भारतीय मानक

Indian Standard

IS 17805 (Part 20) : 2024
ISO 8102-20 : 2022

लिफ्ट्स, स्वचलित सीढ़ियाँ और मूविंग वॉक की विद्युतीय आवश्यकताएँ

भाग 20 साइबर सुरक्षा

Electrical Requirements for Lifts Escalators and Moving Walks

Part 20 Cyber Security

ICS 91.140.90

भारतीय मानक ब्यूरो
BUREAU OF INDIAN STANDARDS
मानक भवन, 9 बहादुर शाह ज़फर मार्ग, नई दिल्ली - 110002
MANAK BHAVAN, 9 BAHADUR SHAH ZAFAR MARG
NEW DELHI - 110002
www.bis.gov.in www.standardsbis.in

June 2024 **Price Group 13**

Lifts, Escalators and Moving Walks Sectional Committee, ETD 25

NATIONAL FOREWORD

This Indian Standard which is identical to ISO 8102-20 : 2022 'Electrical requirements for lifts, escalators and moving walks — Part 20: Cyber security' issued by the International Organization for Standardization (ISO) was adopted by the Bureau of Indian Standards on recommendation of the Lifts, Escalators and Moving Walks Sectional Committee and approval of the Electrotechnical Division Council.

The text of the ISO standard has been approved as suitable for publication as an Indian Standard without deviations. Certain terminologies and conventions are, however, not identical to those used in Indian Standards. Attention is particularly drawn to the following:

a) Wherever the words 'International Standard' appear referring to this standard, they should be read as 'Indian Standard'; and

b) Comma (,) has been used as a decimal marker, while in Indian Standards, the current practice is to use a point (.) as the decimal marker.

In this adopted standard, reference appears to the following International Standard for which Indian Standard also exist. The corresponding Indian Standard, which is to be substituted in its place, is listed below along with its degree of equivalence for the edition indicated:

International Standard	*Corresponding Indian Standard*	*Degree of Equivalence*
ISO 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	IS 17900 (Part 1) : 2022 Lifts for the transport of persons and goods: Part 1 Safety rules	Modified/Technical Equivalent
IEC/TS 62443-1-1: 2009 Industrial communication networks — Network and system security — Part 1-1: Terminology concepts and models	IS/IEC 62443-1-1 : 2009 Industrial communication networks: Part 1 Network and system security, Section 1 Terminology concepts and models	Identical
IEC 62443-3-3: 2013 Industrial communication networks — Network and system security — Part 3-3: System security requirements and security levels	IS/IEC 62443-3-3 : 2013 Industrial communication networks: Part 3 Network and system security, Section 3 System security requirements and security levels	Identical
IEC 62443-4-1: 2018 Security for industrial automation and control systems — Part 4-1: Secure product development lifecycle requirements	IS/IEC 62443-4-1 : 2018 Security for industrial automation and control Systems: Part 4, Section 1 Secure product development lifecycle requirements	Identical
IEC 62443-4-2: 2019, Security for industrial automation and control systems — Part 4-2: Technical security requirements for IACS components	IS/IEC 62443-4-2 : 2019 Security for industrial automation and control systems: Part 4, Section 2 Technical security requirements for IACS components	Identical

(*Continued on third cover*)

Contents

Page

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 industry-specific requirements that are necessary when applying the IEC 62443 series.

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.

Indian Standard

ELECTRICAL REQUIREMENTS FOR LIFTS ESCALATORS AND MOVING WALKS

PART 20 CYBER SECURITY

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. It is also applicable with other lift, escalator and moving walk standards that specify similar requirements, and to other lift-related equipment connected to the EUC.

This document specifies product and system requirements related to cybersecurity threats in the following lifecycle steps:

— product development (process and product requirements);

— manufacturing;

— installation;

— operation and maintenance;

— decommissioning.

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

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 product supplier and system integrator of the EUC to establish documentation allowing the asset owner, referred to as the "EUC owner" in this document, to achieve and maintain the security of the EUC.

This document specifies the minimum cybersecurity requirements for:

— essential functions;

— safety functions;

— alarm functions.

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 to 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.

ISO 8100-1:2019, *Lifts for the transport of persons and goods — Part 1: Safety rules for the construction and installation of passenger and goods passenger lifts*

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

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

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

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

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

3 Terms, definitions and abbreviated terms

3.1 Terms and definitions

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

ISO and IEC maintain 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, lift, escalator and moving walk control systems are considered to be computer systems.

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

[SOURCE: IEC 62443-3-2:2020, 3.1.7, modified — Note 1 to entry changed and Note 2 to entry have been added.]

3.1.2
equipment under control
EUC
lift, escalator or moving walk

3.1.3
equipment under control owner
EUC owner
individual or organization responsible for the EUC

Note 1 to entry: The EUC owner is equivalent to the term "asset owner" given in IEC 62443-4-1:2018, 3.1.6.

