

DRAFT INTERNATIONAL STANDARD

ISO/DIS 8102-20

ISO/TC 178

Secretariat: **AFNOR**

Voting begins on:
2021-08-30

Voting terminates on:
2021-11-22

Electrical requirements for lifts, escalators and moving walks —

Part 20: Cybersecurity

ICS: 91.140.90

THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENT AND APPROVAL. IT IS THEREFORE SUBJECT TO CHANGE AND MAY NOT BE REFERRED TO AS AN INTERNATIONAL STANDARD UNTIL PUBLISHED AS SUCH.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

This document is circulated as received from the committee secretariat.



Reference number
ISO/DIS 8102-20:2021(E)

© ISO 2021



COPYRIGHT PROTECTED DOCUMENT

© ISO 2021

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

	Page
Foreword	v
Introduction	vi
1 Scope	1
2 Normative references	2
3 Terms and definitions and abbreviated terms	2
3.1 Terms and definitions	2
3.2 Abbreviated terms	3
4 Secure development life cycle for lifts, escalators and moving walks	4
4.1 General	4
4.2 Security management	4
4.2.1 Development process	4
4.2.2 Identification of responsibilities	4
4.2.3 Identification of applicability	4
4.2.4 Security expertise	4
4.2.5 Process scoping	4
4.2.6 File integrity	4
4.2.7 Development environment security	4
4.2.8 Controls for private keys	4
4.2.9 Security requirements for externally provided components	5
4.2.10 Custom developed components from third-party suppliers	5
4.2.11 Assessing and addressing security-related issues	5
4.2.12 Process verification	5
4.2.13 Continuous improvement	5
4.3 Specification of security requirements	5
4.3.1 Product security context	5
4.3.2 Threat model	5
4.3.3 Product security requirements	5
4.3.4 Product security requirements content	5
4.3.5 Security requirements review	5
4.4 Secure by design	6
4.4.1 Secure design principles	6
4.4.2 Defence in depth design	6
4.4.3 Security design review	6
4.4.4 Secure design best practices	6
4.5 Secure implementation	6
4.5.1 Security implementation review	6
4.5.2 Secure coding standards	6
4.6 Security verification and validation testing	6
4.6.1 Security requirements testing	6
4.6.2 Threat mitigation testing	6
4.6.3 Vulnerability testing	6
4.6.4 Penetration testing	6
4.6.5 Independence of testers	6
4.7 Management of security-related issues	6
4.7.1 Receiving notifications of security-related issues	6
4.7.2 Reviewing security-related issues	7
4.7.3 Assessing security-related issues	7
4.7.4 Addressing security-related issues	7
4.7.5 Disclosing security-related issues	7
4.7.6 Periodic review of security defect management practice	7
4.8 Security update management	7
4.8.1 Security update qualification	7
4.8.2 Security update documentation	7

4.8.3	Dependent component or operating system security update documentation	7
4.8.4	Security update delivery	7
4.8.5	Timely delivery of security patches	7
4.9	Security guidelines	8
4.9.1	Product defence in depth	8
4.9.2	Defence in depth measures expected in the environment	8
4.9.3	Security hardening guidelines	8
4.9.4	Secure disposal guidelines	8
4.9.5	Secure operation guidelines	8
4.9.6	Account management guidelines	8
4.9.7	Documentation review	8
5	Security requirements	8
5.1	General	8
5.2	Foundational requirements	8
5.3	Domains of the EUC functions	9
5.4	EUC security level requirements	10
5.5	Selection of countermeasures	10
5.6	Common security constraints	11
5.6.1	General	11
5.6.2	Support of essential functions	11
5.6.3	Compensating countermeasures	11
5.6.4	Least privilege	11
5.6.5	Software development process	11
6	Information for use	11
Annex A	(informative) Additional information on secure development life cycle for lifts, escalators and moving walks	13
Annex B	(informative) Additional information on how to apply the general method of risk assessments	25
Annex C	(informative) List of Security Practices	29
Annex D	(informative) Guidance for application of zones and conduits	31
Bibliography	34

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 178, *Lifts, escalators and moving walks*.

This document is product security publication (see IEC Guide 120:2018).

A list of all parts in the ISO 8102 series can be found on the ISO website.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

Market requirements and enhanced cyber security awareness has prompted the need of this document. State of the art cyber security standard for operational technology is IEC 62443 series. This particular document addresses industry specific requirements found necessary when applying IEC 62443 series.

The fundamental principle of cybersecurity is a strong cybersecurity process life cycle. This life cycle needs to include adequate training, tools, resources, and processes to develop, harden and maintain the resiliency of the equipment under control (EUC) against cyber-attacks. The life cycle approach is also a fundamental premise of best practices utilized for various cybersecurity standards and approaches.

Electrical requirements for lifts, escalators and moving walks —

Part 20: Cybersecurity

1 Scope

This document specifies cybersecurity requirements for new lifts, escalators and moving walks, later in this document called as EUC (Equipment Under Control) designed according to ISO 8100 series and may be applied to other lift, escalator, and moving walk standards that specify similar requirements. This document may be applied to other lift-related equipment connected to the EUC.

This document covers product and system requirements related to cybersecurity threats in following life cycle steps:

- product development (process and product requirements);
- manufacturing;
- installation;
- operation and maintenance;
- decommissioning.

This document addresses the roles of product supplier and system integrator as shown in IEC 62443-4-1 Figure 2 for the EUC.

This document does not address the role of asset owner as shown in IEC 62443-4-1 Figure 2, but defines requirements for the product supplier and system integrator of the EUC to establish documentation allowing the asset owner, referred to as EUC owner in this document, to achieve and maintain the security level.

This document gives minimum cybersecurity requirements for

- essential functions;
- safety functions;
- alarm functions.

This document covers EUCs capable of connectivity, either through equipment permanently available on site, or equipment temporarily brought to the location during the installation, operation and maintenance, or decommissioning steps.

EUC interfaces to external systems and services are in the scope of this document. However, the external systems and services as such are out of the scope.

NOTE External systems and services, which the EUC may rely upon, are assumed to comply with their own security standard, e.g. IEC 62443-2-4 or ISO 27017 for cloud platform.

This document is not applicable to EUC, which are installed before the date of its publication.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

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*

IEC/TS 62443-1-1:2009, *Industrial communication networks — Network and system security — Part 1-1: Terminology, concepts and models*

IEC 62443-3-2:2020, *Security for industrial automation and control systems — Part 3-2: Security risk assessment for system design*

IEC 62443-3-3:2013, *Industrial communication networks — Network and system security — Part 3-3: System security requirements and security levels*

IEC 62443-4-1:2018, *Security for industrial automation and control systems — Part 4-1: Secure product development lifecycle requirements*

IEC 62443-4-2:2019, *Security for industrial automation and control systems — Part 4-2: Technical security requirements for IACS components*

3 Terms and definitions and abbreviated terms

3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 8100-1:2019, IEC/TS 62443-1-1:2009, IEC 62443-3-2:2020 and the following apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at <https://www.iso.org/obp>

— IEC Electropedia: available at <https://www.electropedia.org/>

3.1.1 cybersecurity

measures taken to protect a computer or computer system against unauthorized access or attack

Note 1 to entry: Lift, escalator and moving walk control systems are considered in this document as a computer systems.

Note 2 to entry: In this document term security includes cybersecurity.

[SOURCE: IEC 62443-3-2:2020, 3.1.7, modified]

3.1.2 EUC equipment under control

lift, escalator or moving walk

3.1.3 EUC owner

individual or organization responsible for the EUC

Note 1 to entry: EUC owner is equivalent to IEC 62443-4-1:2018 term 3.1.6 asset owner.

[SOURCE: IEC 62443-4-1:2018, 3.1.6, modified]

3.2 Abbreviated terms

BPCS	basic process control system
CR	component requirement
CCSC	common component security constraint
DoS	denial of service
DM	defect management
E/E/PE	electrical/electronic/programmable electronic
EDR	embedded device requirement
EUC	equipment under control
FR	foundational requirement
HDR	host device requirement
HFT	hardware fault tolerance
IAC	identification and authentication control
IACS	industrial automation and control systems
NDR	network device requirement
RA	resource availability
RDF	restricted data flow
RE	requirement enhancement
SAR	software application requirement
SC	systematic capability
SIL	safety integrity level
SL	security level
SL-T	target security level
SL-C	capability security level
SD	secure design
SG	security guideline
SI	secure implementation
SM	security management
SR	security requirement
SUM	security update management

SVV	security verification and validation
TRE	timely response to events
UC	use control

4 Secure development life cycle for lifts, escalators and moving walks

4.1 General

The requirements of this clause shall apply to component development and system integration. See [Annex A](#) for additional information on secure development life cycle, [Annex B](#) for additional information on security risk assessments and [Annex C](#) for list of security practices.

4.2 Security management

4.2.1 Development process

The requirements of IEC 62443-4-1:2018, SM-1: Development process, shall apply.

4.2.2 Identification of responsibilities

The requirements of IEC 62443-4-1:2018, SM-2: Identification of responsibilities, shall apply.

