DRAFT International Standard

ISO/DIS 8102-20

Electrical requirements for lifts, escalators and moving walks —

Part 20: Cybersecurity

Exigences électriques pour les ascenseurs, les escaliers mécaniques et les trottoirs roulants —

Partie 20: Cybersécurité

ICS: 91.140.90

ISO/TC **178**

Secretariat: **AFNOR**

Voting begins on:
2026-04-06

Voting terminates on:
2026-06-29

This document is circulated as received from the committee secretariat.

ISO/CEN PARALLEL PROCESSING

Reference number
ISO/DIS 8102-20:2026(en)

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

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*.

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

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

This document has been developed in response to market requirements and enhanced cybersecurity awareness. The state of the art cybersecurity standard for operational technology is the IEC 62443 series. This document addresses the requirements specific to lifts, escalators and moving walks when applying the IEC 62443 series. The term "lifts" includes:

— lifts for the transport of persons and goods;

— lifts for the transport of goods only;

— special lifts (lifting appliances) for the transport of persons and goods.

The fundamental principle of cybersecurity is a strong cybersecurity process lifecycle. This lifecycle 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 lifecycle 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, referred to in this document as "equipment under control (EUC)", designed in accordance with the ISO 8100 series, as well as the required information for use. It is also applicable with other lift, escalator and moving walk standards that specify similar requirements, and can be applied to EUC components or to other EUC-related equipment connected to the EUC.

This document specifies requirements related to cybersecurity in the following lifecycle steps:

— product development (process and product requirements);

— manufacturing;

— installation;

— operation and maintenance;

— decommissioning.

This document addresses EUC requirements relevant to the roles of product supplier and system integrator as shown in IEC 62443-4-1:2018, Figure 2.

This document does not address the role of asset owner as shown in IEC 62443-4-1:2018, Figure 2, but defines requirements for the information for use of the EUC which is relevant to the asset owner to achieve and maintain the security of the EUC.

This document is applicable to EUCs that are capable of connectivity to external systems such as building networks, cloud services, or service tools. The capability of connectivity can exist 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. External systems and services as such are out of the scope of this document.

This document does not apply to EUC that 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.

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*

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

3 Terms, definitions and abbreviated terms

3.1 Terms and definitions

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

ISO and IEC maintain terminology 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: In this document, the term "security" includes cybersecurity.

[SOURCE: IEC 62443-3-2:2020, 3.1.7, modified — Note 1 replaced.]

3.1.2
software
executable code and/or configuration parameters

Note 1 to entry: Both the change of the value of a configuration parameter as well as the change of executable code typically impact the behaviour of a component or a system.

3.1.3
software update
process of updating *software* (3.1.2)

3.1.4
software package
collection of *software* (3.1.2) and information necessary for the *software update* (3.1.3)

3.1.5
important function
function or capability belonging to the domains SIL-rated, essential or alarm

3.1.6
activation
step in the *software update* (3.1.3) when an executable code becomes executable on an EUC and/or configuration parameter(s) become active on an EUC

3.1.7
on-site
at the site of the EUC installation with physical access to the EUC

3.2 Abbreviated terms

CCSC	common component security constraint
DM	defect management
EDR	embedded device requirement
EUC	equipment under control
FR	foundational requirement
HDR	host device requirement
IACS	industrial automation and control systems
NDR	network device requirement
RACI	responsible, accountable, consulted and informed
RE	requirement enhancement
SAR	software application requirement
SD	secure design
SG	security guideline
SI	secure implementation
SIL	safety integrity level
SL	security level
SL-C	security level capability
SL-T	security level target
SM	security management
SR	security requirement
SUM	security update management
SVV	security verification and validation

4 Secure development lifecycle

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 lifecycle, Annex B for additional information on security risk assessment and Annex C for a list of security practices.

The secure development lifecycle covers the development of the initial product as well as the development of product updates including successive software updates. Software updates can include security, safety or other functional updates.

Change of a configuration parameter value shall be considered as a new software development if the impact to the behavior of the EUC or its components has not been evaluated earlier during the software development process.

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 cybersecurity, training programmes shall also include EUC-specific safety expertise.

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 means 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 to identify and manage the security risks of all externally provided components used 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.

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 utilization 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 lifecycle 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 Defense in depth design

The requirements of IEC 62443-4-1:2018, SD-2: Defense 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.

The information for use shall indicate the means to report security-related issues, including vulnerabilities.

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 to address security-related issues over the full life-cycle of the EUC.

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 means to obtain information on security updates.

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 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 to apply security patches.

4.9 Security guidelines

4.9.1 Product defense in depth

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

The information for use shall give an overview of the security defense in depth strategy to the extent required to maintain the security of the EUC.

4.9.2 Defense in depth measures expected in the environment

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

The information for use shall indicate the conditions for use of the EUC to achieve and maintain the security of 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 hardening the EUC during installation and maintenance.

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 EUC requirements

5.1 General

IEC 62443-3-3:2013 and IEC 62443-4-2:2019 are the reference security publications for the security requirements specified in this document. IEC 62443-3-3:2013 applies to the EUC and IEC 62443-4-2:2019 applies to the components of the EUC.

Software update of the EUC and its components shall comply with 5.9.

5.2 Foundational requirements

IEC/TS 62443-1-1:2009 defines seven FRs, which are applied to the EUC functions, as specified in 5.3 and 5.8. The FRs which apply to the EUC functions are applied to the EUC component(s) where the functions are implemented.

5.3 Domains of the EUC functions

Each of the EUC functions shall be classified into one of the domains of "SIL-rated", "Essential", "Alarm" or "Other". An EUC function belonging to the SIL-rated, essential or alarm function is called important function. Functions which do not belong to the mentioned domains are classified as "Other". The domains are described in Table 1.

Table 1 — Domains of the EUC functions

Domain	Description	
SIL-rated	Important function	SIL-rated control functions.
Essential		Functions that are required to ensure the availability of the EUC and its compliance to safety regulations, and which do not belong to SIL-rated or Alarm function domains.
Alarm		Functions used to verify entrapment, to call for help and to rescue passengers in case of entrapment.
Other	Additional functions not related to SIL-rated, essential or alarm domains.	

5.4 EUC security level requirements

The EUC shall provide the security measures defined in IEC 62443-3-3:2013, clauses 5 to 11.

For each EUC function of the domain "alarm", "essential" and "SIL-rated", these measures shall have at least SL-C required as specified in Table 2.

NOTE 1 For functions for domain "Other", see 7.1.

NOTE 2 The required SL-C is defined as a vector of SLs, with a separate SL specified for each of the seven FRs.

EUC components shall provide the security measures defined in IEC 62443-4-2:2019. If an EUC component is used to implement more than one EUC function, the highest SL-C required by these functions shall be applied to this component.

If a component is used to enable connectivity between an EUC function and equipment external to the EUC, it shall have a security level (SL) of at least the SL-C required for that EUC function.

Table 2 — Security level vectors for EUC function domains

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

NOTE 3 Table 2 can be presented in the vector format described in IEC 62443-3-3:2013, A.3.3, e.g. “SL-C(Essential) = {2 2 2 2 1 1 2}”.

NOTE 4 Networks used for domain SIL-rated, essential and alarm are considered control system networks as per IEC 62443-3-3:2013. Networks used for domain other are considered non-control system networks as per IEC 62443-3-3:2013.

5.5 Support of essential functions

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

The essential functions referenced in IEC 62443-4-2:2019, CCSC 1 are called important functions in this document, i.e. they are the functions of domains SIL-rated, essential and alarm as defined in 5.3.

Security measures shall not adversely affect the availability of the alarm function.

5.6 Compensating countermeasures

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

An EUC component is permitted not to fulfil the security level requirements as per 5.4 if this component is part of an EUC providing the compensating countermeasures ensuring that this EUC fulfils the SL-C required in 5.4.

In this case, the information for use of the EUC component (see 6.1) shall:

— indicate the security requirements that the component does not fulfil itself for achieving the expected security level vector; and

— indicate the need for compensating countermeasures in the EUC in which the component can be integrated.

NOTE Examples of application specific compensating countermeasures are given in A.3.9.

5.7 Least privilege

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

5.8 Software development process

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

5.9 Software Updates

5.9.1 General

This sub-clause defines technical requirements for the software update steps. Where there are no dependencies, the steps may be in arbitrary order or may be combined.

Steps of a software update can be carried out either on-site or not on-site, by manual or automatic means.

An example of software update sequence is described in Annex E.

5.9.2 Initiation

The initiation of a software update may be manual or automatic.

If automatic initiation of the software update is possible, the EUC shall have the capability to prevent the initiation of the software update.

