NORME INTERNATIONALE

ISO 8102-20

Première édition
2022-08

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

Partie 20: **Cybersécurité**

Electrical requirements for lifts, escalators and moving walks —

Part 20: Cybersecurity

Numéro de référence
ISO 8102-20:2022(F)

ISO copyright office
Case postale 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Genève
Tél.: +41 22 749 01 11
E-mail: copyright@iso.org
Web: www.iso.org

Publié en Suisse

Sommaire

Page

Avant-propos

L'ISO (Organisation internationale de normalisation) est une fédération mondiale d'organismes nationaux de normalisation (comités membres de l'ISO). L'élaboration des Normes internationales est en général confiée aux comités techniques de l'ISO. Chaque comité membre intéressé par une étude a le droit de faire partie du comité technique créé à cet effet. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'ISO participent également aux travaux. L'ISO collabore étroitement avec la Commission électrotechnique internationale (IEC) en ce qui concerne la normalisation électrotechnique.

Les procédures utilisées pour élaborer le présent document et celles destinées à sa mise à jour sont décrites dans les Directives ISO/IEC, Partie 1. Il convient, en particulier, de prendre note des différents critères d'approbation requis pour les différents types de documents ISO. Le présent document a été rédigé conformément aux règles de rédaction données dans les Directives ISO/IEC, Partie 2 (voir www.iso.org/directives).

L'attention est attirée sur le fait que certains des éléments du présent document peuvent faire l'objet de droits de propriété intellectuelle ou de droits analogues. L'ISO ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de propriété et averti de leur existence. Les détails concernant les références aux droits de propriété intellectuelle ou autres droits analogues identifiés lors de l'élaboration du document sont indiqués dans l'Introduction et/ou dans la liste des déclarations de brevets reçues par l'ISO (voir www.iso.org/brevets).

Les appellations commerciales éventuellement mentionnées dans le présent document sont données pour information, par souci de commodité, à l'intention des utilisateurs et ne sauraient constituer un engagement.

Pour une explication de la nature volontaire des normes, la signification des termes et expressions spécifiques de l'ISO liés à l'évaluation de la conformité, ou pour toute information au sujet de l'adhésion de l'ISO aux principes de l'Organisation mondiale du commerce (OMC) concernant les obstacles techniques au commerce (OTC), voir www.iso.org/avant-propos.

Le présent document a été élaboré par le comité technique ISO/TC 178, *Ascenseurs, escaliers mécaniques et trottoirs roulants*.

Une liste de toutes les parties de la série ISO 8102 se trouve sur le site web de l'ISO.

Il convient que l'utilisateur adresse tout retour d'information ou toute question concernant le présent document à l'organisme national de normalisation de son pays. Une liste exhaustive desdits organismes se trouve à l'adresse www.iso.org/fr/members.html.

Introduction

Le présent document est une publication de sécurité de produit (voir le Guide IEC 120:2018).

Il a été élaboré en réponse aux exigences du marché et à une sensibilisation accrue à la cybersécurité. La norme de référence en matière de cybersécurité pour les technologies opérationnelles est la série IEC 62443. Le présent document aborde les exigences spécifiques à l'industrie qui sont nécessaires lors de l'application de la série IEC 62443.

Le principe fondamental de la cybersécurité repose sur un cycle de vie solide des processus de cybersécurité. Ce cycle de vie doit inclure des formations, des outils, des ressources et des processus adéquats pour développer, renforcer et maintenir la résilience de l'équipement commandé (EUC) contre les cyberattaques. La pensée cycle de vie est également une prémisse fondamentale des meilleures pratiques utilisées pour différentes normes et approches de cybersécurité.