[SOURCE: IEC 62443-4-1:2018, 3.1.6, modified — the text "one or more IACSs" in definition replaced with the text "the EUC" and Note 1 to entry added]

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-T	target security level
SM	security management
SR	security requirement
SUM	security update management
SVV	security verification and validation

4 Secure development lifecycle for lifts, escalators and moving walks

4.1 General

The requirements of this clause shall apply to component development and system integration. See Annex A for additional information on secure development lifecycle, Annex B for additional information on security risk assessments and Annex C for a list of security practices.

4.2 Security management

4.2.1 Development process

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

4.2.2 Identification of responsibilities

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

4.2.3 Identification of applicability

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

4.2.4 Security expertise

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

In addition to 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.

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 in a timely manner.

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 Security requirements

5.1 General

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

5.2 Foundational requirements

IEC/TS 62443-1-1:2009 defines seven FRs, which shall be applied to the EUC functions, as specified in 5.3 to 5.6.

5.3 Domains of the EUC functions

In the scope of this document, the EUC functions are classified into the domains of "Safety", "Essential", and "Alarm". 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	Non-comprehensive list of functions under the domains as examples
Safety	SIL-rated control functions.	— SIL-rated electric safety devices and electrical protective devices — SIL-rated motor and brake control functions
Essential	Function or capability that is required to ensure the availability of the lift, escalator or moving walk, and its compliance to safety regulations, and which do not belong to Safety or Alarm function domains.	Lifts: — Normal control — Car and landing call devices — Access control — Energy saving (car light, ventilation, etc.) — Car and landing indicators — Hoisting machine motor control — Door control including its protective devices — Load control — Run time limiter — Fire service operation — Return to normal operation of the lift — Re-opening of the door — Remote monitoring and interaction Escalator and moving walks: — Start and stop functionalities — Timetable and system clock operations — Direction indicators — Preventing from starting when permitted stopping distance exceeded — Protection of motors — Automatic operation: starting in predetermined direction — Remote monitoring and interaction

Table 1 *(continued)*

Domain	Description	Non-comprehensive list of functions under the domains as examples
Alarm	Devices used to verify entrapment, to call for help and to rescue passengers in case of entrapment.	— Alarm, intercom and video devices — Emergency supply — Evacuation device — Displays and voice announcements used for rescue
Other	Additional functions not related to safety, essential or alarm domains.	— Advertising displays — Music and gaming devices — User applications

5.4 EUC security level requirements

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

NOTE 1 The SL-T for the domain “other” is not defined in this document.

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

NOTE 2 The security level vector approach is discussed in IEC 62443-3-3:2013, Annex A.

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

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

Security level vectors for the domain "Other" in Table 1 are not defined in this document. See Annex D for examples of extending security requirements to the domain "Other".

Table 2 — Security level vectors for EUC function domains

Foundational requirement	Security level		
	Alarm	Essential	Safety
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-T(Essential) = {2 2 2 2 1 1 2}”.

5.5 Selection of security controls and countermeasures

After the EUC function domain and the corresponding security level vector from Table 2 have been selected, security controls and countermeasures shall be selected from IEC 62443-3-3:2013 and IEC 62443-4-2:2019, as applicable. However, should the threat model required in 4.3.2 yield threats

that are not adequately mitigated by using Table 2 alone, the residual threats shall be mitigated by additional security controls and countermeasures.

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

NOTE 2 IEC 62443-4-2:2019 describes the component requirements and requirement enhancements (REs) that are applied to components of the system. There are component specific requirements for software applications (SARs), embedded devices (EDRs), host devices (HDRs) and network devices (NDRs).

5.6 Common security constraints

5.6.1 General

When implementing system requirements and component requirements, the common component security constraints (CCSCs) specified in 5.6.2 to 5.6.5 shall be applied.

5.6.2 Support of essential functions

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

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

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

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

5.6.3 Compensating countermeasures

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

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

5.6.4 Least privilege

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

5.6.5 Software development process

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

6 Information for use

The purpose of the information for use is to provide to asset owners, maintainers and other relevant stakeholders the information that is useful for achieving and maintaining the security of the EUC in the location where it is installed.

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

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

The information for use shall list and explain all security configuration options present in the EUC and make note of their default and optional settings.

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

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

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

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

Table 3 — Summary of requirements for the information for use

Clause in this document	Reference	Requirement for the information for use
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.
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	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.
4.9.5	IEC 62443-4-1:2018, SG-5: Secure operation guidelines	The information for use shall include cybersecurity guidelines for operating the EUC.
4.9.6	IEC 62443-4-1:2018, SG-6: Account management guidelines	The information for use shall document the management accounts, permissions and privileges required for operating the EUC.

