SLOVENSKI STANDARD
oSIST prEN ISO 8102-20:2026

01-junij-2026

Električne zahteve za dvigala (lifte), tekoče stopnice in tekoče steze - 20. del: Kibernetska varnost (ISO/DIS 8102-20:2026)

Electrical requirements for lifts, escalators and moving walks - Part 20: Cybersecurity (ISO/DIS 8102-20:2026)

Elektrische Anforderungen für Aufzüge, Fahrtreppen und Fahrsteige - Teil 20: Cybersicherheit (ISO/DIS 8102-20:2026)

Exigences électriques pour les ascenseurs, les escaliers mécaniques et les trottoirs roulants - Partie 20 : Cybersécurité (ISO/DIS 8102-20:2026)

Ta slovenski standard je istoveten z: **prEN ISO 8102-20**

ICS:

35.030	Informacijska varnost	IT Security
91.140.90	Dvigala. Tekoče stopnice	Lifts. Escalators

oSIST prEN ISO 8102-20:2026 **en,fr,de**

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)

COPYRIGHT PROTECTED DOCUMENT

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.