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

Partie 20: Cybersécurité

1 Domaine d'application

Le présent document spécifie les exigences de cybersécurité pour les nouveaux ascenseurs, escaliers mécaniques et trottoirs roulants, dénommés dans le présent document « EUC » (Equipement Under Control ou « équipement commandé »), conçus conformément à la série ISO 8100. Il peut être appliqué à d'autres normes d'ascenseurs, d'escaliers mécaniques et de trottoirs roulants qui spécifient des exigences similaires, ainsi qu'à d'autres équipements d'ascenseurs raccordés à l'EUC.

Le présent document spécifie les exigences de produit et de système liées aux menaces de cybersécurité durant les étapes suivantes du cycle de vie:

— développement du produit (exigences relatives au processus et au produit);

— fabrication;

— installation;

— exploitation et maintenance;

— mise hors service.

Le présent document traite des rôles de fournisseur de produit et d'intégrateur de système tels qu'indiqués dans l'IEC 62443-4-1:2018, Figure 2, pour l'EUC.

Le présent document ne traite pas le rôle du propriétaire d'actif tel qu'indiqué dans l'IEC 62443-4-1:2018, Figure 2, mais définit les exigences à respecter pour le fournisseur de produit et l'intégrateur de système de l'EUC afin d'établir une documentation permettant au propriétaire d'actif, dénommé « propriétaire de l'EUC » dans le présent document, d'atteindre et de maintenir la sécurité de l'EUC.

Le présent document spécifie les exigences minimales de cybersécurité pour:

— les fonctions essentielles;

— les fonctions de sécurité;

— les fonctions d'alarme.

Le présent document s'applique aux EUC capables de se connecter à des systèmes externes tels que les réseaux des bâtiments, les services en nuage (ou cloud) ou les outils de service. La capacité de connexion peut exister par le biais d'équipements disponibles en permanence sur le site ou d'équipements temporairement amenés sur place lors des étapes d'installation, d'exploitation et de maintenance ou de mise hors service.

Les interfaces de l'EUC avec les systèmes et services externes font partie du domaine d'application du présent document. Les systèmes et services externes en tant que tels n'entrent pas dans le domaine d'application du présent document.

Le présent document ne s'applique pas aux EUC installés avant sa date de publication.

2 Références normatives

Les documents suivants sont cités dans le texte de sorte qu'ils constituent, pour tout ou partie de leur contenu, des exigences du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

ISO 8100-1:2019, *Elévateurs pour le transport de personnes et d'objets — Partie 1: Règles de sécurité pour la construction et l'installation d'ascenseurs et d'ascenseurs de charge*

IEC/TS 62443-1-1:2009, *Industrial communication networks — Network and system security — Part 1-1: Terminology, concepts and models (disponible en anglais seulement)*

IEC 62443-3-2:2020, *Sécurité des systèmes d'automatisation et de commande industriels — Partie 3-2: Évaluation des risques de sécurité pour la conception des systèmes*

IEC 62443-3-3:2013, *Réseaux industriels de communication — Sécurité dans les réseaux et les systèmes — Partie 3-3: Exigences de sécurité des systèmes et niveaux de sécurité*

IEC 62443-4-1:2018, *Sécurité des automatismes industriels et des systèmes de commande — Partie 4-1: Exigences relatives au cycle de développement de produit sécurisé*

IEC 62443-4-2:2019, *Sécurité des systèmes d'automatisation et de commande industrielles — Partie 4-2: Exigences de sécurité technique des composants IACS*

3 Termes, définitions et abréviations

3.1 Termes et définitions

Pour les besoins du présent document, les termes et définitions de l'ISO 8100-1:2019, l'IEC/TS 62443-1-1:2009, l'IEC 62443-3-2:2020 ainsi que les suivants, s'appliquent.

L'ISO et l'IEC tiennent à jour des bases de données terminologiques destinées à être utilisées en normalisation, consultables aux adresses suivantes:

— ISO Online browsing platform: disponible à l'adresse https://www.iso.org/obp;

— IEC Electropedia: disponible à l'adresse https://www.electropedia.org/.