Annex A
(informative)

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

A.1 General

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

The recommended cybersecurity process lifecycle practices are shown in Table C.1.

A.2 Security management

A.2.1 Process scoping

It is important to understand the type of equipment as well as the context in which the equipment is to be deployed. Components being developed for integration into an EUC can contain no external connections, and/or be physically isolated, as per relevant requirements. However, some components can have external connections, not as a requirement of their primary function, but as an enhancement to their operation (as in providing data to service systems or accepting software updates). It is important, therefore, to have a robust process to analyse and/or model the component, and review in order to determine whether the requirements of this 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: — third party code/library analysis report; — dynamic security analysis report; — static code analysis report.	4.5.1
Test reports	— Fuzz testing report — Internal penetration testing report — External penetration testing report	4.6.1 to 4.6.5
Information for use	See Clause 6	Clause 6

Table A.1 *(continued)*

Document	Description	Reference
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:

— decide for a threat modelling approach;

— identify and delimit the EUC;

— identify the specific assets of the EUC;

— identify relevant attacker types;

— identify threats endangering the identified assets;

— identify individual risk events;

— assess individual risk events;

— create security requirements;

— repeat assessment of individual risk events.

Details for each step are given in 4.3.1 to 4.3.5. See also Annex B.

A.3.2 Threat modelling approach

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

— attacker-centric;

— system-centric;

— asset-centric.

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

A.3.3 Identify the specific assets of the EUC

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

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.