4.2.3 Identification of applicability

The requirements of IEC 62443-4-1:2018, SM-3: Identification of applicability, shall apply.

4.2.4 Security expertise

The requirements of IEC 62443-4-1:2018, SM-4: Security expertise, shall apply.

In addition to cyber-security, training programs shall also include safety expertise as defined in the ISO 8100 series.

NOTE ISO/TR 22100-4:2018 gives machine manufacturers guidance on potential security aspects in relation to safety of machinery.

4.2.5 Process scoping

The requirements of IEC 62443-4-1:2018, SM-5: Process scoping, shall apply.

4.2.6 File integrity

The requirements of IEC 62443-4-1:2018, SM-6: File integrity, shall apply.

The information for use shall indicate the possible need for the EUC owner to verify the integrity for all scripts, executables and other important files included in a product.

4.2.7 Development environment security

The requirements of IEC 62443-4-1:2018, SM-7: Development environment security, shall apply.

4.2.8 Controls for private keys

The requirements of IEC 62443-4-1:2018, SM-8: Controls for private keys, shall apply.

4.2.9 Security requirements for externally provided components

The requirements of IEC 62443-4-1:2018, SM-9: Security requirements for externally provided components, shall apply.

The information for use shall indicate the need for the EUC owner to identify and manage the security risks of all externally provided components used subsequently within the product.

4.2.10 Custom developed components from third-party suppliers

The requirements of IEC 62443-4-1:2018, SM-10: Custom developed components from third-party suppliers, shall apply.

4.2.11 Assessing and addressing security-related issues

The requirements of IEC 62443-4-1:2018, SM-11: Assessing and addressing security-related issues, shall apply.

4.2.12 Process verification

The requirements of IEC 62443-4-1:2018, SM-12: Process verification, shall apply.

4.2.13 Continuous improvement

The requirements of IEC 62443-4-1:2018, SM-13: Continuous improvement, shall apply.

The information for use shall indicate the need for the EUC owner to co-operate with component manufacturer and system integrator to continuously improve the cyber-security of the EUC.

4.3 Specification of security requirements**4.3.1 Product security context**

The requirements of IEC 62443-4-1:2018, SR-1: Product security context, shall apply.

The information for use shall indicate assumptions about the environment of the EUC.

4.3.2 Threat model

The requirements of IEC 62443-4-1:2018, SR-2: Threat model, shall apply.

The threat model shall consider the complete life cycle of the EUC.

4.3.3 Product security requirements

The requirements of IEC 62443-4-1:2018, SR-3: Product security requirements, shall apply.

4.3.4 Product security requirements content

The requirements of IEC 62443-4-1:2018, SR-4: Product security requirements content, shall apply.

4.3.5 Security requirements review

The requirements of IEC 62443-4-1:2018, SR-5: Security requirements review, shall apply.

4.4 Secure by design

4.4.1 Secure design principles

The requirements of IEC 62443-4-1:2018, SD-1: Secure design principles, shall apply.

4.4.2 Defence in depth design

The requirements of IEC 62443-4-1:2018, SD-2: Defence in depth design, shall apply

4.4.3 Security design review

The requirements of IEC 62443-4-1:2018, SD-3: Security design review, shall apply

4.4.4 Secure design best practices

The requirements of IEC 62443-4-1:2018, SD-4: Secure design best practices, shall apply

4.5 Secure implementation

4.5.1 Security implementation review

The requirements of IEC 62443-4-1:2018, SI-1: Security implementation review, shall apply.

4.5.2 Secure coding standards

The requirements of IEC 62443-4-1:2018, SI-2: Secure coding standards, shall apply.

4.6 Security verification and validation testing

4.6.1 Security requirements testing

The requirements of IEC 62443-4-1:2018, SVV-1: Security requirements testing, shall apply.

4.6.2 Threat mitigation testing

The requirements of IEC 62443-4-1:2018, SVV-2: Threat mitigation testing, shall apply.

4.6.3 Vulnerability testing

The requirements of IEC 62443-4-1:2018, SVV-3: Vulnerability testing, shall apply.

4.6.4 Penetration testing

The requirements of IEC 62443-4-1:2018, SVV-4: Penetration testing, shall apply.

4.6.5 Independence of testers

The requirements of IEC 62443-4-1:2018, SVV-5: Independence of testers, shall apply.

4.7 Management of security-related issues

4.7.1 Receiving notifications of security-related issues

The requirements of IEC 62443-4-1:2018, DM-1: Receiving notifications of security-related issues, shall apply.

4.7.2 Reviewing security-related issues

The requirements of IEC 62443-4-1:2018, DM-2: Reviewing security-related issues, shall apply.

4.7.3 Assessing security-related issues

The requirements of IEC 62443-4-1:2018, DM-3: Assessing security-related issues, shall apply.

4.7.4 Addressing security-related issues

The requirements of IEC 62443-4-1:2018, DM-4: Addressing security-related issues, shall apply.

The information for use shall indicate the need for the EUC owner to address security-related issues.

4.7.5 Disclosing security-related issues

The requirements of IEC 62443-4-1:2018, DM-5: Disclosing security-related issues, shall apply.

4.7.6 Periodic review of security defect management practice

The requirements of IEC 62443-4-1:2018, DM-6: Periodic review of security defect management practice, shall apply.

4.8 Security update management**4.8.1 Security update qualification**

The requirements of IEC 62443-4-1:2018, SUM-1: Security update qualification, shall apply.

4.8.2 Security update documentation

The requirements of IEC 62443-4-1:2018, SUM-2: Security update documentation, shall apply.

The information for use shall indicate the need for the EUC owner to maintain the security documentation up to date.

4.8.3 Dependent component or operating system security update documentation

The requirements of IEC 62443-4-1:2018, SUM-3: Dependent component or operating system security update documentation, shall apply.

4.8.4 Security update delivery

The requirements of IEC 62443-4-1:2018, SUM-4: Security update delivery, shall apply.

The information for use shall indicate the means for the EUC owner to verify security patch authenticity.

4.8.5 Timely delivery of security patches

The requirements of IEC 62443-4-1:2018, SUM-5: Timely delivery of security patches, shall apply.

The information for use shall indicate the means for the EUC owner to apply security patches in a timely manner.

4.9 Security guidelines

4.9.1 Product defence in depth

The requirements of IEC 62443-4-1:2018, SG-1: Product defence in depth, shall apply.

The information for use shall give an overview of the security defence in depth strategy to the extent required by the asset owner to maintain the EUC security level.

4.9.2 Defence in depth measures expected in the environment

The requirements of IEC 62443-4-1:2018, SG-2: Defence in depth measures expected in the environment, shall apply.

The information for use shall indicate the measures expected to be provided by the EUC owner for hardening the EUC.

4.9.3 Security hardening guidelines

The requirements of IEC 62443-4-1:2018, SG-3: Security hardening guidelines, shall apply.

The information for use shall include guidelines for installing and maintaining the cybersecurity of the EUC.

4.9.4 Secure disposal guidelines

The requirements of IEC 62443-4-1:2018, SG-4: Secure disposal guidelines, shall apply.

The information for use shall include cybersecurity guidelines for removing the EUC from use.

4.9.5 Secure operation guidelines

The requirements of IEC 62443-4-1:2018, SG-5: Secure operation guidelines, shall apply.

The information for use shall include cybersecurity guidelines for operating the EUC.

4.9.6 Account management guidelines

The requirements of IEC 62443-4-1:2018, SG-6: Account management guidelines, shall apply.

The information for use shall document the management accounts, permissions and privileges required for operating the EUC.

4.9.7 Documentation review

The requirements of IEC 62443-4-1:2018, SG-7: Documentation review, shall apply.

5 Security requirements

5.1 General

IEC 62443-3-3:2013 and IEC 62443-4-2:2019 form the basis of the security requirements specified in this document.

5.2 Foundational requirements

IEC/TS 62443-1-1:2009 defines seven foundational requirements (FRs), which shall be applied to EUC functions defined in [5.5](#).

Security requirements from IEC 62443 series shall result in the selection and application of security controls, documented, developed and validated according to [Clause 4](#).

5.3 Domains of the EUC functions

In the scope of this document, the EUC functions are classified into the domains of safety, essential, alarm and other. The domains are described in [Table 1](#).