5.9.3 Delivery

The delivery of a software package may be manual or automatic. Instructions necessary for the software update may be delivered separately from the software itself.

Automatic delivery shall not impede any important function of the EUC.

5.9.4 Protection of persons

5.9.4.1 Lifts

If the software update can cause entrapment or can lead to a hazardous situation, activation and validation shall not start unless the car is unoccupied and stopped with doors closed.

NOTE Protection for maintenance operations as specified in ISO/FDIS 8100-1 [1] is one example of means to ensure that the car is unoccupied and the lift it is stopped with doors closed.

5.9.4.2 Escalators and moving walks

If the software update can lead to a hazardous situation:

— activation and validation shall not start unless the EUC is stopped; and

— the information for use shall require the use of devices to prevent access to the escalator or moving walk during the activation and validation.

NOTE Means to stop the escalator or moving walk and devices to prevent access as specified in ISO 8103-1 [2] are examples of such means.

5.9.5 Compatibility check

5.9.5.1 General

There shall be a capability to check the compatibility of the new software package against the current EUC configuration. The information of the current EUC configuration required for the compatibility check can include identification of hardware revisions, software revisions, parameters, interfaces and input-output mappings.

5.9.5.2 Automatic compatibility check

In case of automatic compatibility check, there shall be one or more automatic functions to check the compatibility of the new software package before activation. These functions may be implemented in the EUC, in external systems, or in both.

5.9.5.3 Manual compatibility check

In case of manual compatibility check, the EUC shall provide capability to access all information required for the compatibility check. In case of on-site manual compatibility check, this information shall be available in human-readable form, either by a built-in system or by an external tool. If this external tool is a special tool, it shall be provided with the EUC.

NOTE A generic portable device with standard interfaces, such as a laptop, tablet or phone, with freely available application, is not considered as a special tool.

5.9.6 Activation

The automatic activation of the new software shall only be possible after a successful compatibility check.

In case of manual activation of the new software, the information for use shall indicate that the manual activation is only performed after a successful compatibility check.

5.9.7 Validation

5.9.7.1 General

After activation, the important functions of the EUC directly or indirectly affected by the new software shall be automatically or manually validated unless failure of these important functions can be excluded. In addition, the availability of the basic functions of the EUC shall be checked automatically or manually.

Validation shall be manual in the following cases:

— If the validation requires an unoccupied car and no means of automatically ensuring that the car is unoccupied is available;

— If the validation depends on building requirements, and a building requirements cannot be automatically verified (e.g. evacuation floor, restricted access);

— If validation of the software can cause a dangerous failure mode which cannot be automatically mitigated;

— If validation of the software requires operation of the actuating means and this operation cannot be automatically simulated or verified.

5.9.7.2 Automatic validation

In case of automatic validation of important functions of the EUC, there shall be one or more automatic functions to check the correct operation of the important functions of the EUC affected by the software and for which the failure cannot be excluded.

For other functions or capabilities of the EUC which can impact the availability of the EUC, the availability of the EUC shall be checked automatically.

Automatic validation should include automated tests where operation of the EUC is compared to the acceptance criteria.

The EUC shall provide capability to access the result of validation and availability check in human-readable form, either by a built-in system or by an external tool. If this external tool is a special tool, it shall be provided with the EUC.

NOTE A generic portable device, such as a laptop, tablet or phone, with freely available application, is not considered as a special tool.

5.9.7.3 Manual validation

In case of manual validation, the information for use shall specify

— instructions how to check the correct operation of the important functions of the EUC affected by the software and for which the failure cannot be excluded;

— instructions how to check the availability of the basic functions of the EUC;

— the need for additional protective measures, if there is a risk of entrapment or hazardous situation during the manual validation.

5.9.8 Completion of software update

In the case the automatic validation fails for an important function that can cause entrapment or can lead to a hazardous situation of the EUC, the means described in 5.9.4 shall remain active. In the case the automatic validation is successful, the means described in 5.9.4 may be released. In the case of manual validation fails for an important function that can cause entrapment or can lead to a hazardous situation of the EUC, information for use shall require the means described in 5.9.4 to remain active. In the case the manual validation is successful, the information of use may permit the release of the means described in 5.9.4.

5.9.9 Recovery from validation failure

Recovery from a validation failure may be manual or automatic. The means described in 5.9.4 shall be maintained until the successful validation as per 5.9.8. In case of manual recovery, information for use shall specify a safe recovery procedure.

5.9.10 Auditing and reporting

Records of auditable events resulting from the requirements of FR2 SL1 (i.e. CR 2.8 as per IEC 62443-4-2:2019) shall also include the following successful and unsuccessful events (not a sequential list):

— automatic initiation (see 5.9.2);

— automatic delivery (see 5.9.3);

— enabling the means for protection of persons (see 5.9.4);

— automatic compatibility check (see 5.9.5);

— activation, including information about previous and new executable code identification, identification of parameter sets or individual parameter values (see 5.9.6);

— automatic validation (see 5.9.7);

— releasing the means for protection of persons (see 5.9.8);

— automatic recovery (see 5.9.9).

Audit records may include recording of one or more events.

When not all steps of the software update can be done on-site, the EUC shall have the capability to make the records of all events listed above available to external systems.

6 Information for use

6.1 General

The Table 3 gives an overview of the required content of the information for use of the EUC.

The Table 4 gives an overview of the required content of the information for use of the EUC components which are provided independently of the EUC.

Table 3 — Overview of required content of the information for use of the EUC

Clause in this document	Reference	Description
4.2.6	IEC 62443-4-1:2018, SM-6: File integrity	The information for use shall indicate the means 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 within the product.
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 utilization of the EUC
4.7.1	The requirements of IEC 62443-4-1:2018, DM-1: Receiving notifications of security-related issues, shall apply.	The information for use shall indicate the means to report security-related issues, including vulnerabilities.
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 over the full life-cycle of the EUC.
4.8.2	IEC 62443-4-1:2018, SUM-2: Security update documentation	The information for use shall indicate the means to obtain information on security updates.
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 defense in depth	The information for use shall give an overview of the security defense in depth strategy to the extent required to maintain the security of the EUC.
4.9.2 6.2 6.3	IEC 62443-4-1:2018, SG-2: Defense in depth measures expected in the environment	The information for use shall indicate the conditions for use of the EUC to achieve and maintain the security of the EUC.
4.9.3	IEC 62443-4-1:2018, SG-3: Security hardening guidelines	The information for use shall include guidelines for hardening the EUC during installation and maintenance.
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.

Table 3 *(continued)*

Clause in this document	Reference	Description
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.
5.9.2		The information for use shall indicate the means for preventing initiation of an automatic software update

Table 4 — Overview of required content of the information for use of the EUC components

Clause in this document	Reference	Description
5.6	IEC 62443-4-2:2019, CCSC 2	Where applicable, the information for use shall: — indicate the security requirements that the component does not fulfil itself for achieving the expected security level vector; and — indicate the need for compensating countermeasures in the EUC in which the component can be integrated.

6.2 Instructions to achieve and maintain security

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

6.2.2 The information for use shall list and explain all relevant security configuration options present in the EUC and indicate their default and optional settings.

6.2.3 If the EUC depends on external systems or services for achieving and maintaining its security, the information for use shall define the necessary requirements applicable to these external systems and services.

6.2.4 An remote management platform may be connected to the EUC to manage, for example, remote diagnostics, remote interaction operation, or software updates. The instructions shall indicate the need for addressing cybersecurity requirements for such an remote management platform. In particular, it shall be instructed that the security level of the functions of the EUC need to be considered in the interfaces of the remote management platform towards the EUC.

6.3 Instructions for software update

The instruction of the software update shall include the following, as applicable:

— information specific to the software update (e.g. purpose of the software update, parameter changes, additional operations that the software update requires);

— information on determining target EUC(s) for the software update;

— the means to verify software package authenticity;

— method and conditions to deploy the software package (e.g. automatic, requiring a skilled person on-site to complete the update, the need for special tools);

— procedures to check compatibility of the software package;

— in case protective means are required, information on their activation and release;

— in case of manual validation, instructions for manual validation;

— in case of manual activation, instructions for manual activation;

— in case of manual recovery, instructions for a safe recovery procedure;

— corrective actions to be performed in the event of unsuccessful software update, including information in case of unavailability (see the note);

— competency requirements for persons applying the software packages;

— instructions to maintain a record of current software configuration;

— information that the special tools provided with the EUC need to be available on-site.

NOTE Unavailability of the EUC can lead to a hazardous situation in the building. Hazardous situations that can arise during the software update to consider include, but are not limited to, a temporary loss of lift service where lift availability is critical to the operation of the facility, for example hospitals. Mitigation can be established to address such hazards, such as planned deployment rollout of the software update.