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

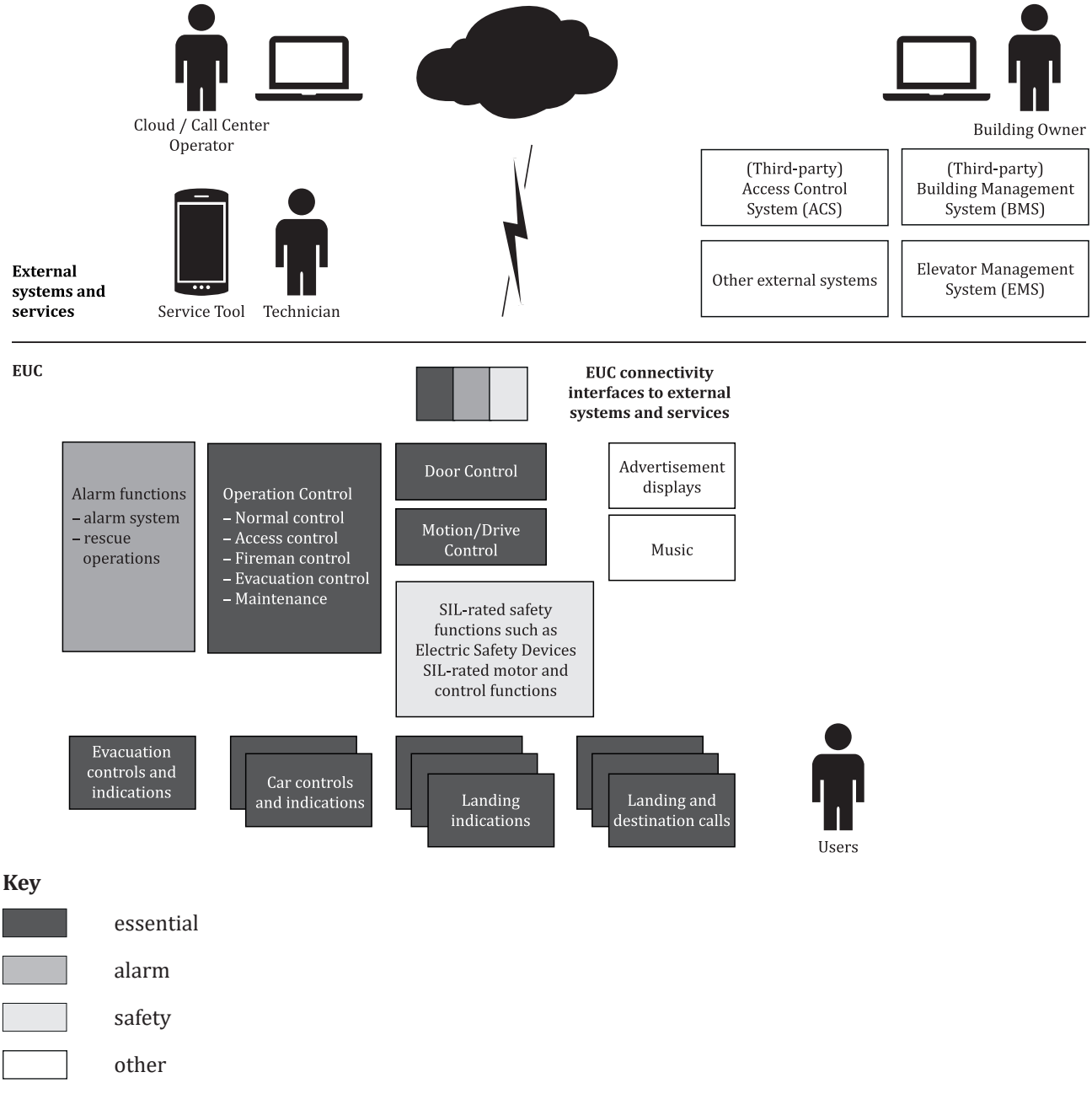

Figure A.1 — Example of assets of a lift system

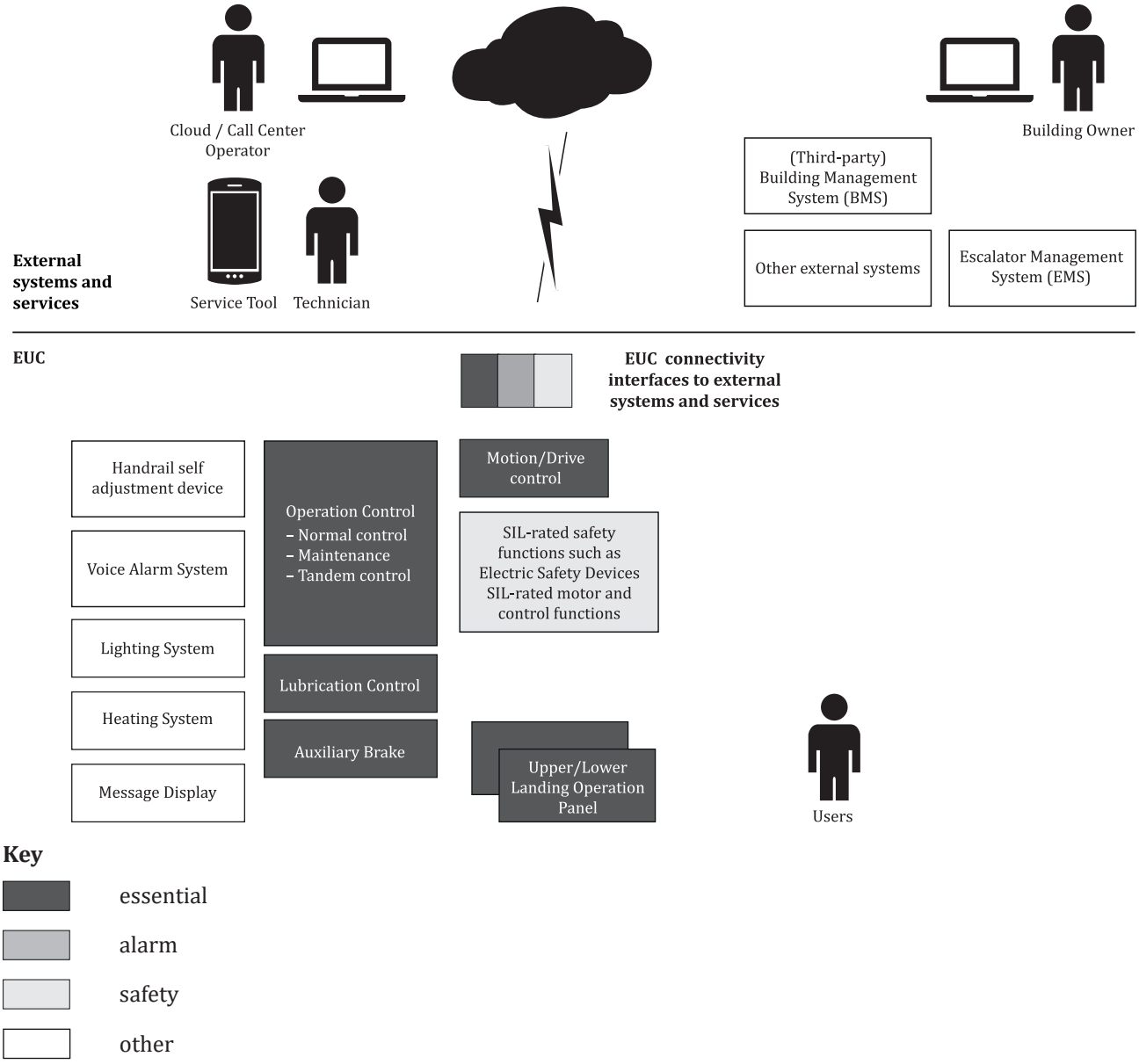

Figure A.2 — Example of assets of an escalator system

A.3.4 Identify relevant attacker types

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

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

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

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

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

The cybersecurity requirements specified in Clause 5 are minimum requirements. Specialized building, structures or utilization (e.g. government facilities, critical care facilities) can require that the application of the facility be considered to determine if higher levels of cybersecurity or complete isolation from the internet are required. For example, protection against cyber threats that can result in a denial of lift service can be necessary. See the note in IEC 62443-3-3:2013, 4.2, for guidance on cybersecurity risk (threat) assessment.