3.1.1
cybersécurité
mesures prises pour protéger un ordinateur ou un système informatique contre un accès non autorisé ou une attaque

Note 1 à l'article: Dans le présent document, les systèmes de commande des ascenseurs, escaliers mécaniques et trottoirs roulants sont considérés comme des systèmes informatiques.

Note 2 à l'article: Dans le présent document, le terme « sécurité » inclut la cybersécurité.

[SOURCE: IEC 62443-3-2:2020, 3.1.7, modifié — La Note 1 à l'article a été modifiée et la Note 2 à l'article a été ajoutée.]

3.1.2
équipement commandé
EUC
ascenseur, escalier mécanique ou trottoir roulant

3.1.3
propriétaire de l'équipement commandé
propriétaire de l'EUC
individu ou organisme responsable de l'EUC

Note 1 à l'article: Le propriétaire de l'EUC équivaut au « propriétaire d'actif » défini dans l'IEC 62443-4-1:2018, 3.1.6.

[SOURCE: IEC 62443-4-1:2018, 3.1.6, modifié — Dans la définition, le texte « d'un ou de plusieurs IACS » a été remplacé par « de l'EUC » et la Note 1 à l'article a été ajoutée.]

3.2 Abréviations

CCSC Common Component Security Constraint (contrainte commune en matière de sécurité du composant)

DM Defect Management (gestion des défauts)

EDR Embedded Device Requirement (exigence relative aux appareils intégrés)

EUC Equipment Under Control (équipement commandé)

FR Foundational Requirement (exigence fondamentale)

HDR Host Device Requirement (exigence relative aux appareils hôtes)

IACS Industrial Automation and Control System (système d'automatisation et de commande industrielles)

NDR Network Device Requirement (exigence relative aux appareils de réseaux)

RACI Réalisateur, Approbateur, Consulté et Informé

RE Requirement Enhancement (amélioration d'exigences)

SAR Software Application Requirement (exigence relative aux applications logicielles)

SD Secure Design (conception sécurisée)

SG Security Guidelines (lignes directrices de sécurité)

SI Secure Implementation (mise en œuvre sécurisée)

SIL Safety Integrity Level (niveau d'intégrité de sécurité)

SL Security Level (niveau de sécurité)

SL-T Target Security Level (niveau de sécurité cible)

SM Security Management (gestion de la sécurité)

SR Security Requirement (exigences de sécurité)

SUM Security Update Management (gestion des mises à jour de sécurité)

SVV Security Verification and Validation (vérification et validation de sécurité)

4 Cycle de développement sécurisé des ascenseurs, escaliers mécaniques et trottoirs roulants

4.1 Généralités

Les exigences du présent article doivent s'appliquer au développement de composants et à l'intégration du système. Voir l'Annexe A pour obtenir des informations supplémentaires sur le cycle de développement sécurisé, l'Annexe B pour en savoir plus sur les évaluations des risques de sécurité et l'Annexe C pour consulter la liste des pratiques de sécurité.

4.2 Gestion de la sécurité

4.2.1 Processus de développement

Les exigences de l'IEC 62443-4-1:2018, SM-1: Processus de développement, doivent s'appliquer.

4.2.2 Identification des responsabilités

Les exigences de l'IEC 62443-4-1:2018, SM-2: Identification des responsabilités, doivent s'appliquer.

4.2.3 Identification de l'applicabilité

Les exigences de l'IEC 62443-4-1:2018, SM-3: Identification de l'applicabilité, doivent s'appliquer.

4.2.4 Expertise en sécurité

Les exigences de l'IEC 62443-4-1:2018, SM-4: Expertise en sécurité, doivent s'appliquer.

Outre la cybersécurité, les programmes de formation doivent également comprendre une expertise en sécurité spécifique à l'EUC.

NOTE L'ISO/TR 221004:2018 donne aux fabricants de machines des recommandations sur les aspects de sécurité des machines.

4.2.5 Définition du processus

Les exigences de l'IEC 62443-4-1:2018, SM-5: Définition du processus, doivent s'appliquer.