Table 1 — Domains of the EUC functions

Domain	Description	Non-comprehensive list of functions under the domains as examples
Safety	SIL-rated control functions.	<ul style="list-style-type: none"> — SIL-rated electric safety devices and electrical protective devices — SIL rated motor and brake control functions
Essential	Function or capability that is required to ensure the availability of the lift, escalator or moving walk, and its compliance to safety regulations.	<ul style="list-style-type: none"> — Normal control — Car and landing call devices — Access control — Energy saving (car light, ventilation etc....) — Car and landing indicators — Machine motor and car motor control — Overload detection (to avoid opening the brake) — Run time limiter — Fire service operation — Return to normal operation of the lift — Re-opening of the door <p>Escalator and moving walks</p> <ul style="list-style-type: none"> — Start and stop functionalities — Timetable and system clock operations — Escalator direction indicators — Preventing from starting when permitted stopping distance exceeded — Protection of motors — Automatic operation - starting in predetermined direction
Alarm	Devices used to call help and rescue passenger in case of entrapment.	<ul style="list-style-type: none"> — Alarm and intercom devices — Emergency supply — Evacuation device — Displays and voice announcements used for rescue

Table 1 (continued)

Domain	Description	Non-comprehensive list of functions under the domains as examples
Other	Additional function not related to safety, essential or alarm domains	<ul style="list-style-type: none"> — Advertising displays — Music and gaming devices — User applications

5.4 EUC security level requirements

Each EUC function domain shall have the minimum security level capability (SL-C) defined in [Table 2](#). The SL-C requirement is defined as a vector of SLs, with a separate SL specified for each of the seven FRs.

NOTE Security level capability (SL-C) for domain “Other” is not defined in this document.

The information for use shall document the means to achieve the minimum security level target (SL-T) defined in [Table 2](#).

NOTE The security level vector approach is discussed in Annex A of IEC 62443-3-3:2019.

If functions or components of the EUC are part of functions with different security level vectors, the highest security level vector shall be applied.

The EUC interfaces to external systems and services as well as service functions within EUC shall have at least the security level vector of the alarm, essential or safety function they service.

Security level vectors for other functions are not defined in this document.

Table 2 — Security level vectors for EUC function domains

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

NOTE [Table 2](#) can be presented in vector format described in IEC 62443-3-3:2013, A.3.3, as example “SL-T(Alarm) = {2 2 2 1 1 1 1}”.

5.5 Selection of countermeasures

After the EUC function domain and the corresponding security level vector from [Table 2](#) has been selected, the countermeasures shall be selected from IEC 62443-3-3:2013 and IEC 62443-4-2:2019, as applicable. However, should the threat model required in [4.3.2](#) yield threats that are not adequately mitigated by using [Table 2](#) alone, the residual threats shall be mitigated by additional security controls and countermeasures.

NOTE 1 IEC 62443-3-3:2013 describes the system requirements (SR) and requirement enhancements (RE) that are applied to the entire system under consideration.

Normen-Download-Beuth- VFA- Interliff. e. V.-KdNr.: 6363432-ID.9MEKVIKOCNIP90LXJPEW5SLM6.1-2021-10-11 16:25:18

NOTE 2 IEC 62443-4-2:2019 describes the component requirements (CR) and requirement enhancements (RE) that are applied to components of the system. There are component specific requirements for software applications (SAR), embedded devices (EDR), host devices (HDR) and network devices (NDR).

5.6 Common security constraints

5.6.1 General

When implementing the security requirements (SRs or CRs), common component security constraints (CCSCs) specified in [5.6.2](#) to [5.6.5](#) shall be applied.

5.6.2 Support of essential functions

The requirements of IEC 62443-4-2:2019, CCSC 1: Support of essential functions, shall apply.

For lifts, escalators and moving walks, the essential functions referenced in CCSC 1 include safety, essential and alarm functions as shown in [5.3](#).

Availability of alarm functions required by ISO 8100-1:2019 shall take precedence over confidentiality.

Control system networks used for alarm functions required by ISO 8100-1:2019 shall be defined as critical control system networks in IEC 62443-3-3:2013.

5.6.3 Compensating countermeasures

The requirements of IEC 62443-4-2:2019, CCSC 2: Compensating countermeasures, shall apply.

NOTE Examples of application specific compensating countermeasures are given in [A.3.5](#).

5.6.4 Least privilege

The requirements of IEC 62443-4-2:2019, CCSC 3: Least privilege, shall apply.

5.6.5 Software development process

The requirements of IEC 62443-4-2:2019, CCSC 4: Software development process, shall apply.

6 Information for use

Information for use shall describe how to integrate, configure, and maintain the security of the EUC. The information for use shall also include target security level and necessary guidance to assess and maintain the achieved level.

The information for use shall address the roles of different stakeholders including potential changes and required knowledge transfer during the life cycle, e.g. change of maintenance provider.

Information for use shall include guidance on secure installation of the EUC. Installation guidance shall list and explain all security configuration options present in the EUC and make note of their default and optional settings. Additionally, the installation guidance shall contain all field and external testing requirements to be performed before commissioning to create a secure installation.

There shall be means to store the documentation of the secure installation and forward it to other stakeholders on a need-to-know basis when requested.

Information for use shall contain procedures for reporting security vulnerabilities in a way that does not risk other installations using similar components, e.g. email address and PGP key to encrypt the message contents.

Table 3 sets the requirements for information for use in addition to the ones mentioned above.

NOTE See ISO/TR 22100-4:2018 for guidance on cooperation and coordination between different stakeholders during the whole life cycle.

Table 3 — Requirements for information for use

Clause in this document	Reference	Requirement for information for use
4.2.6	IEC 62443-4-1:2018, SM-6: File integrity	The information for use shall indicate the possible need for the EUC owner to verify the integrity for all scripts, executables and other important files included in a product.
4.2.9	IEC 62443-4-1:2018, SM-9: Security requirements for externally provided components	The information for use shall indicate the need to identify and manage the security risks of all externally provided components used subsequently within the product.
4.2.13	IEC 62443-4-1:2018, SM-13: Continuous improvement	The information for use shall indicate the need for the EUC owner to co-operate with component manufacturer and system integrator to continuously improve the cybersecurity of the EUC.
4.3.1	The requirements of IEC 62443-4-1:2018, SR-1: Product security context	The information for use shall indicate assumptions about the environment of the EUC.
4.7.4	IEC 62443-4-1:2018, DM-4: Addressing security-related issues	The information for use shall indicate the need to address security-related issues.
4.8.2	IEC 62443-4-1:2018, SUM-2: Security update documentation	The information for use shall indicate the need to maintain the security documentation up to date.
4.8.4	IEC 62443-4-1:2018, SUM-4: Security update delivery	The information for use shall indicate the means to verify security patch authenticity.
4.8.5	IEC 62443-4-1:2018, SUM-5: Timely delivery of security patches	The information for use shall indicate the means to apply security patches in a timely manner.
4.9.1	IEC 62443-4-1:2018, SG-1: Product defence in depth	The information for use shall give an overview of the security defence in depth strategy to the extent required by the asset owner to maintain the EUC security level.
4.9.2	IEC 62443-4-1:2018, SG-2: Defence in depth measures expected in the environment	The information for use shall indicate the measures expected to be provided by the external environment in which the product is to be used.
4.9.3	IEC 62443-4-1:2018, SG-3: Security hardening guidelines	The information for use shall include guidelines for installing and maintaining the cybersecurity of the EUC.
4.9.4	IEC 62443-4-1:2018, SG-4: Secure disposal guidelines	The information for use shall include cybersecurity guidelines for removing the EUC from use.
4.9.5	IEC 62443-4-1:2018, SG-5: Secure operation guidelines	The information for use shall include cybersecurity guidelines for operating the EUC.
4.9.6	IEC 62443-4-1:2018, SG-6: Account management guidelines	The information for use shall document the management accounts, permissions and privileges required for operating the EUC.

Annex A (informative)

Additional information on secure development life cycle for lifts, escalators and moving walks

A.1 General

The fundamental principle of cybersecurity is a mature cybersecurity process life cycle. This life cycle should include adequate training, tools, resources, and processes to harden and maintain the EUC from cyber-attacks.

The recommended cybersecurity process life cycle practices are shown in [Table C.1](#).

A.2 Security management

A.2.1 Process scoping

It is important to understand the type of equipment under development as well as the context in which the equipment under design is to be deployed. Components being developed for integration into an EUC may contain no external connections, and/or be physically isolated, per relevant requirements. However, some components may have external connections, not as a requirement of their primary function, but as an enhancement to their operation (as in providing data to service systems or accepting software updates). It is important, therefore, to have a robust process to analyse and/or model the component, and review in order to determine whether the requirements of this specification are applicable to the component.

A.2.2 Security development documentation

[Table A.1](#) lists the typical documentation produced during secure development life cycle.

Table A.1 — Typical secure development life cycle documentation

Document	Description	Reference
Threat modelling and risk assessment	The threat model with residual risks identified.	4.3.9
Security requirement and secure design	The design document, identifying each security requirement and associated security control.	4.2.5
Security test plan	Testing plan showing how each security control has been tested to ensure it meets the security requirement.	4.6.1
Analysis reports	Reports summarizing the results of performed analyses and highlighting any found issues and insufficient security controls. Examples: <ul style="list-style-type: none"> — third party code/library analysis report; — dynamic security analysis report; — static code analysis report. 	4.5.1
Test reports	<ul style="list-style-type: none"> — Fuzz testing report — Internal penetration testing report — External penetration testing report 	4.6.2 to 4.6.7
Information for use	See Clause 6 .	Clause 6

Table A.1 (continued)

Incident response plan	Documented procedures for structured reaction in case of an incident, including a responsible, accountable, consulted and informed (RACI) matrix with contact details.	4.8
------------------------	--	---------------------

A.3 Security requirements specification

A.3.1 General

It is important to define adequate security requirements for an EUC. This process includes identifying and managing existing risks, defining the level of tolerable risk and results in a documentation of security requirements. The following process should be applied:

- decide for a threat modelling approach;
- identify and delimit the EUC;
- identify the specific assets of the EUC;
- identify relevant attacker types;
- identify threats endangering the identified assets;
- identify individual risk events;
- assess individual risk events;
- create security requirements;
- repeat assessment of individual risk events.