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

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.

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 authorized persons (see ISO 8100-1:2019, 5.2.2.1);
  - emergency unlocking means (see ISO 8100-1:2019, 5.3.9.3 and 5.12.1.5.2.2);
  - locked cabinet or inspection door (see ISO 8100-1:2019, 5.2.6.4.3.4, 5.2.6.4.4.1 and 5.12.1.5.2.2);
- one-way or limited connection:
  - parallel connection to electric safety device (see ISO 8100-1:2019, 5.11.2.1.2);
  - car controls and indications and landing indications connected through limited-purpose/ limited-bandwidth connections;
- system integrity:
  - reliability of remote alarm system in accordance with EN 81-28 (see ISO 8100-1:2019, 5.12.3).

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 5.6.3.

A.3.9.2 Remote alarm system phone number

Lifts designed according to ISO 8100-1 are required to have a remote alarm system. This typically includes a phone line connection to a rescue service (5.12.3.1). 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 alarm phone number is not acceptable for achieving SL1.

If modification of such phone number requires access to the well, machinery spaces and pulley rooms, or in 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 be applicable.

Furthermore, erroneous modification of the phone number will be detected at the latest after three days (EN 81-28, 4.2.1). 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 8100-1 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.

ISO 8100-1:2019, 5.11.2.1.2, permits connection 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 technologies for these means can be found in ISO 8100-2, 5.15. 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, means found in ISO 8100-2, 5.15 do not restrict information flow and therefore are not technical measures to comply with FR 4 (Data confidentiality).

A.3.9.4 Firmware update

The ability to securely update the software or firmware of an EUC is an important functionality and is relevant to all EUC function domains. The manner in which the remote update functionality is carried out is a key aspect in the consideration of risk. For example, the cyber risk of an EUC function domain is greatly enhanced if the update functionality is permissible from the open internet as opposed to the case when physical presence is required to perform or trigger the update. Compensating countermeasures such as locked cabinet may further reduce the risk and hence can be used to substitute equivalent security controls required to support the security requirements corresponding to different security levels.

A.3.9.5 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 the alarm function can be installed between the lift and the on-site rescue service in a way to ensure the confidentiality required by the building security.

A.3.10 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;

— 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 [12] to [22] 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).

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

A.6 Security validation

A.6.1 General

In addition to the normal testing and validation processes which are a part of product development, cybersecurity verification and test plans are part of a formalized process in the product verification phase. The 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 target 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 [14] 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)[21] 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

IEC 62443-4-1:2018, 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, parameter sets, certificates) 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 how to apply the general method of risk assessments

B.1 Additional information on security risk assessments

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

In addressing a specific product the following should be considered:

— extending the risk assessment by additional risks (and therefore possibly additional countermeasures);

— extending the risk assessment by additional assets (and therefore possibly additional risks);

— modifying the functionality grouping assumed in this document;

— deviating from given requirements if they are not applicable or it can be shown that their fulfilment is not necessary in a certain risk context.

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

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

— While the minimum security requirements are defined in Table 2, the level of acceptable risk in other cases has to be agreed upon with the vested stakeholders. This level depends on legal aspects, the organization, the intended use case of the EUC and (local) societal values.

— In addition to risk assessments according to functional safety standards such as ISO 14798, multiple industry specific aspects of security risk impact have to be considered. An example of a possible system of risk types can be found in Table B.1.

— It is advisable to create a system of risk ratings which allows the comparison of different risk types.

— In security risk assessment, quantitative assessment of risk probability is often impossible. A qualitative approach is used instead. An example of qualitative rating of risk probabilities based on adversary capability and intent and system vulnerabilities is given in Table B.2.

— Every risk reduction measure is a trade-off between costs (both unit costs and effort) and security benefit. For this reason, protection against an unrealistic threat level is neither necessary nor economically reasonable. The implementation of unnecessary risk reduction measures is sometimes even counterproductive, e.g. risk reduction measures often have an impact on the usability of a product, legitimate end-users can try to bypass/disable them if they are too inconvenient, every risk reduction measure can also introduce additional vulnerabilities on its own. In any case, the occurrence of a risk event must not result in any harm of persons due to negligence.