4.2.6 Intégrité de fichier

Les exigences de l'IEC 62443-4-1:2018, SM-6: Intégrité de fichier, doivent s'appliquer.

Les informations pour l'utilisation doivent indiquer les moyens de vérifier l'intégrité de tous les scripts, fichiers exécutables et autres fichiers importants inclus dans un produit.

4.2.7 Sécurité de l'environnement de développement

Les exigences de l'IEC 62443-4-1:2018, SM-7: Sécurité de l'environnement de développement, doivent s'appliquer.

4.2.8 Commandes pour les clés privées

Les exigences de l'IEC 62443-4-1:2018, SM-8: Commandes pour les clés privées, doivent s'appliquer.

4.2.9 Exigences de sécurité pour les composants fournis par des prestataires externes

Les exigences de l'IEC 62443-4-1:2018, SM-9: Exigences de sécurité pour les composants fournis par des prestataires externes, doivent s'appliquer.

Les informations pour l'utilisation doivent indiquer la nécessité d'identifier et de gérer les risques de sécurité de tous les composants fournis par des prestataires externes utilisés dans le produit.

4.2.10 Composants développés à la demande par des fournisseurs tiers

Les exigences de l'IEC 62443-4-1:2018, SM-10: Composants développés à la demande par des fournisseurs tiers, doivent s'appliquer.

4.2.11 Évaluation et traitement des questions liées à la sécurité

Les exigences de l'IEC 62443-4-1:2018, SM-11: Évaluation et traitement des questions liées à la sécurité, doivent s'appliquer.

4.2.12 Vérification du processus

Les exigences de l'IEC 62443-4-1:2018, SM-12: Vérification du processus, doivent s'appliquer.

4.2.13 Amélioration continue

Les exigences de l'IEC 62443-4-1:2018, SM-13: Amélioration continue, doivent s'appliquer.

4.3 Spécification des exigences de sécurité

4.3.1 Contexte de sécurité du produit

Les exigences de l'IEC 62443-4-1:2018, SR-1: Contexte de sécurité du produit, doivent s'appliquer.

Les informations pour l'utilisation doivent indiquer les hypothèses concernant l'utilisation de l'EUC.

4.3.2 Modèle des menaces

Les exigences de l'IEC 62443-4-1:2018, SR-2: Modèle des menaces, doivent s'appliquer.

Le modèle des menaces doit tenir compte du cycle de vie complet de l'EUC.

4.3.3 Exigences de sécurité du produit

Les exigences de l'IEC 62443-4-1:2018, SR-3: Exigences de sécurité du produit, doivent s'appliquer.

4.3.4 Contenu des exigences de sécurité du produit

Les exigences de l'IEC 62443-4-1:2018, SR-4: Contenu des exigences de sécurité du produit, doivent s'appliquer.

4.3.5 Examen des exigences de sécurité

Les exigences de l'IEC 62443-4-1:2018, SR-5: Examen des exigences de sécurité, doivent s'appliquer.

4.4 Sécurité par la conception

4.4.1 Principes de conception sécurisée

Les exigences de l'IEC 62443-4-1:2018, SD-1: Principes de conception sécurisée, doivent s'appliquer.

4.4.2 Conception de la défense en profondeur

Les exigences de l'IEC 62443-4-1:2018, SD-2: Conception de la défense en profondeur, doivent s'appliquer.

4.4.3 Examen de la conception de sécurité

Les exigences de l'IEC 62443-4-1:2018, SD-3: Examen de la conception de sécurité, doivent s'appliquer.

4.4.4 Meilleures pratiques de conception sécurisée

Les exigences de l'IEC 62443-4-1:2018, SD-4: Meilleures pratiques de conception sécurisée, doivent s'appliquer.

4.5 Mise en œuvre sécurisée

4.5.1 Examen de la mise en œuvre de sécurité

Les exigences de l'IEC 62443-4-1:2018, SI-1: Examen de la mise en œuvre de sécurité, doivent s'appliquer.