Details for each step are given in [4.3.2](#) to 4.3.10. See also [Annex B](#).

A.3.2 Threat modelling approach

A threat model helps to identify the assets of an EUC. Different threat modelling approaches are available:

- attacker-centric;
- system-centric;
- asset-centric.

NOTE Depending on the chosen approach, a different starting point is used but all will lead to the same results if done right.

A.3.3 Identify the specific assets of the EUC

[Figures A.1](#) and [A.2](#) give examples when defining assets for an EUC. [Figures A.1](#) and [A.2](#) show an EUC divided into different assets, such as safety functions or complementary functions, in lift and escalator context. These assets can include multiple sub-assets, e.g. the audio connection and the help call function being two emergency function assets.

Depending on the design, assets can be grouped into zones and connected with conduits. [Annex D](#) gives guidance for application of zones and conduits.

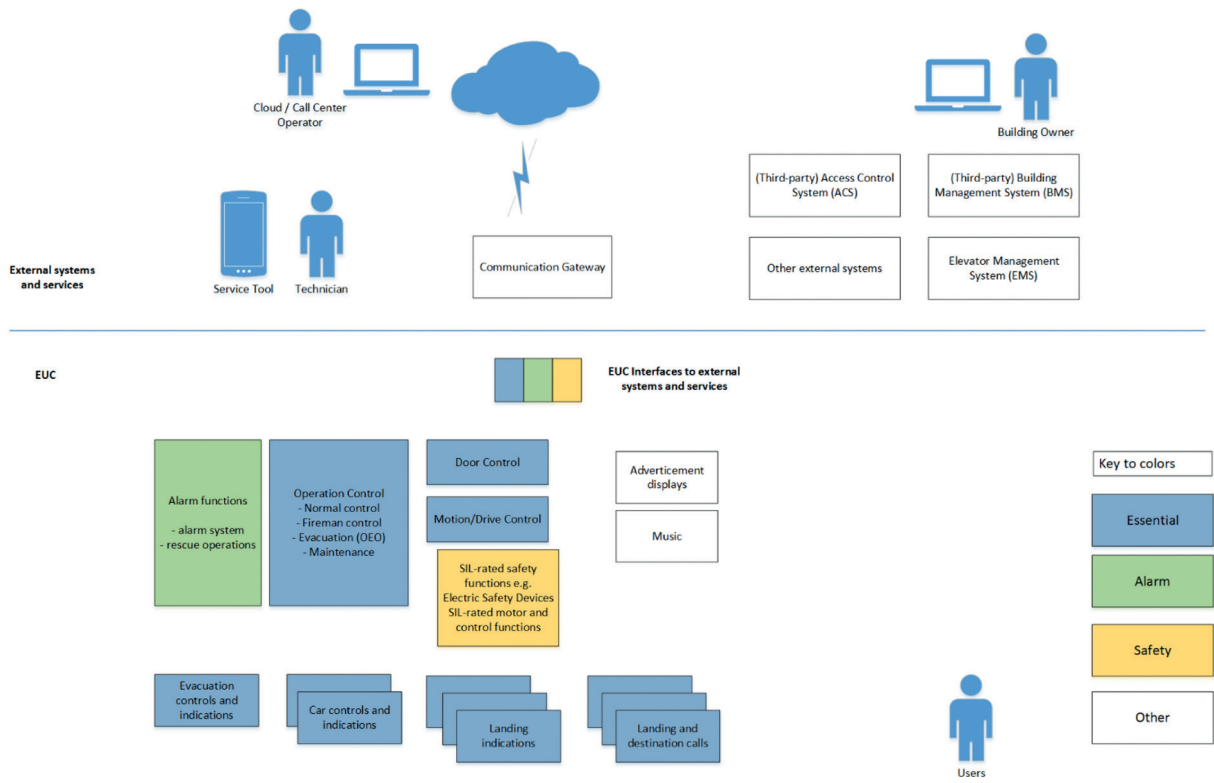


Figure A.1 — Example of assets of a lift system

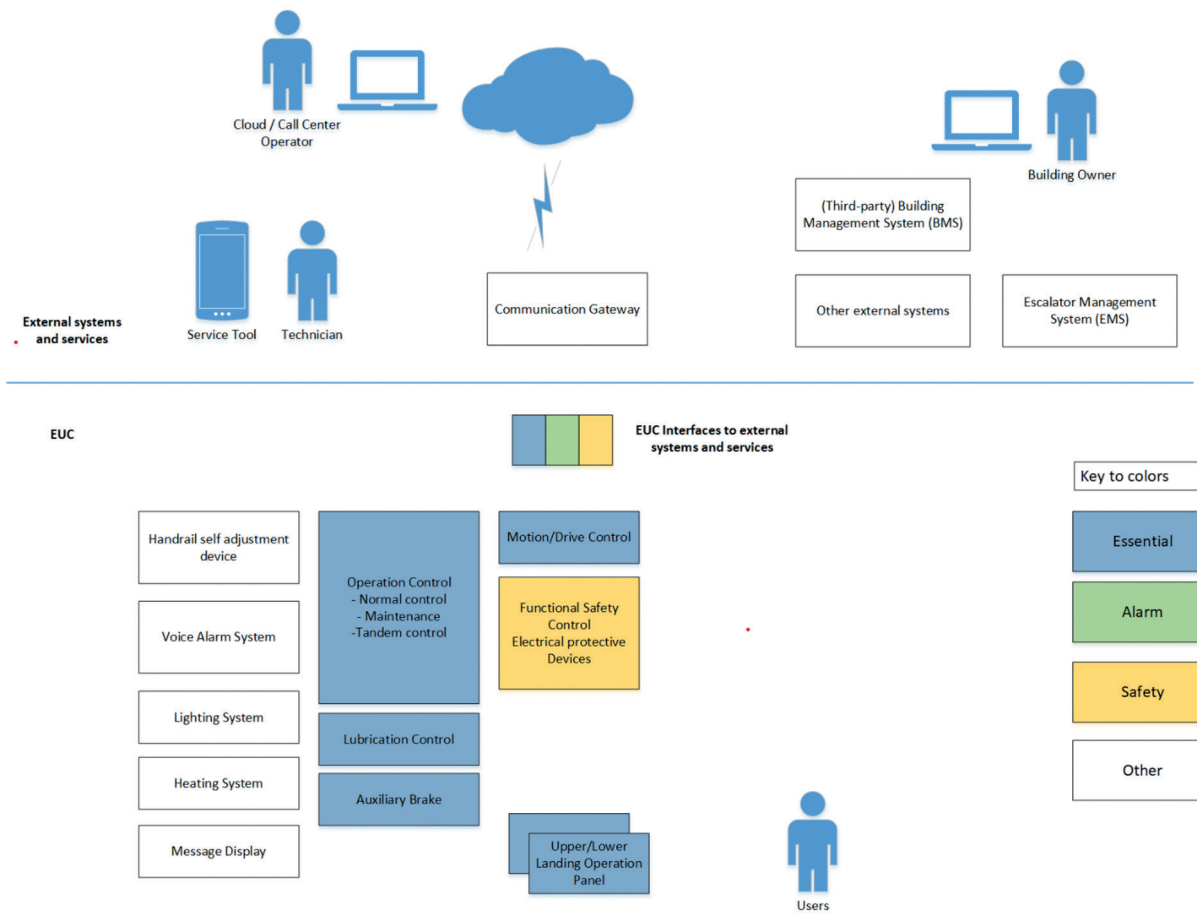


Figure A.2 — Example of assets of an escalator system

A.3.4 Identify relevant attacker types

The threat model and the risk analysis should start with identification of relevant attacker types.

An attacker can be an individual or organization that performs malicious activities to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset. These attackers range from script kiddies and hacktivists to cyber criminals and state sponsored attackers, each differing in their capabilities, intent/motivation and resources they have available to carry out the attack.

An attacker may also be an insider, e.g. someone from the development of the EUC.

The treatment of attack vectors can be complex. Depending on the attacker and attack type, the activity required for carrying out an attack can range from a simple reconnaissance consisting of identifying and exploiting a publicly known weak point in a target, to deliberate attempts to extract information (i.e. social engineering), and to a more sophisticated and planned activity including infiltration into manufacturing supply chain and product development.

For the purposes of this document, typical attackers have been taken into account. If attackers with immense resources (such as those that are state sponsored or big budget operations) are relevant, a dedicated risk analysis should be made.