7 Additional security requirements

7.1 General

For each EUC function of the domain "other", the measures required in 5.4 shall have at least the SL-C required for the domain "alarm".

7.2 Software bill of materials

In addition to vulnerability handling requirements in Clause 4, there shall be a process to document the software bill of materials in a commonly used and machine-readable format covering at the very least the top-level dependencies of the EUC.

7.3 Reset of the EUC to secure by default configuration

The EUC shall be capable of resetting back to its original secure by default state.

The original secure by default state of the EUC is:

— a secure by default configuration established when or after putting into service, including configuration of interfaces to external systems and activation of automatic security updates if automatic security updates were active when put into service; and

— a state where the lifecycle counters have not been reset.

NOTE Lifecycle counters include trip counters and bending counters.

Software or configuration which was updated for compliance to safety requirement) shall not be affected by the reset.

7.4 Factory reset of EUC components

EUC components shall be capable of reverting back to their original state or they shall be capable of fulfilling the reset of the EUC per 7.3.

The original state of an EUC component is the state:

— as delivered from the factory; and

— that ensures an EUC that has already been put into service to remain safe and secure if the EUC component is part of this EUC. In this case the EUC is not required to remain in normal operation; and

— where its security settings ensure compliance with the security level as described in its information for use.

NOTE 1 In case of EUC components capable of fulfilling the reset of the EUC, reset of the EUC does not necessarily need to result in the EUC component reaching its original state.

NOTE 2 Factory reset of the EUC component does not necessarily need to remove all the data and settings permanently, if this component is installed in an EUC that has already been put into service. This can be necessary in order to fulfil clause 7.3.

7.5 Data minimisation

The EUC shall only process data, personal or other, that is adequate, relevant and limited to what is necessary for the intended purpose of the EUC.

7.6 Impact on availability of external services

The EUC shall limit its capability to be used in attacks against systems external to the EUC, including distributed denial-of-service.

NOTE Rate limitation is a typical method to minimize impact of denial-of-service attacks.

7.7 Opt-out mechanism

The EUC shall provide an opt-out mechanism for disabling and postponing automatic security updates.

The EUC shall provide an opt-out mechanism for disabling recording of auditable events.

7.8 Additional information for use

In addition to information for use given in Clause 6 the information for use of the EUC shall indicate:

— contact information of the manufacturer for vulnerability disclosure policy and reporting vulnerabilities;

— the technical security support offered;

— significant cybersecurity risks related to reasonably foreseeable misuse;

— the end-date of the support period for vulnerability handling;

— how to access the software bill of materials, if it is made available;

— how to opt-out from the automatic installation of security updates;

— how to opt-out from the recording of auditable events.

Annex A
(informative)

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

A.1 General

One of the fundamental principles of cybersecurity is a mature secure product development lifecycle. This lifecycle should include training, tools, resources, and processes to harden and maintain the EUC against cyber-attacks.

The recommended secure development lifecycle practices are shown in Table C.1.

A.2 Security management

A.2.1 Process scoping

The requirements of this standard apply to EUCs that are capable of connectivity. When starting the development process, it is important to understand the type of EUC being developed as well as the context in which the EUC will be deployed. Some components developed for integration into an EUC may contain no external connections, and/or be physically isolated. However, some other components may have external connections, not as a requirement of their primary function, but as an enhancement to their operation, for example, providing data to a remote management platform or accepting remote software updates. Therefore, it is important to have a robust process to analyse and model the components to determine whether the requirements of this document are applicable to the component.

A.2.2 Security development documentation

Table A.1 lists the typical documentation produced during a secure development lifecycle.

Table A.1 — Typical secure development lifecycle documentation

Document	Description	Reference
Threat modelling and risk assessment	The threat model with residual risks identified.	4.3.2
Security requirements 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:	4.5.1
	— third party code/library analysis report; — dynamic security analysis report; — static code analysis report.	

Table A.1 *(continued)*

Document	Description	Reference
Test reports	— Fuzz testing report — Internal penetration testing report — External penetration testing report	4.6.1 to 4.6.5
Information for use	See 6.1	6.1
Incident response plan	Documented procedures for a 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:

— choose 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 A.3.2 to A.3.8. See also Annex B.

A.3.2 Threat modelling approach

A threat model helps to identify the assets of an EUC, threats, and countermeasures. 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.

NOTE There are various threat modelling frameworks that are vetted and recommended to be used such as STRIDE, VAST, OCTAVE, PASTA, Attack Trees etc.

A.3.3 Identify the specific assets of the EUC

Figure A.1 and Figure A.2 show examples of assets that can be part of the EUC or belong to external systems and services. In these examples, the assets that are part of the EUC have been classified to domains SIL-rated, Essential, Alarm and Other. These assets can include multiple sub-assets and multiple functionalities.

Whenever an EUC connects to an external system, the EUC interface shall fulfil the corresponding security level requirement. For example, the interface used for the Alarm function, shall fulfil the security level of the Alarm function.

Functionalities shown outside the EUC may be implemented inside the EUC. In this case the requirements of this document apply to them. For the functionalities implemented outside the EUC, the requirements of this document can be used.

