INTERNATIONAL STANDARD

ISO 8102-20

First edition
2022-08

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

Reference number
ISO 8102-20:2022(E)

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 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.

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. 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.