4.5.2 Normes de codage sécurisé

Les exigences de l'IEC 62443-4-1:2018, SI-2: Normes de codage sécurisé, doivent s'appliquer.

4.6 Essai de vérification et de validation de la sécurité

4.6.1 Essais des exigences de sécurité

Les exigences de l'IEC 62443-4-1:2018, SVV-1: Essais des exigences de sécurité, doivent s'appliquer.

4.6.2 Essais d'atténuation des menaces

Les exigences de l'IEC 62443-4-1:2018, SVV-2: Essais d'atténuation des menaces, doivent s'appliquer.

4.6.3 Essais de vulnérabilité

Les exigences de l'IEC 62443-4-1:2018, SVV-3: Essais de vulnérabilité, doivent s'appliquer.

4.6.4 Essais de pénétration

Les exigences de l'IEC 62443-4-1:2018, SVV-4: Essais de pénétration, doivent s'appliquer.

4.6.5 Indépendance des personnes qui procèdent aux essais

Les exigences de l'IEC 62443-4-1:2018, SVV-5: Indépendance des personnes qui procèdent aux essais, doivent s'appliquer.

4.7 Gestion des questions liées à la sécurité

4.7.1 Réception des notifications de questions liées à la sécurité

Les exigences de l'IEC 62443-4-1:2018, DM-1: Réception des notifications de questions liées à la sécurité, doivent s'appliquer.

Les informations pour l'utilisation doivent indiquer les moyens de signaler les questions liées à la sécurité.

4.7.2 Examen des questions liées à la sécurité

Les exigences de l'IEC 62443-4-1:2018, DM-2: Examen des questions liées à la sécurité, doivent s'appliquer.

4.7.3 Évaluation des questions liées à la sécurité

Les exigences de l'IEC 62443-4-1:2018, DM-3: Évaluation des questions liées à la sécurité, doivent s'appliquer.

4.7.4 Traitement des questions liées à la sécurité

Les exigences de l'IEC 62443-4-1:2018, DM-4: Traitement des questions liées à la sécurité, doivent s'appliquer.

Les informations pour l'utilisation doivent indiquer la nécessité de traiter les questions liées à la sécurité pendant toute la durée du cycle de vie de l'EUC.

4.7.5 Divulgation des questions liées à la sécurité

Les exigences de l'IEC 62443-4-1:2018, DM-5: Divulgation des questions liées à la sécurité, doivent s'appliquer.

4.7.6 Examen périodique de la pratique de gestion des défauts de sécurité

Les exigences de l'IEC 62443-4-1:2018, DM-6: Examen périodique de la pratique de gestion des défauts de sécurité, doivent s'appliquer.

4.8 Gestion des mises à jour de sécurité

4.8.1 Qualification de mise à jour de sécurité

Les exigences de l'IEC 62443-4-1:2018, SUM-1: Qualification de mise à jour de sécurité, doivent s'appliquer.

4.8.2 Documentation de mise à jour de sécurité

Les exigences de l'IEC 62443-4-1:2018, SUM-2: Documentation de mise à jour de sécurité, doivent s'appliquer.

Les informations pour l'utilisation doivent indiquer les moyens d'obtenir des informations sur les mises à jour de sécurité.

4.8.3 Documentation de mise à jour de sécurité des systèmes d'exploitation ou de composants dépendants

Les exigences de l'IEC 62443-4-1:2018, SUM-3: Documentation de mise à jour de sécurité des systèmes d'exploitation ou de composants dépendants, doivent s'appliquer.

4.8.4 Livraison de mise à jour de sécurité

Les exigences de l'IEC 62443-4-1:2018, SUM-4: Livraison de mise à jour de sécurité, doivent s'appliquer.

Les informations pour l'utilisation doivent indiquer les moyens de vérifier l'authenticité du correctif de sécurité.