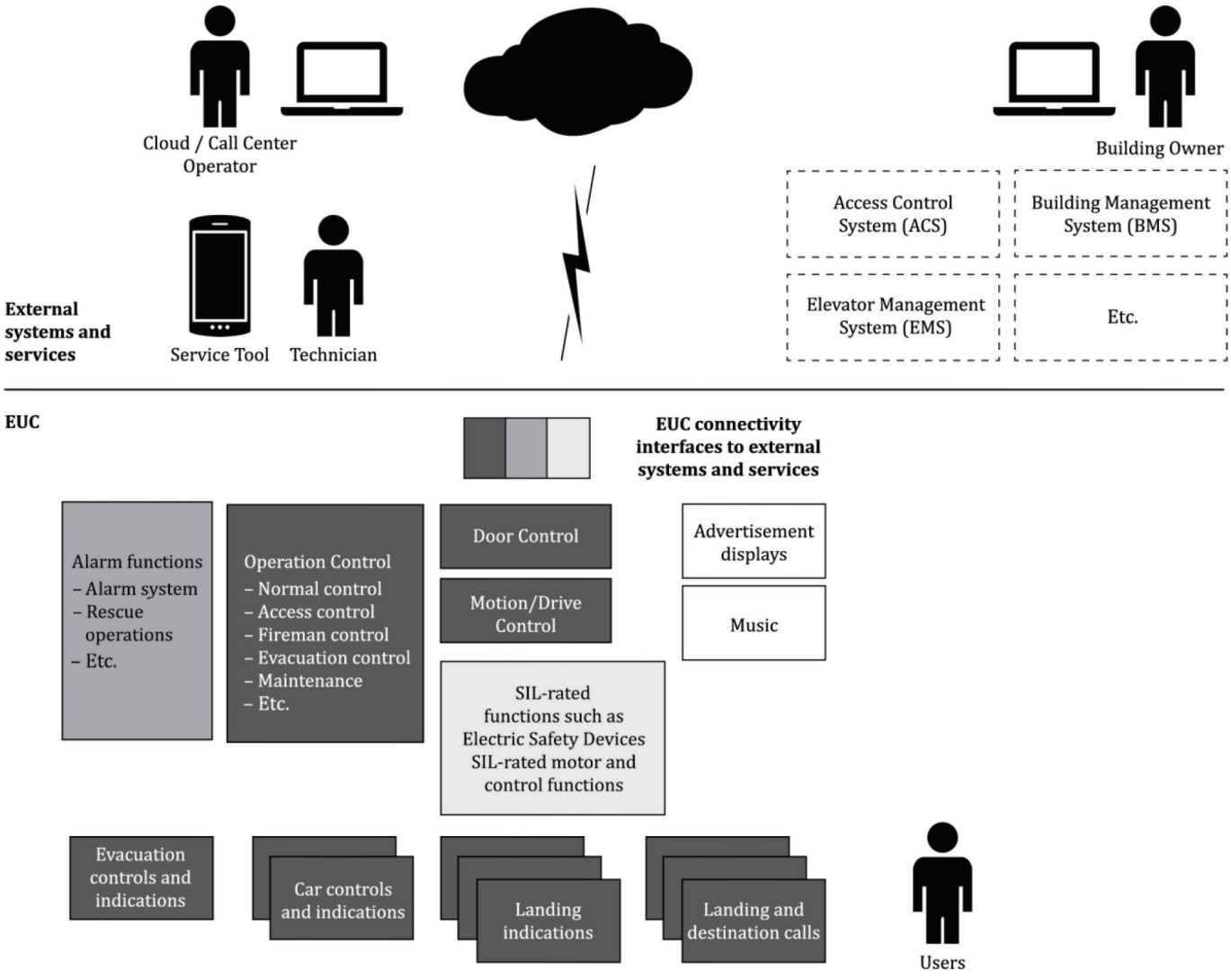


Figure A.1 — Example of assets of a lift system

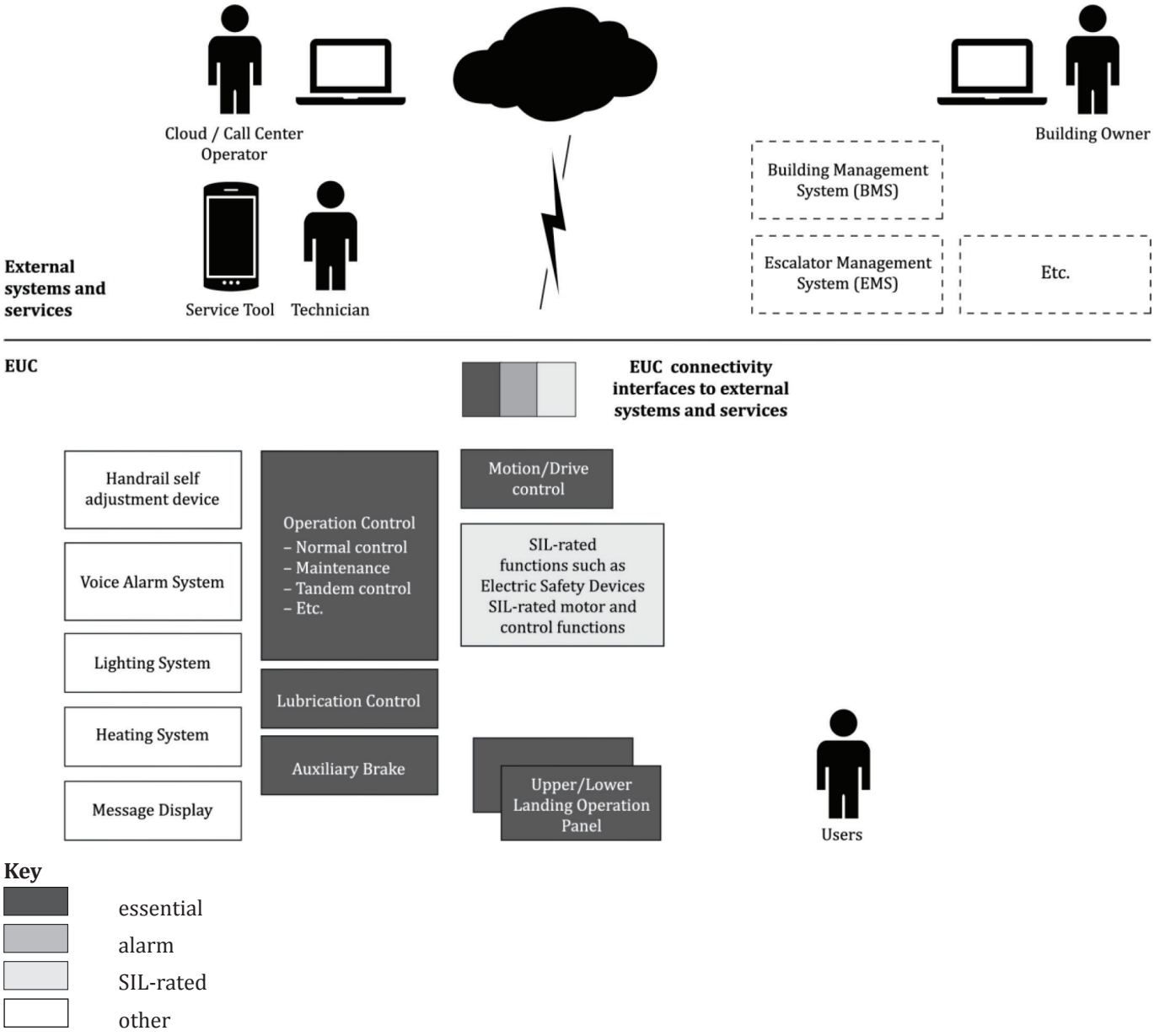


Figure A.2 — Example of assets of an escalator system

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. The attackers differ between capabilities, motivation/gain and resources available to realize the attack. The attackers can be external or internal and both types should be considered.

To identify threats from different attack types, a systematic approach must be followed to ensure holistic coverage and identification of adequate treatment.

For the purposes of this document, typical attackers have been considered. For additional attack types targeting certain building installations (e.g. government facilities, hospitals), a dedicated risk assessment should be made.

Accessibility of the attacker to the EUC is another important aspect. It is important to link the type of attacker motivation and required accessibility of the EUC.

EXAMPLE DOS (denial-of-service) attack requiring physical access may not be relevant but ability to DOS through a remote interface should be considered as a relevant attack type.

A.3.5 Individual risk events identification

It should be defined how the threats according to 4.3.2 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.3.6 Assess individual risk events

The previously identified risk events should be assessed by performing a risk assessment. A risk assessment is an iterative process and sometimes has 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. The following questions, among others, can be used when developing the documentation:

— 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 an intention/motivation to start an attack, the necessary skill and resources, and the probability that a started attack actually affects the protected assets;

— 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 acceptable level of risk;

— if the determined level of risk is above the acceptable level, define the security requirements in order to manage this risk event.

A.3.7 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 defense but utilize multiple layers of protection. If one line of defense 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.3.8 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.

It is recommended that a defined risk management framework is used to manage the risk to an acceptable level. For examples of such frameworks, see ISO 14798, ISO 31000, or NIST SP 800-30.

A.3.9 Application examples of compensating countermeasures

A.3.9.1 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:
  — access to machinery spaces;
  — emergency unlocking key;
  — machinery cabinet or inspection door, which can be opened only with a key or a tool;
— one-way or limited connection:
  — gathering information from the electric safety devices;
  — car controls and indications and landing indications connected through limited-purpose/limited-bandwidth connections;
— system integrity:
  — reliability of the two-way communication system.

The sufficiency of mitigation of compensating countermeasures is determined in the threat analysis. Assumptions and conclusions are documented as per secure development lifecycle in Clause 4.

The following examples illustrate how to apply compensating countermeasures as defined in 5.6.

A.3.9.2 Remote alarm system phone number

Lifts designed according to ISO/FDIS 8100-1 [1] can have a two-way communication system. This typically includes a phone line connection to a rescue service. In order to set up this connection, the phone number(s) of the rescue service need to be defined.

Allowing uncontrolled access to change the phone number is not acceptable for achieving SL1.

If modification of such phone number requires access to the well, machinery spaces, pulley rooms, or a locked cabinet, which are accessible only to authorized persons, then this is sufficient to achieve SL1 for FR 1 (Identification and authentication control) for the purpose of modifying the phone number(s).

If the phone number(s) can be modified through communication that extend beyond the well, machinery spaces and pulley rooms, or a locked cabinet, then additional measures are required to reach SL1.

For communications that do not extend beyond the well, machinery spaces and pulley rooms, or a locked cabinet, such countermeasure may also be applicable.

Furthermore, erroneous modification of the phone number will be detected at the latest after three days (see EN 81-28). This is sufficient to achieve SL1 for FR 3 (System integrity) for the purpose of modifying the phone number(s).

A.3.9.3 Reading the state of the safety chain

Lifts designed according to ISO/FDIS 8100-1 [1] have a safety chain. For the operation of the lift, it is usual for the control system to connect to the safety chain to read its state at different locations.

Unhindered direct electrical access to the safety chain is not acceptable for achieving SL2.

Connection to safety chain is permitted if specific means are being used. Such means ensure that the integrity of the safety chain is maintained even in case of failure or malfunction of the control system connecting to

it. Possible failure exclusion technologies can be found in ISO/FDIS 8100-2.[4] This is sufficient to achieve SL2 for FR 3 (System integrity) for the purpose of reading the state of the safety chain.

On the other hand, failure exclusion technologies found in ISO/FDIS 8100-2 [4] do not restrict information flow and therefore are not technical measures to comply with FR 4 (Data confidentiality).

A.3.9.4 EUC integration into larger systems

A risk assessment for a building sometimes demonstrates 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 can be higher.

A typical lift can still fulfil the higher security level if the countermeasures are provided by the building. As an example, the building can provide an on-site permanently staffed rescue service, and a two-way communication 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.3.10 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 temporary connections (e.g. service tools);

— unauthorized access;

— unauthorized actions by employees or by others;

— unintended employee actions;

— denial of service attacks;

— exploitation of enabled backdoors;

— sabotage/vandalism.