— Security is not a subset of functional safety and a security risk assessment should therefore not be carried out under the responsibility of functional safety personnel. Functional safety and security are different domains and require different approaches and knowledge. For example, the risk

assessment approach and the necessary mindset are fundamentally different. A few of the core differences are:

— statistical negligibility of double/multiple faults versus a series of targeted actions following an attack vector;

— random (unmotivated) faults versus intelligent threat sources;

— likelihood as a single value versus likelihood as the combination of multiple and often soft and hard to estimate factors.

— A diverse team is beneficial to utilize different experiences and different points of view. It is suggested to include at least people with a functional safety, production, installation and maintenance background.

— Possible threat actors can differ significantly based on the specific product and its threat landscape, based, for example, on the product specific use case, the site of the installation, the expected passengers and security measures expected in the utilization of the EUC.

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

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

Table B.2 — Example of probability levels

Level of probability	Probability per unit per lifetime	Description of adversary capability and intent versus system vulnerability
A. Highly probable	Likely to occur frequently in the lifecycle	System is exposed over the network and security controls are not implemented and not planned; exploitable by a casual attacker with limited resources and expertise.
B. Probable	Likely to occur several times in the lifecycle	System is exposed over the network, minimal security controls are implemented and minimally effective; exploit requires low resources, expertise and motivation.
NOTE If the system is operated in a closed network or there are other compensating countermeasures in place, the probability can be considered to be lower.		

Table B.2 *(continued)*

Level of probability	Probability per unit per lifetime	Description of adversary capability and intent versus system vulnerability
C. Occasional	Likely to occur at least once in the lifecycle	System 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	System 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	System 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 system is operated in a closed network or there are other compensating countermeasures in place, the probability can be considered to be lower.		

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

As described in A.3.5 and A.3.7, the risk assessment should be repeated after the countermeasures have been defined.

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

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

B.2 Further guidance

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

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

— Annex D, Guidance for application of zones and conduits;

— IEC 62443-3-2:2020 describes a process of partitioning the EUC into zones and conduits, assessing risk for each zone and conduit, and establishing the target security level (SL-T) for each zone and conduit;

— ISO/IEC 27005:2018 describes the general activities which are necessary in order to implement a risk assessment and risk treatment process without prescribing specific methods;

— NIST SP 800-30 describes a mature risk assessment approach which is proven in use by various industries in its pure or some adapted form.

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

— OWASP Top 10[16] states the most relevant types of risks to web applications. Although lifts are a very different kind of product then a web application, all of these risks can apply to lift systems nonetheless (such as configuration user interfaces or diagnosis interfaces);

— OWASP API Top 10[16] contains a similar list especially targeted towards the most common types of risk regarding APIs;

— OWASP IoT Top 10[16] contains a similar list especially targeted towards the most common types of risk regarding IoT devices;

— CWE Top 25[22] Most Dangerous Software Weaknesses;

— BSI ICS Security Compendium[15] gives an overview about possible threats and best practices in an industrial control system context;

— CAPEC[12] provides a list of attack mechanisms and attack patterns at various levels of abstraction.

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 application of zones and conduits

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

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

The security level for each FR is defined by taking the highest security level of each FR defined for functions within that zone.

Functions located within zones Z1 and Z2 in the example system shown in Figure D.1 should use the security level vector defined in Table D.1, column Z1 and Z2. Since the safety component has the highest security level vector requirements for each FR, all assets in the same zone should follow the same, which is also the case for the essential and alarm domains.

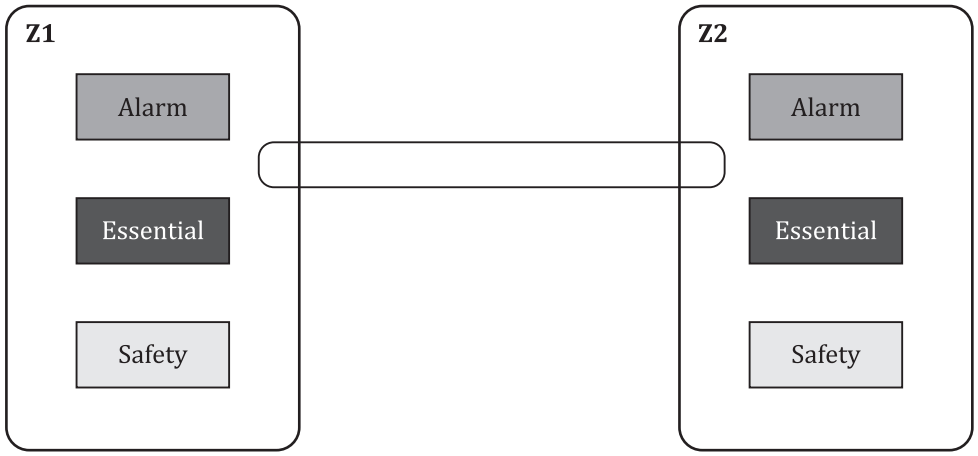

Figure D.1 — Example showing two zones and a conduit connecting them

Table D.1 — Security level vector example for the system given in Figure D.1

Foundational requirement				
	Alarm	Essential	Safety	Z1 and Z2
FR 1 – Identification and authentication control	1	2	3	3
FR 2 – Use control	1	2	2	2
FR 3 – System integrity	1	2	2	2
FR 4 – Data confidentiality	1	2	2	2
FR 5 – Restricted data flow	1	1	1	1
FR 6 – Timely response to events	1	1	1	1
FR 7 – Resource availability	1	2	2	2