The cybersecurity requirements specified in [Clause 5](#) are minimum requirements. Specialized building, structures, or use environment, e.g. government facilities, critical care facilities etc., may require that the application of the facility be considered to determine if higher levels of cybersecurity or complete isolation from the internet are required. For example, protection against cyber threats that could result

in a denial of lift service may be necessary. See note in 4.2 in IEC 62443-3-3:2013 for guidance on cyber security risk (threat) assessment.

Accessibility of the attacker to the EUC is another important aspect. Attacks that are carried out remotely have traditionally been the primary source of cyber-attacks. There are however cyber-attacks that leverage short range wireless communication such as WiFi and Bluetooth as well as those that require physical access to the EUC, such as access via the JTAG port.

A.3.5 Application examples of compensating countermeasures

A.3.5.1 Possible measures

Measures defined in EUC application standards can be taken into account for the threat model required in [4.3.2](#). Such measures can include but are not limited to:

- physical access restriction:
- emergency unlocking means (ISO 8100-1:2019 5.12.1.5.2.2);
- locked cabinet or inspection door (ISO 8100-1:2019 5.2.6.4.3.4, 5.2.6.4.4.1, 5.12.1.5.2.2);
- failure exclusion:
- parallel connection to electric safety device (ISO 8100-1:2019 5.11.2.1.2);
- system integrity:
- reliability of remote alarm system in accordance with EN 81-28 (ISO 8100-1:2019 5.12.3).

A.3.5.2 Safety chain tap

The following example illustrates how to apply compensating countermeasures as defined in [5.6.3](#).

ISO 8100-1:2019, 5.11.2.1.2, states: “Apart from exceptions permitted in this document (see 5.12.1.4, 5.12.1.5, 5.12.1.6 and 5.12.1.8), no electric equipment shall be connected in parallel with an electric safety device. Connections to different points of the electric safety chain are only permitted for gathering information. The devices used for that purpose shall fulfil the requirements for safety circuits according to 5.11.2.3.2 and 5.11.2.3.3.”

Typically, such connections to different points of the electric safety chain are made using resistors or safety relays whose construction ensure that the state of the electric safety chain cannot be influenced by external factors.

A safety chain also requires a power supply. Other requirements of ISO 8100-1 not listed here apply to such a power supply. Typically, such a power supply can be controlled by the normal means in order to minimize power consumption when the safety chain is not needed.

Depending on the foundational requirement considered, a safety chain built following the requirements of ISO 8100-1 might or might not fulfil the required security level.

[Table A.3](#) shows examples of applicability of the countermeasures defined in ISO 8100-1:2019, 5.11.2.1.2, for the considered foundational requirement.

Table A.3 — Example of applicability of countermeasures to foundational requirements

Foundational requirement (FR)	SL	Safety chain taps
FR 1 – Identification and authentication control (IAC)	3	Applicable
FR 2 – Use control (UC)	2	Applicable
FR 3 – System integrity (SI)	2	Applicable

Table A.3 (continued)

Foundational requirement (FR)	SL	Safety chain taps
FR 4 – Data confidentiality	2	Not applicable
FR 5 – Restricted data flow (RDF)	1	Applicable
FR 6 – Timely response to events (TRE)	1	Not relevant
FR 7 – Resource availability (RA)	2	Applicable

A.3.5.3 Alarm function

A risk assessment for a building might demonstrate the need for a higher security level than the one defined for typical lifts in this document. For example, the requirements for confidentiality or availability might be higher.

A typical lift might still fulfil the higher security level if the countermeasures are provided by the building. As an example, the building could provide an on-site permanently staffed rescue service, and the alarm function can be installed between the lift and the on-site rescue service in a way to ensure the confidentiality required by the building security.

A.3.6 Identify threats endangering the identified assets

Threats can be categorized as:

- deliberate or
- accidental.

Security threats for the EUC include, but are not limited to:

- exploitation of vulnerabilities due to software errors;
- malware, such as worms and viruses via the network, transportable media (e.g. USB memory sticks), and via temporary connections (e.g. service tools);
- unauthorized access;
- unauthorized actions by employees or by others;
- unintended employee actions;
- denial of service attacks;
- sabotage/vandalism.

A.3.7 Individual risk events identification

It should be defined how the threats according to 4.3.6 can occur by identifying individual risk events for every defined asset, which can be assessed. The level of acceptable risk for the EUC should be defined during this step. When evaluating the level of acceptable risk, the list of assets and the impact to the assets should be taken into account.

A.3.8 Assess individual risk events

The previously identified risk events should be assessed performing a risk assessment. A risk assessment is an iterative process and might have to be repeated several times during the development phase of the EUC. The risk assessment should be matured as the design of the EUC progresses. It is mandatory to repeat the risk assessment at least at every major change of the EUC or threat landscape.

Therefore, documentation is needed for reproducible results. Following questions can be used when developing the documentation, but not limiting into them:

- how was the risk assessment done?
- what were the assumptions?
- what was the level of accepted risk?

The initial risk assessment should be performed under the assumption that no countermeasures are in place. The following points should be taken into account when performing the initial risk assessment:

- the likelihood of a risk event is always a combination of intention/motivation to start an attack, the necessary skill and resources, and the probability that a started attack actually affects the assets to be protected;
- the occurrence of a risk event can have an impact on one or multiple risk types;
- the likelihood and the one or multiple identified severity levels have to be combined in order to get the unmitigated level of risk;
- the determined level of risk has to be compared to the accepted level of risk;
- if the determined level of risk is above the accepted level, define security requirements in order to manage this risk event.

A.3.9 Create security requirements

After the initial risk assessment, meaningful countermeasures should be chosen in order to mitigate the assessed risks exceeding the previously defined acceptable level of risk. Best practice when defining countermeasures is the so called “defense in depth” approach. Countermeasures should not rely on a single line of defence but utilize multiple layers of protection. If one line of defence breaks, the asset is still defended by at least another layer. Compensating countermeasures, such as physical access control or detective controls, may also be used to satisfy one or more security requirements.

A.3.10 Repeat assessment of individual risk events

The initial risk assessment should be repeated with the chosen countermeasures. This process should be repeated until the residual risk is below the accepted risk.

A.4 Secure by design

When designing a product, it is important to use a process which ensures the product is secure by design.

The goal of the design phase is the development of the system’s architecture. In this phase, all decisions regarding the high-level design choices and key components to be used are made. Furthermore, during this development of the architecture, the product’s complete functionality should be outlined to the degree necessary in order to achieve an architecture which fits to the required functionality. This outline could, for example, consist of the involved entities, the resulting flow of data and important security or non-security properties already assignable.

Due to the far-reaching effects of the choices made during the design phase, this phase is especially prone to the introduction of security vulnerabilities. Flaws in the developed architecture might lead directly or indirectly to vulnerabilities which might be hard to identify at this high-level stage, since they might be very specific or only recognizable on a much lower level. Fixing these security issues is most efficient if identified as early as possible, preferably during the design phase. If security flaws are only discovered in later phases, such as during testing or operations, it becomes increasingly complex and expensive to deal with them. It is therefore very important to try to detect the vulnerabilities

already in the design phase and use industry standard best practices for reducing the attack surface exposed.

Best practices include:

- the principle of least privilege, meaning a process or a user should by design not have higher privileges than necessary for the fulfillment of its task.
- attack surface identification and minimization.
- modular design methodology to reduce the impact of security threats.
- defence in depth, meaning that no risk should be mitigated by a single measure but by a set of layered measures still effective if one of the individual measures fail (also described in the requirements phase).
- restricting the access of a user, interfacing system or task to just the data which is required for the respective functionality.
- preferring simple, proven in use concepts or components over unnecessary complex, proprietary or inadequately tested ones.
- performing security design reviews on a regular basis in order to detect security requirements that are not yet addressed by the present design and check whether the system's current architecture is in conformity with the best practices.

For further information on security best practices, see Bibliography.

A.5 Secure implementation

A.5.1 Implementation activities and reviews

Secure implementation refers to processes and guidelines that ensure products are being developed securely. Suppliers of EUC are required to establish such processes and guidelines, as called out in IEC 62443-4-1:2018 Practice 4, SI-1: Security reviews and SI-2: Secure coding standards.

At a minimum the following main attributes associated with secure implementation should include:

- the use of secure coding guidelines;
- the use of static analysis tools;
- unit testing of critical functions;
- analysis of third party and open source software.

In addition to good coding practices for different languages, the guidelines should list potentially exploitable coding constructs or designs that should not be used, and these should be from real world examples. Typically, they should also include a list of banned/deprecated functions.

At a minimum, code that meets the following criteria should be analysed using static code analysis tools:

- code listening on or connecting to a network that may be connected outside the trusted/security zone of the device, system or application under consideration.
- code with prior vulnerabilities identified.
- code executing with high privilege (for example system, administrator, root). Code running with higher privileges should have valid reasons for doing so.

- security related code module (for example, authentication, authorization, cryptographic and firewall code).
- code that parses data structures from external sources
- code obtained from external sources
- setup code that set access controls or handles encryption keys or passwords.

All risks identified by the static analysis tool in violation of the coding standard should be mitigated unless the risk can be shown to be not relevant.