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 can, 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 can lead directly or indirectly to vulnerabilities which can be hard to identify at this high-level stage, since they can 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 fulfilment of its task;

— attack surface identification and minimization;

— modular design methodology to reduce the impact of security threats;

— defense 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;

— restricting the access of a user, interfacing system or task to just the data which are 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 References [5] to [6] in the 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 described in IEC 62443-4-1:2018, Practice 4, SI-1: Security implementation review and SI-2: Secure coding standards.

At a minimum, the 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 can 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 (e.g. system, administrator, root); code running with higher privileges should have valid reasons for doing so;

— security related code module (e.g. authentication, authorization, cryptographic and firewall code);

— code that parses data structures from external sources;

— code obtained from external sources;

— setup code that sets 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, escalators and moving walks are designed to operate as a system. The EUC system manufacturer and/or the installation company can 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 the secure use of the 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 a security requirement (this can be necessary to ensure that the stated security of the component is intact).

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 key activities related to security described in A.6.2 to A.6.6 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 which documents 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 an attempt should be made to exploit all threats identified in the threat model that have been mitigated.

Any attack surface not captured in the 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 level of 2 or more. Alternatively, red teaming and blue teaming can be considered as appropriate testing methods to qualify the entire system security. See Reference [7] in the Bibliography.

A.7 Security management during product lifecycle

A.7.1 Management of security-related issues

While addressing vulnerabilities that surface during testing is part of the secure development process, any other security issues or vulnerabilities that are discovered by the manufacturer or any external organization (for example, product users or security researchers) after product installation also need to be addressed. This starts with a process for gathering threat intelligence or providing avenues for receiving information about security issues from both internal and external sources. Best practice suggests that these security issues or vulnerabilities should be reviewed, addressed and tracked to closure through a well-defined process. The process typically involves an analysis and verification phase, followed by impact assessment, notification to customer if required, development of an update and rollout.

An inventory of hardware and software in use at different installations, assumptions or specifics of the installation environments, any special configurations, etc., can help with efficient verification of issues and better impact assessment. Potential impact is examined and understood to support decisions related to how the issue is to be notified and addressed. Based on this, a further process for fixing the issue by either updating, replacing, or using compensating controls is followed. It is recommended that product manufacturers and integrators maintain written procedures that outline the different aspects of an incident response process.

For further guidance, refer to IEC 62443-4-1:2018 (DM1-DM6) and other sources.

NOTE The Forum of Incident Response and Security Teams (FIRST)[8] defines both product incident response team (PSIRT) and computer incident response team (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

A.7.2.1 General

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 EUC owner based on the intended use case of the equipment. Furthermore, the equipment manufacturer should have processes in place in order to inform EUC owners about security vulnerabilities in their installed products and instructions to address them. Since the EUC owner is not always the equipment service provider, the EUC manufacturer should also have means for the EUC service provider to apply any patches or fixes. See Table A.2 for the roles of manufacturer, service provider and EUC owner.

Table A.2 — Security documentation

IEC62443-4-1:2018,Practice 7		Manufacturer/ Integrator	EUC owner/ Service provider
SUM-1	Security update qualification	Performs	
SUM-2	Security update documentation	Delivers	Takes action
SUM-3	Dependent component or operating system security update documentation	Delivers	Takes action
SUM-4	Security update delivery	Delivers	Takes action
SUM-5	Timely delivery of security patches	Performs	
A.7.2.2	Check on implementation of security updates for high impact scenarios	Performs	Takes action

A.7.2.2 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.7.2.3 Considerations regarding delivery of security patches to lifts, escalators and moving walks

It is important to adhere to the applicable lift, escalator and moving walk code requirements when delivering a security update. The type of component and its function in the system can make it impossible to automatically deliver a security update. In this case, alternate means should be provided to ensure 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 a lift, escalator or moving walk system, since sensitive information can be stored on some components (e.g. IDs, credentials, keys, parameter sets) which can be used maliciously or provide insight into the asset and other linked assets if disclosed. Erasing the information or destroying the asset physically can be necessary. Decommissioning of an asset should be reflected in the asset inventory.

Annex B
(informative)

Additional information on security risk assessment

B.1 General

This annex provides an example of security risk assessment for lifts, escalators, and moving walks. Other methods for assessing security risks are equally acceptable as long as they are used consistently.

While the minimum EUC security level capability requirements (SL-C) are defined in Clause 5, the secure development lifecycle requirements defined in Clause 4 and described in Clause A.3 nevertheless require a security risk assessment during system design. The risk assessment done for an EUC in a specific building may indicate the need for a higher target security level (SL-T). This can be the case, for example, for an EUC installed in a government facility or a hospital.

IEC 62443-3-2:2020 specifies a method of security risk assessment for system design. It specifies a process of partitioning the EUC into zones and conduits, assessing the risk for each zone and conduit, and establishing the target security level (SL-T) for each zone and conduit. This method can be used for EUC during the design phase to set the SL-T. If this method is used, it is possible to consider a typical EUC as a single zone. For a typical EUC in a typical building, it is also possible to use the SL-C defined in 5.4 directly as the SL-T (see IEC 62443-3-2:2020, ZCR 5.6).

Security risk assessment can also be used in managing security-related issues (4.7.3 and A.7.1) to understand the impact of newly discovered vulnerabilities on the EUC.

B.2 Risk assessment scales and risk matrix

IEC 62443-3-2:2020 Annex B gives examples of risk matrices that are not specific to any system type. ISO 14798 defines a risk assessment and reduction methodology for lifts, escalators and moving walks, and is widely used in the industry. For EUC, the risk scales for severity and probability and the 6 × 4 matrix based on ISO 14798 can be used.

Assessment of safety risks for an EUC is a well-established practice. Security risks can lead to safety consequences, but also to other types of consequences, which are not considered in safety risk assessments. Table B.1 amends the severity table from ISO 14798 with the severities of impact to service availability and information integrity.

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)

In security risk assessment, quantitative assessment of risk probability is often impossible. A qualitative approach has to be used instead. Table B.2 amends the probability table from ISO 14798 with probabilities of security risks expressed as qualitative combinations of adversary capability and intent and vulnerabilities.

Table B.2 — Example of probability levels

Level of probability	Probability per unit per lifetime	Description of adversary capability and intent versus EUC vulnerability
A. Highly probable	Likely to occur frequently in the lifecycle	EUC 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 lifecycle	EUC 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 lifecycle	EUC is exposed over the network, security controls are partially implemented and somewhat effective; exploit requires moderate resources, some EUC system specific skills and moderate motivation.
D. Remote	Unlikely, but can possibly occur in the lifecycle	EUC is exposed over the network, security controls are mostly implemented and effective; exploit requires significant resources, EUC system specific skills and high motivation.
E. Improbable	Very unlikely to occur in the lifecycle	EUC is exposed over the network, security controls are fully implemented and effective; exploitation requires a 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 EUC 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 in Table B.3). The resulting risk level will indicate whether the risk is acceptable without action or whether additional countermeasures or mitigations are required.

Low risk is typically acceptable. Moderate risk must be reviewed to understand if additional countermeasures are needed. High risk is typically unacceptable and must be mitigated.

As described in A.3.6 and A.3.8, 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.3 Further guidance

When conducting security risk assessments for lifts, escalators and moving walks, the following additional references can be useful:

— Annex D provides guidance for evaluating internal and external EUC interfaces;

— NIST SP 800-30 describes a risk assessment approach for information systems and organizations, including tables for likelihood and impact, which are widely used for cybersecurity-related risks in various industries;

— ISO 31000 [11] provides guidelines for managing all kinds of risks in organizations, without prescribing specific methods or risk tables.

Annex C
(informative)

List of security practices

Table C.1 gives an overview of the applicable requirement as listed in Clause 4. Subclauses where this document specifies additional requirements in addition to the relevant subclause from the IEC 62443 series are marked “yes” in the rightmost column.

Table C.1 — List of security practices

No	Practice	Subclause 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	no
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	Defense in depth design	no
		4.4.3	SD-3	Security design review	no
		4.4.4	SD-4	Secure design best practices	no

Table C.1 *(continued)*

No	Practice	Subclause in this document	Requirement number	Requirement name	Additional requirements
4	Secure implementation	4.5.1	SI-1	Security implementation review	no
		4.5.2	SI-2	Secure coding standards	no
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	yes
		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 defense in depth	yes
		4.9.2	SG-2	Defense 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

Annex D
(informative)

Guidance for evaluating internal and external EUC interfaces

EUC components are connected through various interfaces both internally and externally. Component of the EUC may communicate to EUC components with the same security level (SL), lower/ or higher security level (SL) or external components outside of EUC.

