:2012, Terminological entries in standards — Part 2: Adoption of standardized terminological entries. International standard, ISO, 2012.
- [32] ISO 12100:2010, Safety of machinery — General principles for design — Risk assessment and risk reduction. International standard, ISO, 2010.
- [33] ISO 8100-1:2019, Lifts for the transport of persons and goods — Part 1: Safety rules for the construction and installation of passenger and goods passenger lifts. International standard, ISO, 2019.
- [34] ISO 8100-2:2019, Lifts for the transport of persons and goods — Part 2: Design rules, calculations, examinations and tests of lift components. International standard, ISO, 2019.

- [35] ISO 8102-20:2022, Electrical requirements for lifts, escalators and moving walks — Part 20: Cybersecurity. International standard, ISO, 2022.
- [36] ISO/IEC 17000:2020, Conformity assessment — Vocabulary and general principles. Standard, ISO/IEC, 2020.
- [37] ISO/IEC 20924:2021, Information technology — Internet of Things (IoT) — Vocabulary. International standard, ISO/IEC, 2021.
- [38] ISO/TR 22100-1:2021, Safety of machinery — Relationship with ISO 12100 — Part 1: How ISO 12100 relates to type-B and type-C standards. Technical report, ISO, 2021.
- [39] ISO/TR 22100-4:2018, Safety of machinery — Relationship with ISO 12100 — Part 4: Guidance to machinery manufacturers for consideration of related IT-security (cyber security) aspects. Technical report, ISO, 2018.
- [40] KONE. Elevators and escalators just got safer — thanks to a new cybersecurity standard. <https://www.kone.com/en/news-and-insights/stories/elevators-and-escalators-just-got-safer-thanks-to-a-new-cybersecurity-standard.aspx>. Press release. Publication date: 2022-10-27.
- [41] LEANDER, B., ČAUŠEVIĆ, A., AND HANSSON, H. Applicability of the IEC 62443 standard in Industry 4.0/IIoT. In *Proceedings of the 14th International Conference on Availability, Reliability and Security* (2019), pp. 1–8.
- [42] MEHRFELD, J. Cyber security threats and incidents in industrial control systems. In *International Conference on Human-Computer Interaction* (2020), Springer, pp. 599–608.
- [43] MOYÓN, F., SOARES, R., PINTO-ALBUQUERQUE, M., MENDEZ, D., AND BECKERS, K. Integration of security standards in devops pipelines: An industry case study. In *International Conference on Product-Focused Software Process Improvement* (2020), Springer, pp. 434–452.
- [44] NIST COMPUTER SECURITY RESOURCE CENTER. Glossary. Certification. <https://csrc.nist.gov/glossary/term/certification>. Accessed: 2022-04-28.
- [45] NIŽETIĆ, S., ŠOLIĆ, P., GONZÁLEZ-DE, D. L.-D.-I., PATRONO, L., ET AL. Internet of Things (IoT): Opportunities, issues and challenges

- towards a smart and sustainable future. *Journal of Cleaner Production* 274 (2020), 122877.
- [46] OZ, H., ARIS, A., LEVI, A., AND ULUAGAC, A. S. A survey on ransomware: Evolution, taxonomy, and defense solutions. *ACM Computing Surveys (CSUR)* 54, 11s (2022), 1–37.
- [47] PARK, C. S., LEE, J. H., SEO, S. C., AND KIM, B. K. Assuring software security against buffer overflow attacks in embedded software development life cycle. In *2010 The 12th International Conference on Advanced Communication Technology (ICACT)* (2010), vol. 1, IEEE, pp. 787–790.
- [48] RASKIN, D., VASSILIEV, A., SAMARIN, V., CABEZAS, D., HIERERRA, S. E., AND KURNIAWAN, Y. Rapid prototyping of distributed embedded systems as a part of internet of things. *procedia computer science* 135 (2018), 503–509.
- [49] SISINNI, E., SAIFULLAH, A., HAN, S., JENNEHAG, U., AND GIDLUND, M. Industrial internet of things: Challenges, opportunities, and directions. *IEEE transactions on industrial informatics* 14, 11 (2018), 4724–4734.
- [50] STEINER, W., BONOMI, F., AND KOPETZ, H. Towards synchronous deterministic channels for the internet of things. In *2014 IEEE world forum on Internet of Things (WF-IoT)* (2014), IEEE, pp. 433–436.
- [51] TUPTUK, N., AND HAILES, S. Security of smart manufacturing systems. *Journal of manufacturing systems* 47 (2018), 93–106.
- [52] VAN OORSCHOT, P. C., AND SMITH, S. W. The internet of things: security challenges. *IEEE Security & Privacy* 17, 5 (2019), 7–9.