A best practice is to carry out continuous source code analysis during the development process, rather than towards the end of the code development phase. When developers check-in the code, the code can be automatically analysed for any possible security issues.

A.5.2 Integration of system components

Lifts and escalators are designed to operate as a system. The lift system manufacturer and/or the installation company may be integrating multiple components as part of the system. Therefore, it is important to consider the components in the context of how they are specified in the system integration in order to derive requirements, implement the design, and verify security measures.

As part of the component design implementation, the manufacturer should provide documentation to capture the responsibilities between the component developer and the system integrator. Conditions for secure use of component should be documented.

As part of the system implementation, the integrator should follow the security requirements as identified by the component manufacturer.

- Conditions that the component expects as it is applied in the system should be documented
- Process level requirements to ensure security (such as key or certificate management) should be documented
- Component assumptions should be considered in the system integration design as security requirement (this may be necessary to insure that stated security of the component is intact).

EXAMPLE In order to fulfil a specific SL, for example, the component may require specific security requirements to be implemented at a system level.

A.6 Security validation

A.6.1 General

In addition to the normal testing and validation processes which are a part of product development, cybersecurity verification and test plans are part of a formalized process in the product verification phase. The following key activities related to security are important.

A.6.2 Dynamic analysis

Dynamic analysis should be performed on the application to identify any memory corruption, race conditions, user privilege issues and any other critical security problems.

A.6.3 Fuzz testing

Fuzz testing should be performed on all components that process data originating external to the security zone or component.

A fuzz testing plan should be created documenting the fuzz testing that will be done. The plan should include a list of all components that will be fuzzed, a description of how the fuzzing will be done, whether smart fuzzing or dumb fuzzing will be done, and the pass/fail criteria for the tests.

A.6.4 Penetration testing

In addition to the use of fuzz testing tools, various penetration testing tools are also recommended for use during testing. The test plan should have specific line items relating to the use of penetration testing tools.

Independent (third party) penetration testing should be considered on a periodic basis.

A.6.5 Verify countermeasures of threat modelling findings are properly implemented

Abuse case tests and known vulnerability testing should be performed on all components and attempt should be made to exploit all threats identified in the threat model that have been mitigated.

Any attack surface not captured in threat modelling process should be identified. The results should be documented.

The effectiveness of the implemented security countermeasures should be verified through testing and the risk assessment should be updated based on test results.

A.6.6 Independent third-party analysis

Depending on the cybersecurity process and skill maturity of the manufacturer, an independent third-party security vulnerability analysis and penetration testing should be carried out. This is specifically recommended for zones and conduits with a security target level of 2 or more.

A.6.7 Red teaming and blue teaming

Red teaming and blue teaming should be considered as appropriate testing methods to qualify the entire system security. See Bibliography.

A.7 Security management during product life cycle

A.7.1 Management of security-related issues

Threats to equipment operation require measures such as keeping track of all exposed hardware and software, monitoring of the installations, and response plans.

Evaluating the current risk of installations requires knowledge about all components that are possibly exposed to an attacker. This asset inventory includes hardware as well as software.

- Keep inventory and version control of hardware/software in use.
- Continuously monitor vulnerability databases and field issues (DM-2).
- If a vulnerability in a hardware or software asset is detected, it is necessary to analyse if the vulnerability has any impact to the asset. (DM-2, DM-3).

If assets are affected by vulnerabilities, a further process for fixing the issue by either updating, replacing, mitigating or accepting the risk, for this vulnerability should be implemented. It would be advisable to use a scoring system to prioritize and assess any identified security issue.

Written procedures, an incident response plan, should be available to execute the necessary next steps in case of an incident. The response plan should contain the necessary information to deal with all kinds

of conceivable incidents and is highly dependent on the specific assets. At a minimum the response plan should contain the following:

- contact details, responsibilities;
- asset components;
- place of installation, if applicable;
- predefined procedures (steps to take).

Examples of incidents include:

- abnormal network traffic;
- unexpected shutdown due to a security breach;
- defacement of a lift display at the landing.

The manufacturer and maintenance provider should develop emergency procedures regarding the before mentioned and additional requirements. A process should be in place to properly maintain the response plans in case of changes or updates.

For example, the forum of incident response and security teams (FIRST, www.first.org) defines both PSIRT and CSIRT as two good practices for manufacturers and maintenance providers to cover both incident response plan aspects of their product when delivered.

A.7.2 Security update management

Once systems are in place to track, discover, and receive potential vulnerabilities, it is the responsibility of the equipment manufacturer to have an effective security update process in place. The manufacturer should verify that the vulnerability exists as well as assess the potential security risks to the customer based on the intended use case of the equipment. Furthermore, the equipment manufacturer should have processes in place in order to inform customers about security vulnerabilities in their installed products and instructions and means to address them. Since the end customer may not be the equipment service provider, the lift equipment manufacturer should also have means for the lift service company to apply any patches or fixes. See [Table A.4](#) for the roles of manufacturer, service provider and component owner.

Table A.4 — Security documentation

IEC 62443-4-1:2018 practice 7		Manufacturer	Service Provider	Component Owner
SUM-1	Security update qualification	Performs		
SUM-2	Security update documentation	Delivers		Reacts
SUM-3	Dependent component or operating system security update documentation	Delivers		Reacts
SUM-4	Security update delivery	Delivers	Performs	
SUM-5	Timely delivery of security patches	Performs		
4.7.2.1 in this document	Check on implementation of security updates for high impact scenarios	Performs		Reacts

A.7.2.1 Check on security patching

If the security vulnerability has a high impact as determined by a product risk analysis, then the manufacturer should ensure that there is follow up communications with the customer to verify that the security vulnerability has been applied.

A.7.2.2 Considerations regarding delivery of security patches to lifts, escalators, and moving walkways

It is important to adhere to the applicable lift, escalator, and moving walkway code requirements when delivering a security update. The type of component and its function in the system may make it impossible to automatically deliver a security update. In this case, alternate means should be provided to insure that the update can be applied, such as instructions to download and apply the patch with available service equipment, shipment of software in a secured physical device, or replacement of the component having a security vulnerability with a component that contains the security patch.

A.8 Decommissioning activities

The manufacturer and/or system provider should also consider how to handle the decommissioning of the lift or escalator system since sensitive information might be stored on some components (IDs, credentials, parameter sets, certificates, etc.) which might be used maliciously or provide insight into the asset and other linked assets if disclosed. Erasing the information or destroying the asset physically might be necessary. Decommissioning of an asset should be reflected in the asset inventory.

Annex B (informative)

Additional information on how to apply the general method of risk assessments

B.1 Additional information on security risk assessments

This annex provides additional information on how to apply the general method of risk assessments mentioned in [Annex A](#).

It might be necessary to adjust the normative part of this document in order to fit to a specific product by either

- extending the risk assessment by additional risks (and therefore possibly additional countermeasures);
- extending the risk assessment by additional assets (and therefore possibly additional risks);
- modifying the functionality-grouping assumed in this document;
- or by deviating from given requirements if they are not applicable or it can be shown that their fulfilment is not necessary in a certain risk context.

Since there is no proven in-use ecosystem of security methods, threat catalogues and best practices specifically for the lifts, escalators and moving walks industry yet, this annex aims to provide industry specific guidance.

When assessing security risks for lifts, escalators or moving walks the following general things should be considered.

- While the minimum security requirements are defined in [Table 2](#), the level of acceptable risk in other cases has to be agreed upon with the vested stakeholders. This level depends on legal aspects, the organization, the intended use case of the EUC and (local) societal values.
- In addition to risk assessments according to functional safety standards like ISO 14798, multiple industry specific aspects of security risk impact have to be considered. An example of a possible system of risk types can be found in [Table B.1](#).
- It is advisable to create a system of risk ratings which allows the comparison of different risk types.
- In security risk assessment, quantitative assessment of risk probability is often impossible. A qualitative approach is used instead. An example of qualitative rating of risk probabilities based on adversary capability and intent and system vulnerabilities is given in [Table B.2](#).
- Every risk reduction measure is a trade-off between costs (both unit costs and effort) and security benefit. For this reason, protection against an unrealistic threat level is neither necessary nor economically reasonable. The implementation of unnecessary risk reduction measures might even be counterproductive: Risk reduction measures often have an impact on the usability of a product, legitimate end-users might try to bypass/disable them if they are too inconvenient, and every risk reduction measure might also introduce additional vulnerabilities on its own. In any case, the occurrence of a risk event must not result in any harm of persons due to negligence.
- Security is not a subset of functional safety and a security risk assessment should therefore not be carried out under the responsibility of functional safety personnel. Functional safety and security are different domains and require different approaches and knowledge. For example,

the risk assessment approach and the necessary mindset are fundamentally different: Statistical negligibility of double/multiple faults vs. series of targeted actions following an attack vector, random (unmotivated) faults vs. intelligent threat sources, and likelihood as a single value vs. likelihood as the combination of multiple and often soft and hard to estimate factors are just a few of the core differences.