The recommended approach is to evaluate all the interfaces of an EUC component to ensure security level (SL) is maintained when the component communicates with EUC components with lower security level (SL).

Similarly, all the interfaces allowing EUC components to communicate with external components (physical tool, WiFi, BT) should go through the same exercice to identify all the threats and countermeasures.

When EUC components communicate only with components at the same security level (SL), evaluating the interface may be optional.

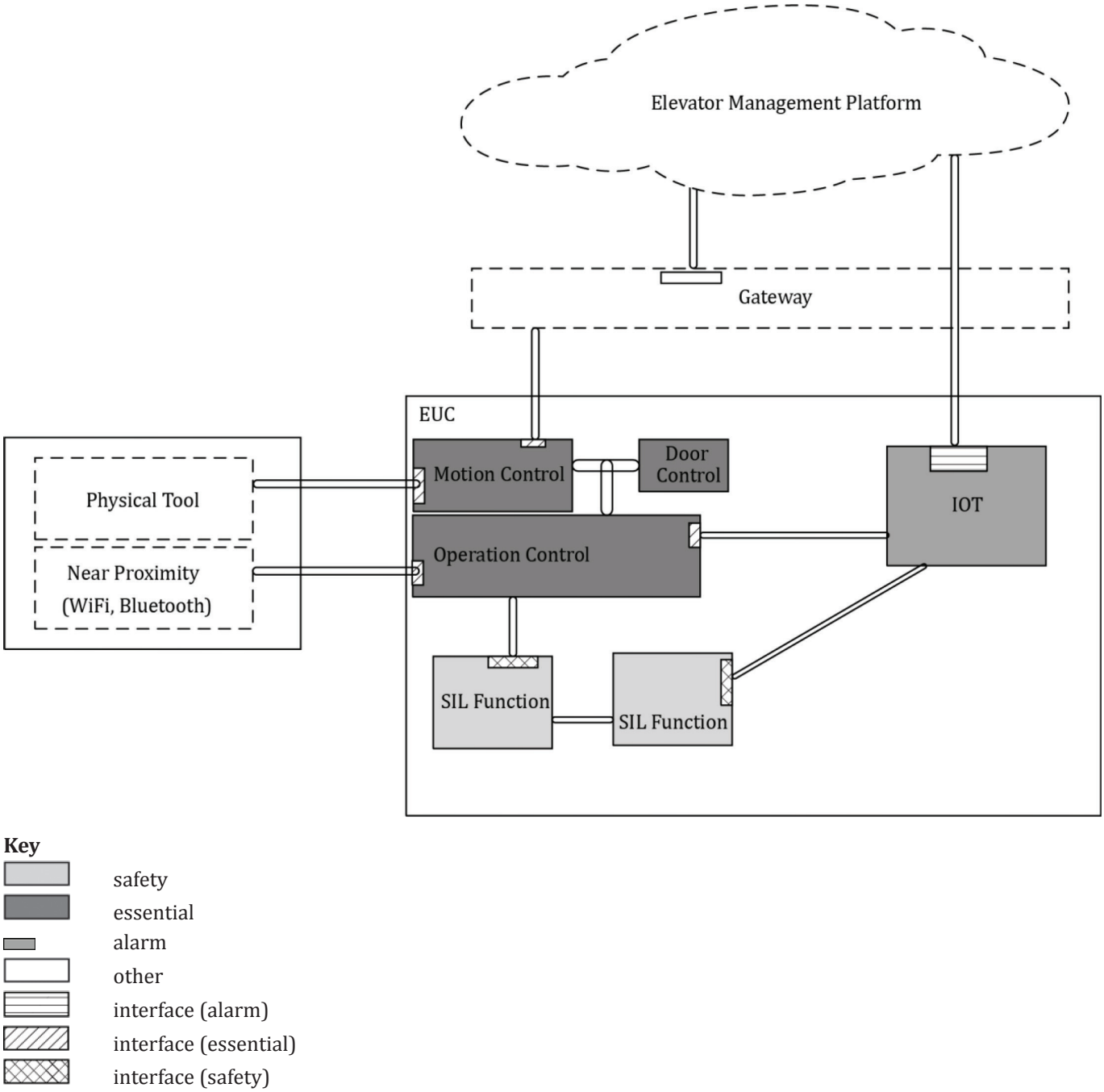
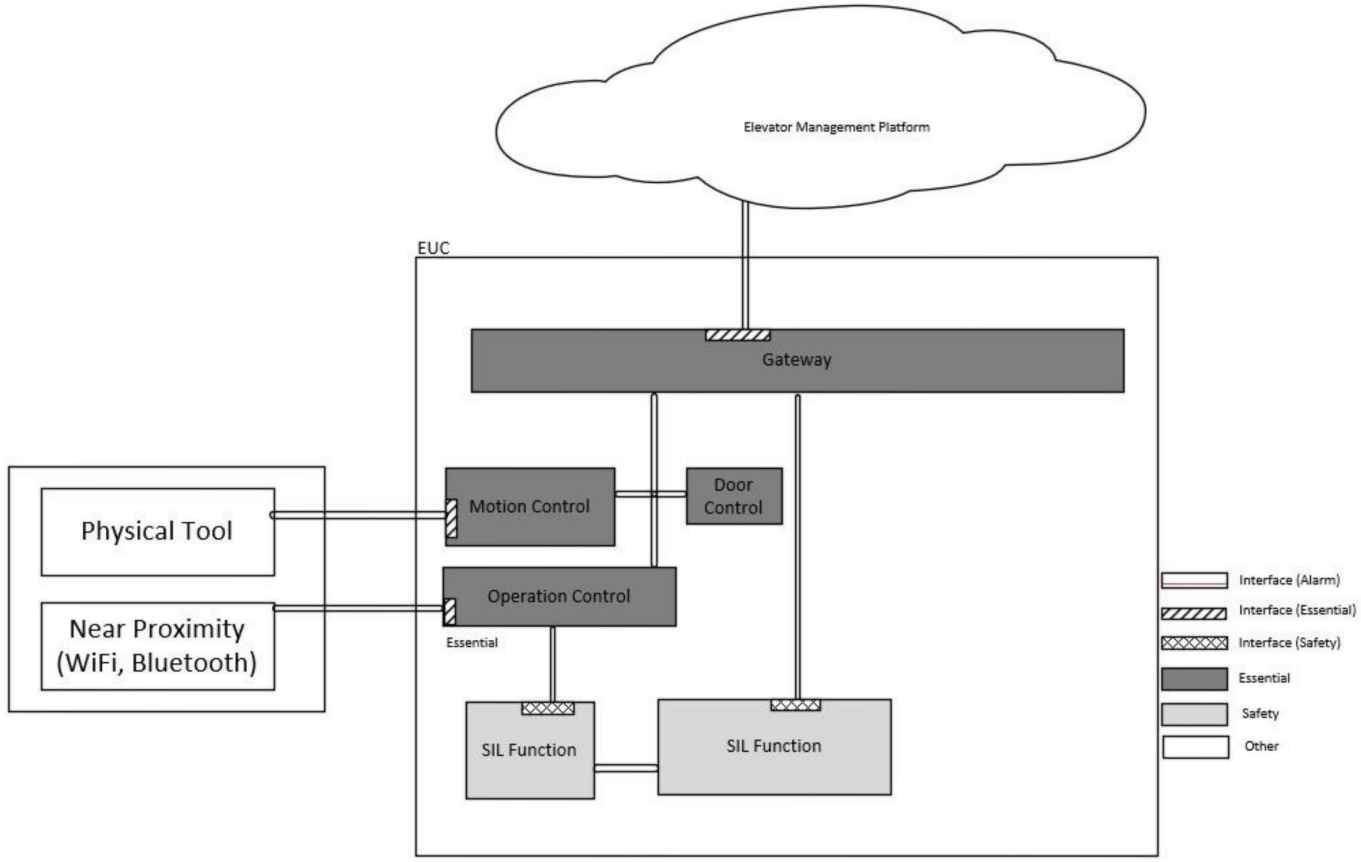


Figure D.1 — Example showing reference architecture of both internal and external connections

The example shown on Figure D.1 shows an example architeture with interaction between EUC components with different functionality. In this case, any information exchange between the gateway and EUC components needs to be evaluated against all the applicable requirements at security level (SL) of the EUC Essential functions (Motion Control component).