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

functions located within zones Z1b and Z2b should use the security level vector defined in column Z1b and Z2b. However, there are no additional requirements for zones Z1 and Z2 as the safety, essential and alarm components are already protected by the countermeasures that meet the security level requirements for the corresponding sub-zones. The function "other" in zones Z1b and Z2b shares the security level vector requirements with the alarm function.

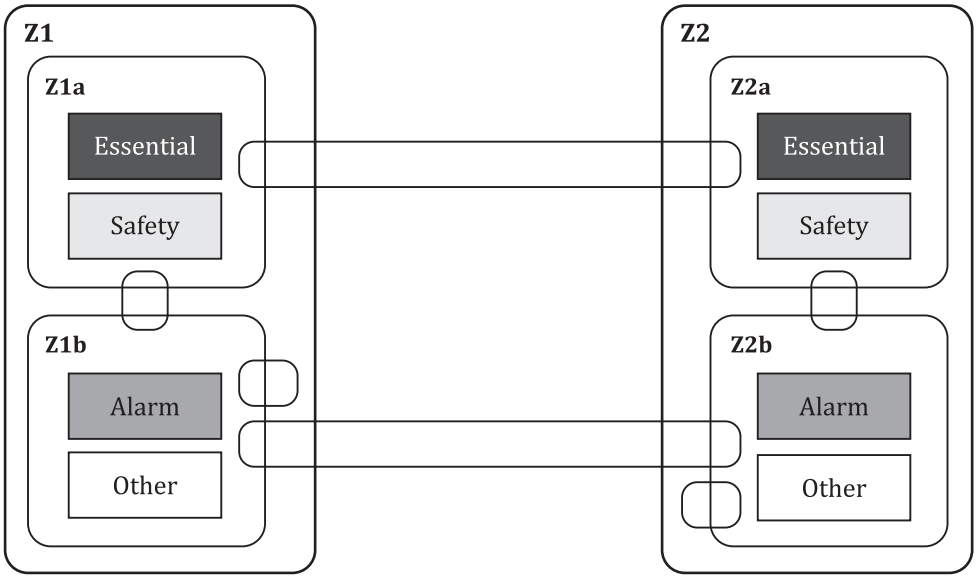

Figure D.2 — Example showing six zones and connecting conduits

Table D.2 — Security level vector example for the system given in Figure D.2

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

The example system shown in Figure D.3 should use the security level vectors defined in Table D.3. Column Z1b defines the security level vector for functions in zone Z1b. Functions located within zones Z1a and Z2a use the security level vector defined in column Z1a and Z2a. There will be no security level requirements for components from the domain "other" in Zones Z1 and Z2.