- A diverse team is beneficial to utilize different experiences and different points of view. It is suggested to include at least people with a functional safety, production, installation, and maintenance background.
- Possible threat actors might differ significantly based on the specific product and its threat landscape, based e.g. on the product specific use case, the site of the installation, the expected passengers and security measures expected in the environment of the installation.

Table B.1 — Example of mapping severity levels of different risk types

Level of severity	Risk type		
	Impact on safety, system, or environment	Impact on service availability (to users)	Impact on information (to operator)
1 - High	Death, system loss, or severe environmental damage	Not applicable	Not applicable
2 - Medium	Severe injury or major system or environmental damage	Not applicable	Not applicable
3 - Low	Minor injury or minor system damage	Service disruption (e.g lifts out of service when no alternate means of transport or loss of access control)	Data integrity compromised (e.g. lift management system data tampered with)
4 - Negligible	Does not result in injury or system or environmental damage	Minor service disruption (e.g. transport capacity reduced)	Loss of non-critical data (e.g. lift management system data)

Table B.2 — Example of probability levels

Level of probability	Probability per unit per life-time	Description of adversary capability and intent vs. system vulnerability
A — Highly probable	Likely to occur frequently in the life cycle	System is exposed over the network and security controls are not implemented and not planned; exploitable by a casual attacker with limited resources and expertise.
B — Probable	Likely to occur several times in the life cycle	System is exposed over the network, minimal security controls are implemented and minimally effective; exploit requires low resources, expertise, and motivation.
C — Occasional	Likely to occur at least once in the life cycle	System is exposed over the network, security controls are partially implemented and somewhat effective; exploit requires moderate resources, some lift and escalator system specific skills and moderate motivation.

Table B.2 (continued)

Level of probability	Probability per unit per life-time	Description of adversary capability and intent vs. system vulnerability
D — Remote	Unlikely, but may possibly occur in the life cycle	System is exposed over the network, security controls are mostly implemented and effective; exploit requires significant resources, lift or escalator system specific skills and high motivation.
E — Improbable	Very unlikely to occur in the life cycle	System is exposed over the network, security controls are fully implemented and effective; exploitation requires very sophisticated level of expertise, significant resources, high motivation and coordination.
F — Highly improbable	Probability cannot be distinguished from zero	No concern, security controls or other measures fully implemented, assessed, and effective.

NOTE If the system is operated in a closed network or there are other compensating countermeasures in place, the probability can be considered to be lower.

After the probability and severity of risk have been determined, the risks can be grouped into a risk matrix (see example from [Table B.3](#)). The resulting risk level will indicate whether the risk is acceptable without action or whether additional countermeasures or mitigations are required.

As described in [A.3.8](#) and [A.3.10](#), the risk assessment should be repeated after the countermeasures have been defined.

Table B.3 — Example of 6 × 4 risk matrix

Level of probability	Level of severity			
	1 - High	2 - Medium	3 - Low	4 - Negligible
A - Highly probable	High	High	High	Moderate
B - Probable	High	High	High	Moderate
C - Occasional	High	High	Moderate	Low
D - Remote	High	Moderate	Moderate	Low
E - Improbable	Moderate	Moderate	Low	Low
F - Highly improbable	Low	Low	Low	Low

B.2 Further guidance

Since there is no ready to use method for assessing security risks for lifts, escalators and moving walks generic standards have to be used in conjunction with lift specific expertise.

When conducting a security risk assessment the following provide valuable input and can be considered:

- [Annex D](#), Guidance for application of zones and conduits;
- IEC 62443-3-2:2020 describes a process of partitioning the EUC into zones and conduits, assessing risk for each zone and conduit, and establishing the target security level (SL-T) for each zone and conduit;
- ISO 27005:2018 describes the general activities which are necessary in order to implement a risk assessment and risk treatment process without prescribing specific methods;
- NIST SP 800-30 describes a mature risk assessment approach which is proven in use by various industries in its pure or some adapted form.

Additional input for possible threats can be found in several documents listing possible threats, the most common type of attacks or typical attack patterns. These documents are kept up-to-date and are distributed by several relevant organizations. Documents that can be considered include:

- OWASP Top 10 states the most relevant types of risks to web applications. Although lifts are a very different kind of product than a web application, all of these risks might apply to lift systems nonetheless (think of configuration GUIs or diagnosis interfaces);
- OWASP API Top 10 contains a similar list especially targeted towards the most common types of risk regarding APIs;
- OWASP IoT Top 10
- CWE Top 25 Most Dangerous Software Weaknesses
- BSI Top 10 gives a list of the top 10 threats to IACS and as well as possible countermeasures;
- CAPEC provides a list of attack mechanisms and attack patterns at various levels of abstraction.

Annex C (informative)

List of Security Practices

The [Table C.1](#) gives an overview of the applicable requirement as listed in [Clause 4](#). Clauses where this document specifies additional requirements in addition to the relevant IEC 62443 clause are marked “y” in the rightmost column.

Table C.1 — List of Security Practices

No	Practice	Clause in this document	Requirement number	Requirement name	Additional requirements
1	Security Management	4.2.1	SM-1	Development process	no
		4.2.2	SM-2	Identification of responsibilities	no
		4.2.3	SM-3	Identification of applicability	no
		4.2.4	SM-4	Security expertise	yes
		4.2.5	SM-5	Process scoping	no
		4.2.6	SM-6	File integrity	yes
		4.2.7	SM-7	Development environment security	no
		4.2.8	SM-8	Controls for private keys	no
		4.2.9	SM-9	Security requirements for externally provided components	yes
		4.2.10	SM-10	Custom developed components from third-party suppliers	no
		4.2.11	SM-11	Assessing and addressing security-related issues	no
		4.2.12	SM-12	Process verification	no
		4.2.13	SM-13	Continuous improvement	yes
2	Specification of security requirements	4.3.1	SR-1	Product security context	yes
		4.3.2	SR-2	Threat model	yes
		4.3.3	SR-3	Product security requirements	no
		4.3.4	SR-4	Product security requirements content	no
		4.3.5	SR-5	Security requirements review	no
3	Secure by design	4.4.1	SD-1	Secure design principles	no
		4.4.2	SD-2	Defence in depth design	no
		4.4.3	SD-3	Security design review	no
		4.4.5	SD-4	Secure design best practices	no
4	Secure implementation	4.5.1	SI-1	Security implementation review	no
		4.5.2	SI-2	Secure coding standards	no

Table C.1 (continued)

No	Practice	Clause in this document	Requirement number	Requirement name	Additional requirements
5	Security verification and validation testing	4.6.1	SVV-1	Security requirements testing	no
		4.6.2	SVV-2	Threat mitigation testing	no
		4.6.3	SVV-3	Vulnerability testing	no
		4.6.4	SVV-4	Penetration testing	no
		4.6.5	SVV-5	Independence of testers	no
6	Management of security-related issues	4.7.1	DM-1	Receiving notifications of security-related issues	no
		4.7.2	DM-2	Reviewing security-related issues	no
		4.7.3	DM-3	Assessing security-related issues	no
		4.7.4	DM-4	Addressing security-related issues	yes
		4.7.5	DM-5	Disclosing security-related issues	no
		4.7.6	DM-6	Periodic review of security defect management practice	no
7	Security update management	4.8.1	SUM-1	Security update qualification	no
		4.8.2	SUM-2	Security update documentation	yes
		4.8.3	SUM-3	Dependent component or operating system security update documentation	no
		4.8.4	SUM-4	Security update delivery	yes
		4.8.5	SUM-5	Timely delivery of security patches	yes
8	Security guidelines	4.9.1	SG-1	Product defence in depth	yes
		4.9.2	SG-2	Defence in depth measures expected in the environment	yes
		4.9.3	SG-3	Security hardening guidelines	yes
		4.9.4	SG-4	Secure disposal guidelines	yes
		4.9.5	SG-5	Secure operation guidelines	yes
		4.9.6	SG-6	Account management guidelines	yes
		4.9.7	SG-7	Documentation review	no

Normen-Download-Beuth-VFA-Interliff-e. V.-KdNr. 6363432-ID.9MEKVIKOCNIP90LXJPEW5SLM6.1-2021-10-11 16:25:18

Annex D (informative)

Guidance for application of zones and conduits

A zone is a grouping of cyber assets that, for each foundational requirement, share the same security level (SL), whereas a conduit consists of assets dedicated exclusively for communication and which share the same security level for each foundational requirement. For the purposes of this document, each zone can include sub-zones, conduits should not have sub-conduits. Zones and sub-zones can have multiple conduits to communicate with each other.

NOTE For additional information on zones and conduits, see IEC 62443-3-2:2020.

Security level for each foundational requirement is defined by taking the highest security level of each foundational requirement defined for functions within that zone.

Functions located within zones Z1 and Z2 in the example system shown in [Figure D.1](#) should use the security level vector defined in [Table D.1](#), column Z1&Z2. Since the Safety component has the highest security level vector requirements for each FR, all assets in the same zone should follow the same also for Essential and Alarm domains.