Key

- safety
- essential
- other
- interface (alarm)
- interface (essential)
- interface (safety)

Figure D.2 — Example showing alternate reference architecture with internal and external connection

The example showing on Figure D.2 shows an alternate architecture where the gateway has the same security level (SL) as the other components participating in the Essential functions. In this case the evaluation of the interface of Motion Control interface to the gateway is optional since both components have the same security level (SL). However, the interface of the SIL-rated component must be evaluated against the security level (SL) for all the incoming communication from the gateway.

Annex E
(informative)

Example of a software update sequence

Figure E.1 gives an example of a software update sequence and related steps. Table E.1 gives examples of manual and automatic update steps. Depending on the actual implementation of the software update, the steps might be in different order or combined.

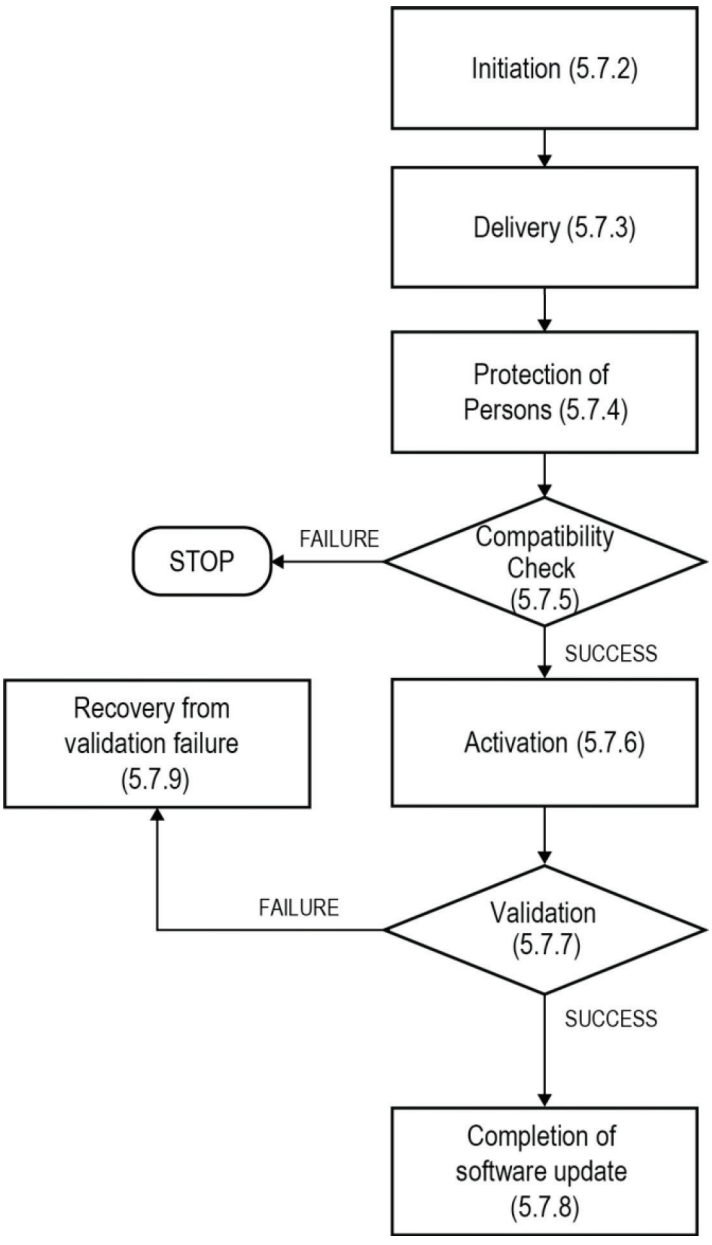


Figure E.1 — Example of a software update sequence

Table E.1 — Examples of manual and automatic update steps

Steps	Manual	Automatic
Initiation	By the maintenance company following the instructions in the information for use and dispatching a person.	By the EUC itself or an external system using a self-triggered connection between EUC and the external system.
Delivery	Using an USB stick containing the software update package. Using a portable device containing the software update package.	Transfer of software update package over a wired or wireless connection from a remote service. Transfer of software update package, in the background, via a portable device connected on-site.
Protection of persons	By using the on-site EUC means for protection for maintenance operations (see 5.9.4). By a person using a remote command to activate the protection for maintenance operation.	By the EUC, based on conditions avoiding risk of entrapment or dangerous situation. By an external system, based on conditions avoiding risk of entrapment or dangerous situation.
Compatibility Check	By following the instructions in the information for use and checking the current configuration of the EUC.	By the EUC, based on verification of authenticity, integrity and compatibility of the software update package.
Activation	By using a command on the EUC. By using a command on a portable device connected to the EUC. By a person using a remote command.	By the EUC.
Validation	By a person on-site executing a test procedure. By a person executing a remote test procedure.	By the EUC or an external system, by execution of a test procedure based on embedded means capable of checking the components that were updated.
Completion of software update	By using the means for return to automatic operation of the lift (see 5.9.4). By a person using a remote command.	By the EUC or an external system.

Annex F
(informative)

Relationship between this European Standard and the essential cybersecurity requirements of Regulation (EU) 2024/2847

Table F.1 and Table F.2 contain a mapping of the essential cybersecurity requirements of Regulation (EU) 2024/2847 to the clauses of this document.

Table F.3 contain a mapping of the information and instructions to the user of Regulation (EU) 2024/2847 to the clauses of this document.

Table F.1 — Correspondence between this European Standard and Annex I part I of Regulation (EU) 2024/2847

The relevant Essential Requirements of Regulation (EU) 2024/2847	Clause(s)/sub-clause(s) of this document	Remarks/Notes
(1) Products with digital elements shall be designed, developed and produced in such a way that they ensure an appropriate level of cybersecurity based on the risks;	4 5.3, 5.4, 5.5, 5.6, 5.7, 5.8 6	
(2) On the basis of the cybersecurity risk assessment referred to in Article 13(2) and where applicable, products with digital elements shall:		
(a) be made available on the market without known exploitable vulnerabilities;	5.3, 5.4, 5.5, 5.6, 5.7, 5.8	
(b) be made available on the market with a secure by default configuration, unless otherwise agreed between manufacturer and business user in relation to a tailor-made product with digital elements, including the possibility to reset the product to its original state;	7.3, 7.4	
(c) ensure that vulnerabilities can be addressed through security updates, including, where applicable, through automatic security updates that are installed within an appropriate timeframe enabled as a default setting, with a clear and easy-to-use optout mechanism, through the notification of available updates to users, and the option to temporarily postpone them;	4.7, 4.8 5.9 7.7	
(d) ensure protection from unauthorised access by appropriate control mechanisms, including but not limited to authentication, identity or access management systems, and report on possible unauthorised access;	5.3, 5.4, 5.5, 5.6, 5.7, 5.8 6	

Table F.1 *(continued)*

The relevant Essential Requirements of Regulation (EU) 2024/2847	Clause(s)/sub-clause(s) of this document	Remarks/Notes
(e) protect the confidentiality of stored, transmitted or otherwise processed data, personal or other, such as by encrypting relevant data at rest or in transit by state of the art mechanisms, and by using other technical means;	5.3, 5.4, 5.5, 5.6, 5.7, 5.8 6	
(f) protect the integrity of stored, transmitted or otherwise processed data, personal or other, commands, programs and configuration against any manipulation or modification not authorised by the user, and report on corruptions;	5.3, 5.4, 5.5, 5.6, 5.7, 5.8 6	
(g) process only data, personal or other, that are adequate, relevant and limited to what is necessary in relation to the intended purpose of the product with digital elements (data minimisation);	7.5	
(h) protect the availability of essential and basic functions, also after an incident, including through resilience and mitigation measures against denial-of-service attacks;	5.3, 5.4, 5.5, 5.6, 5.7, 5.8 6	
(i) minimise the negative impact by the products themselves or connected devices on the availability of services provided by other devices or networks;	7.6	
(j) be designed, developed and produced to limit attack surfaces, including external interfaces;	4 5 6	
(k) be designed, developed and produced to reduce the impact of an incident using appropriate exploitation mitigation mechanisms and techniques;	4 5 6	
(l) provide security related information by recording and monitoring relevant internal activity, including the access to or modification of data, services or functions, with an opt-out mechanism for the user;	5.3, 5.4, 5.5, 5.6, 5.7, 5.8 6 7.7	
(m) provide the possibility for users to securely and easily remove on a permanent basis all data and settings and, where such data can be transferred to other products or systems, ensure that this is done in a secure manner.	7.3, 7.4	

Table F.2 — Correspondence between this European Standard and Annex I part II of Regulation (EU) 2024/2847