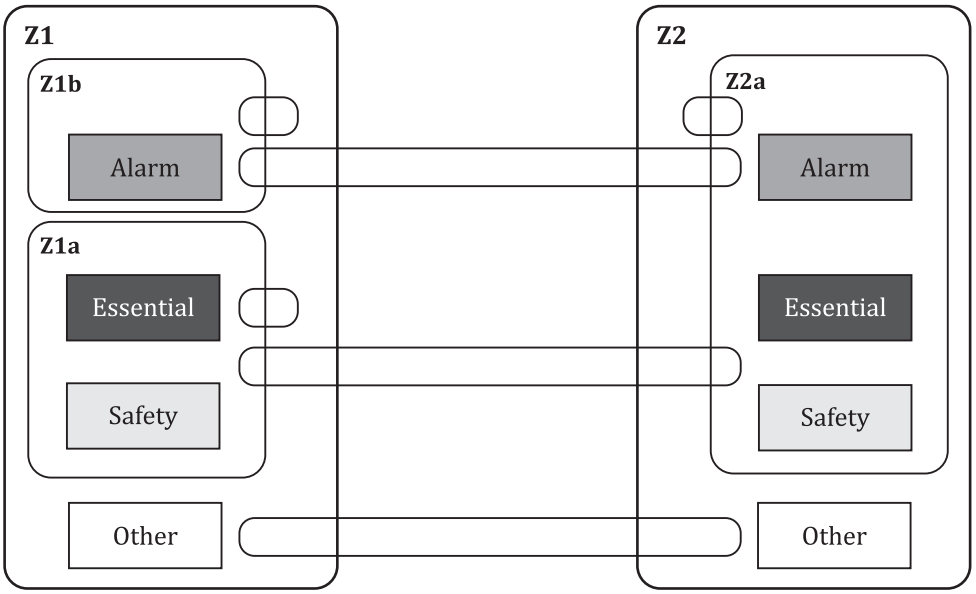

Figure D.3 — Example showing five zones and conduits connecting them

Table D.3 — Security level vector example for the system given in Figure D.3

Foundational requirement					
	Alarm	Essential	Safety	Z1b	Z1a and Z2a
FR 1 – Identification and authentication control	1	2	3	1	3
FR 2 – Use control	1	2	2	1	2
FR 3 – System integrity	1	2	2	1	2
FR 4 – Data confidentiality	1	2	2	1	2
FR 5 – Restricted data flow	1	1	1	1	1
FR 6 – Timely response to events	1	1	1	1	1
FR 7 – Resource availability	1	2	2	1	2

Bibliography

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

[2] 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*

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

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

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

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

[7] 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*

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

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

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

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

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

[13] NIST SP 800-82[1)]

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

[15] BSI ICS Security Compendium https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/ICS/ICS-Security_compendium.pdf?__blob=publicationFile&v=3ISO

[16] OWASP https://owasp.org

[17] NIST SP 800-30, 2012

[18] MISRA C https://www.misra.org.uk/

[19] SEI CERT Coding Standards https://wiki.sei.cmu.edu/confluence/display/seccode/SEI+CERT+Coding+Standards

[20] Secure Coding Practices-Quick Reference Guide OWASP, Version 2.0, 2010, https://owasp.org/www-pdf-archive/OWASP_SCP_Quick_Reference_Guide_v2.pdf

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

[22] CWE https://cwe.mitre.org/top25/archive/2021/2021_cwe_top25.html

1) https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

(*Continued from second cover*)

The Committee has reviewed the provisions of the following International Standards referred in this adopted standard and decided that they are acceptable for use in conjunction with this standard.

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

For the purpose of deciding whether a particular requirement of this standard is complied with the final value, observed or calculated, expressing the result of a test or analysis shall be rounded off in accordance with IS 2 : 2022 'Rules for rounding off numerical values (*revised*)'. The number of significant places retained in the rounded off value should be the same as that of the specified value in this standard.

Bureau of Indian Standards

BIS is a statutory institution established under the *Bureau of Indian Standards Act*, 2016 to promote harmonious development of the activities of standardization, marking and quality certification of goods and attending to connected matters in the country.

Copyright

Review of Indian Standards

Amendments are issued to standards as the need arises on the basis of comments. Standards are also reviewed periodically; a standard along with amendments is reaffirmed when such review indicates that no changes are needed; if the review indicates that changes are needed, it is taken up for revision. Users of Indian Standards should ascertain that they are in possession of the latest amendments or edition by referring to the website-www.bis.gov.in or www.standardsbis.in.

This Indian Standard has been developed from Doc No.: ETD 25 (24769).

Amendments Issued Since Publication

Amend No.	Date of Issue	Text Affected

BUREAU OF INDIAN STANDARDS

Headquarters:

Manak Bhavan, 9 Bahadur Shah Zafar Marg, New Delhi 110002
Telephones: 2323 0131, 2323 3375, 2323 9402 *Website*: www.bis.gov.in

Regional Offices:		*Telephones*
Central	: 601/A, Konnectus Tower -1, 6th Floor, DMRC Building, Bhavbhuti Marg, New Delhi 110002	2323 7617
Eastern	: 8th Floor, Plot No 7/7 & 7/8, CP Block, Sector V, Salt Lake, Kolkata, West Bengal 700091	2367 0012 2320 9474
Northern	: Plot No. 4-A, Sector 27-B, Madhya Marg, Chandigarh 160019	265 9930
Southern	: C.I.T. Campus, IV Cross Road, Taramani, Chennai 600113	2254 1442 2254 1216
Western	: Manakalya, 4th Floor, NTH Complex (W Sector), F-10, MIDC, Andheri (East), Mumbai 400093	283 25838

Branches : AHMEDABAD, BENGALURU, BHOPAL, BHUBANESHWAR, CHANDIGARH, CHENNAI, COIMBATORE, DEHRADUN, DELHI, FARIDABAD, GHAZIABAD, GUWAHATI, HARYNA, HUBLI, HYDERABAD, JAIPUR, JAMMU & KASHMIR, JAMSHEDPUR, KOCHI, KOLKATA, LUCKNOW, MADURAI, MUMBAI, NAGPUR, NOIDA, PARWANOO, PATNA, PUNE, RAIPUR, RAJKOT, SURAT, VIJAYAWADA.

Published by BIS, New Delhi