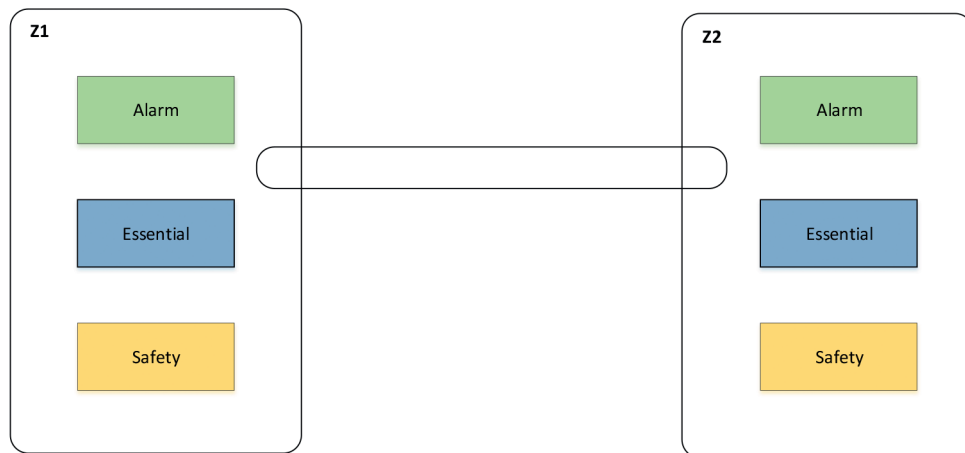


Figure D.1 — Example showing two zones and a conduit connecting them

Table D.1 — Security Level vector example for system in [Figure D.1](#)

Foundational requirement (FR)	Security Level Vector			
	Alarm	Essential	Safety	Z1&Z2
FR 1 – Identification and authentication control (IAC)	2	2	3	3
FR 2 – Use control (UC)	2	2	2	2
FR 3 – System integrity (SI)	2	2	2	2
FR 4 – Data confidentiality	1	2	2	2
FR 5 – Restricted data flow (RDF)	1	1	1	1
FR 6 – Timely response to events (TRE)	1	1	1	1

Likewise, functions located within zones Z1a and Z2a in the example system shown in [Figure D.2](#) should use the security level vector defined in [Table D.2](#), column Z1a&Z2a. Following the same approach,

functions located within zones Z1b and Z2b should use the security level vector defined in column Z1b&Z2b. However, there are no minimum security level requirements for zones Z1 and Z2 as the Safety, Essential, and Alarm components are already protected by the countermeasures that meet the security level requirements for the corresponding sub-zones.

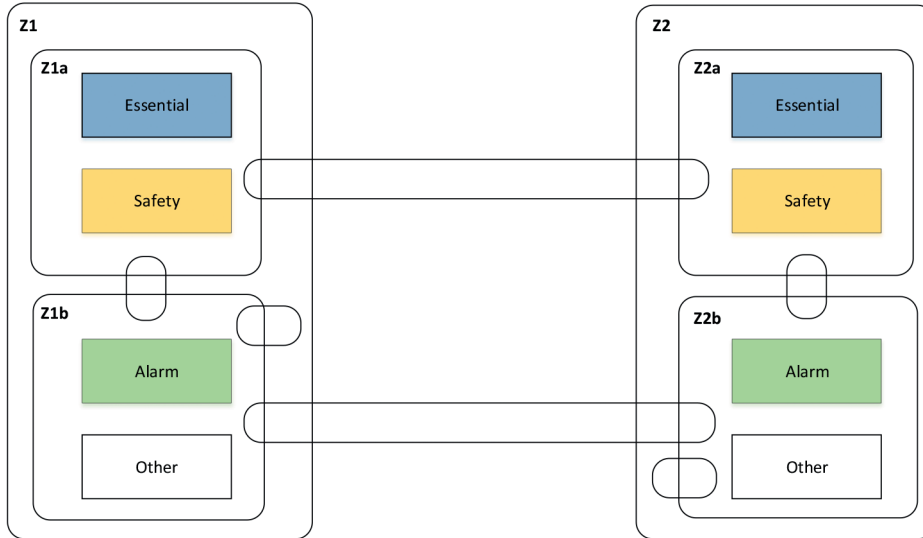


Figure D.2 — Example showing six zones and connecting conduits

Table D.2 — Security Level vector example for system in [Figure D.2](#)

Foundational requirement (FR)	Alarm	Essential	Safety	Z1a and Z2a	Z1b and Z2b
FR 1 – Identification and authentication control (IAC)	2	2	3	3	2
FR 2 – Use control (UC)	2	2	2	2	2
FR 3 – System integrity (SI)	2	2	2	2	2
FR 4 – Data confidentiality	1	2	2	2	1
FR 5 – Restricted data flow (RDF)	1	1	1	1	1
FR 6 – Timely response to events (TRE)	1	1	1	1	1
FR 7 – Resource availability (RA)	1	2	2	2	1

Example system shown in [Figure D.3](#) should use the security level vectors defined in [Table D.3](#). Column Z1b defines the security level vector for functions in zone Z1b. Functions located within zones Z1a and Z2a use the security level vector defined in column Z1a&Z2a. There will be no security level requirements for components from domain Other in Zones Z1 and Z2.

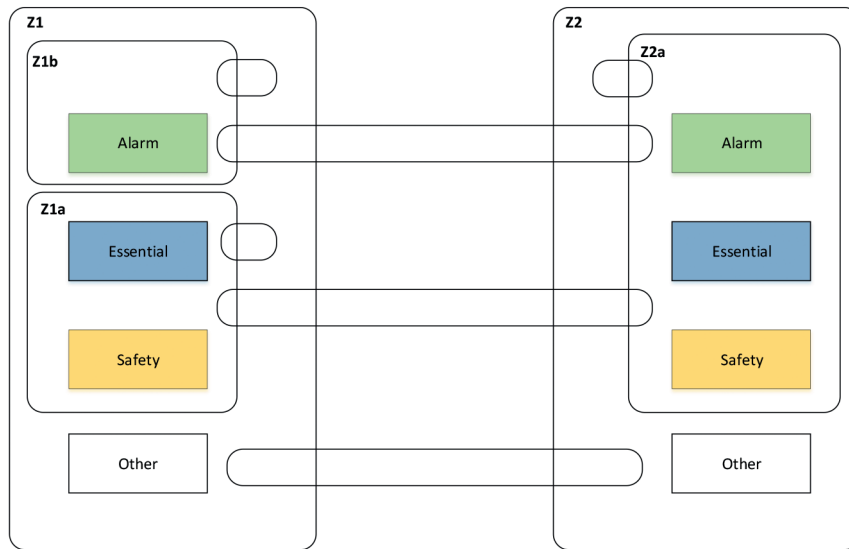


Figure D.3 — Example showing five zones and conduits connecting them

Table D.3 — Security Level vector example for system in [Figure D.3](#)

Foundational requirement (FR)	Alarm	Essential	Safety	Z1b	Z1a and Z2a
	FR 1 – Identification and authentication control (IAC)	2	2	3	2
FR 2 – Use control (UC)	2	2	2	2	2
FR 3 – System integrity (SI)	2	2	2	2	2
FR 4 – Data confidentiality	1	2	2	1	2
FR 5 – Restricted data flow (RDF)	1	1	1	1	1
FR 6 – Timely response to events (TRE)	1	1	1	1	1

Bibliography

- [1] 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*
- [2] ISO 27017:2015, *Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services*
- [3] ISO/IEC 27005:2018, *Information technology — Security techniques — Information security risk management*
- [4] IEC 62443-2-4, 2025, *Security for industrial automation and control systems - Part 2-4: Security program requirements for IACS service providers*
- [5] IEC Guide 120:2018, *Security aspects - Guidelines for their inclusion in publications*
- [6] EN 115-1:2017, *Safety of escalators and moving walks. Part 1: Construction and installation*
- [7] A17 1/CSA B44 - 2019, *Safety Code for Elevators and Escalators*
- [8] GB/T 7588.1 - 2020, *Safety rules for the construction and installation of lifts—Part 1:Passenger and goods passenger lifts*
- [9] CAPEC, <https://capec.mitre.org>
- [10] NIST SP 800-82 <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf>
- [11] NIST Computer security resource center, https://csrc.nist.gov/glossary/term/Red_Team_Blue_Team_Approach
- [12] BSI ICS SECURITY COMPENDIUM. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/ICS/ICS-Security_compendium.pdf?__blob=publicationFile&v=3ISO
- [13] TOP O.W.A.S.P., 10, 2017, https://owasp.org/www-project-top-ten/OWASP_Top_Ten_2017
- [14] NIST SP800-30, 2012, <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf>
- [15] MISRA C. <https://www.misra.org.uk/>
- [16] SEI CERT CODING STANDARDS. <https://wiki.sei.cmu.edu/confluence/display/seccode/SEI+CERT+Coding+Standards>
- [17] SECURE CODING PRACTICES-QUICK REFERENCE GUIDE O.W.A.S.P., Version 2.0, 2010, https://owasp.org/www-pdf-archive/OWASP_SCP_Quick_Reference_Guide_v2.pdf