The relevant Essential Requirements of Regulation (EU) 2024/2847	Clause(s)/sub-clause(s) of this document	Remarks/Notes
(1) identify and document vulnerabilities and components contained in products with digital elements, including by drawing up a software bill of materials in a commonly used and machine-readable format covering at the very least the top-level dependencies of the products	4.7, 4.8 7.2	
(2) in relation to the risks posed to products with digital elements, address and remediate vulnerabilities without delay, including by providing security updates; where technically feasible, new security updates shall be provided separately from functionality updates;	4.8	
(3) apply effective and regular tests and reviews of the security of the product with digital elements;	4.3, 4.4, 4.5, 4.6	
(4) once a security update has been made available, share and publicly disclose information about fixed vulnerabilities, including a description of the vulnerabilities, information allowing users to identify the product with digital elements affected, the impacts of the vulnerabilities, their severity and clear and accessible information helping users to remediate the vulnerabilities; in duly justified cases, where manufacturers consider the security risks of publication to outweigh the security benefits, they may delay making public information regarding a fixed vulnerability until after users have been given the possibility to apply the relevant patch;	4.7	
(5) put in place and enforce a policy on coordinated vulnerability disclosure;	4.7	

Table F.2 *(continued)*

The relevant Essential Requirements of Regulation (EU) 2024/2847	Clause(s)/sub-clause(s) of this document	Remarks/Notes
(6) take measures to facilitate the sharing of information about potential vulnerabilities in their product with digital elements as well as in third party components contained in that product, including by providing a contact address for the reporting of the vulnerabilities discovered in the product with digital elements;	7.8	
(7) provide for mechanisms to securely distribute updates for products with digital elements to ensure that vulnerabilities are fixed or mitigated in a timely manner and, where applicable for security updates, in an automatic manner;	4.8 5.9	
(8) ensure that, where security updates are available to address identified security issues, they are disseminated without delay and, unless otherwise agreed between a manufacturer and a business user in relation to a tailor-made product with digital elements, free of charge, accompanied by advisory messages providing users with the relevant information, including on potential action to be taken.	4.8	

Table F.3 — Correspondence between this European Standard and Annex II of Regulation (EU) 2024/2847

The relevant Essential Requirements of Regulation (EU) 2024/2847	Clause(s)/sub-clause(s) of this document	Remarks/Notes
1. the name, registered trade name or registered trademark of the manufacturer, and the postal address, the email address or other digital contact as well as, where available, the website at which the manufacturer can be contacted;	7.8	
2. the single point of contact where information about vulnerabilities of the product with digital elements can be reported and received, and where the manufacturer's policy on coordinated vulnerability disclosure can be found;	7.8	
3. name and type and any additional information enabling the unique identification of the product with digital elements;		Not covered
4. the intended purpose of the product with digital elements, including the security environment provided by the manufacturer, as well as the product's essential functionalities and information about the security properties;	6	
5. any known or foreseeable circumstance, related to the use of the product with digital elements in accordance with its intended purpose or under conditions of reasonably foreseeable misuse, which may lead to significant cybersecurity risks;	7.8	
6. where applicable, the internet address at which the EU declaration of conformity can be accessed;		Not covered
7. the type of technical security support offered by the manufacturer and the end-date of the support period during which users can expect vulnerabilities to be handled and to receive security updates;	7.8	
8. detailed instructions or an internet address referring to such detailed instructions and information on:		
(a) the necessary measures during initial commissioning and throughout the lifetime of the product with digital elements to ensure its secure use;	6	
(b) how changes to the product with digital elements can affect the security of data;	6	
(c) how security-relevant updates can be installed;	6.3	

Table F.3 *(continued)*

The relevant Essential Requirements of Regulation (EU) 2024/2847	Clause(s)/sub-clause(s) of this document	Remarks/Notes
(d) the secure decommissioning of the product with digital elements, including information on how user data can be securely removed;	6.1	
(e) how the default setting enabling the automatic installation of security updates, as required by Part I, point (2)(c), of Annex I, can be turned off;	7.8	
(f) where the product with digital elements is intended for integration into other products with digital elements, the information necessary for the integrator to comply with the essential cybersecurity requirements set out in Annex I and the documentation requirements set out in Annex VII	6.1	
9. If the manufacturer decides to make available the software bill of materials to the user, information on where the software bill of materials can be accessed.	7.8	

Annex ZA
(informative)

Relationship between this European Standard and the essential requirements of Regulation (EU) 2023/1230 aimed to be covered

This European Standard has been prepared under a Commission's standardization request C(2025)129 final Commission Implementing Decision of 20 January 2025 to the European Committee for Standardization and to the European Committee for Electrotechnical Standardization as regards machinery in support of Regulation (EU) 2023/1230 of the European Parliament and of the Council (M/605) to provide one voluntary means of conforming to essential requirements of Regulation (EU) 2023/1230 of the European Parliament and of the Council of 14 June 2023 on machinery (OJ L 165, 29.6.2023).

Once this standard is cited in the Official Journal of the European Union under that Regulation, compliance with the normative clauses of this standard given in Table ZA.1 confers, within the limits of the scope of this standard, a presumption of conformity with the corresponding essential requirements of that Regulation, and associated EFTA regulations.

Table ZA.1 — Correspondence between this European Standard and Annex III of Regulation (EU) 2023/1230

The relevant Essential Requirements of Regulation (EU) 2023/1230	Clause(s)/sub-clause(s) of this EN	Remarks/Notes
1.1.9	5	
1.2.1, 2nd paragraph, letter a)	5	
1.2.1, 2nd paragraph, letter f)		Not covered

WARNING 1 Presumption of conformity stays valid only as long as a reference to this European Standard is maintained in the list published in the Official Journal of the European Union. Users of this standard should consult frequently the latest list published in the Official Journal of the European Union.

WARNING 2 Other Union legislation may be applicable to the product(s) falling within the scope of this standard.

Bibliography

[1] ISO/FDIS 8100-1, *Lifts for the transport of persons and goods — Part 1: Safety rules for the construction and installation of passenger and goods passenger lifts*

[2] ISO 8103-1:2024, *Escalators and moving walks — Part 1: Safety requirements*

[12] ISO 14798:2009, *Lifts (elevators), escalators and moving walks — Risk assessment and reduction methodology*

[11] ISO 31000:2018, *Risk management — Guidelines*

[10] NIST SP 800-30, *Guide for Conducting Risk Assessments*

[3] EN 81-28:2018, *Safety rules for the construction and installation of lifts. Lifts for the transport of persons and goods - Remote alarm on passenger and goods passenger lifts*

[4] ISO/FDIS 8100-2, *Lifts for the transport of persons and goods — Part 2: Design rules, calculations, verifications and tests of lift components*

[5] CAPEC. https://capec.mitre.org

[6] CWE. https://cwe.mitre.org/top25/index.html

[7] NIST Computer security resource center, https://csrc.nist.gov/glossary/term/Red_Team_Blue_Team_Approach

[8] Forum of Incident Response and Security Teams (FIRST)Available from. https://www.first.org/

[9] ISO 14798:2009, *Lifts (elevators), escalators and moving walks — Risk assessment and reduction methodology*

[13] IEC 62443-2-4:2015, *Security for industrial automation and control systems — Part 2-4: Security program requirements for IACS service providers*

[14] OWASP. https://owasp.org

[15] NIST SP 800-82

[16] 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*

[17] IEC Guide 120:2018, *Security aspects — Guidelines for their inclusion in publications*

[18] ISO/IEC 27005:2018, *Information technology — Security techniques — Information security risk management*

[19] Chttps M.I.S.R.A. www.misra.org.uk/

[20] EN 115-1:2017, *Safety of escalators and moving walks. Part 1: Construction and installation*

[21] SEI CERT Coding Standardshttps. wiki.sei.cmu.edu/confluence/display/seccode/SEI+CERT+Coding+Standards

[22] ISO 9000:2015, *Quality management systems — Fundamentals and vocabulary*

[23] ASME A17.1, *CSA B44 - 2019, Safety Code for Elevators and Escalators*

[24] Secure Coding Practices-Quick Reference GuideOWASPVersion 2.0, 2010, https://owasp.org/www-pdf-archive/OWASP_SCP_Quick_Reference_Guide_v2.pdf

[25] GB/T 7588.1-2020, *Safety rules for the construction and installation of lifts—Part 1: Passenger and goods passenger lifts*

[26] GB/T 24476- 2017, *Specification for internet of things for lifts, escalators and moving walks*

[27] ISO/IEC 27017:2015, *Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services*

[28] BSI ICS SECURITY COMPENDIUMHTTPS. www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/ICS/ICS-Security_compendium.pdf?__blob=publicationFile&v=3ISO