INTERNATIONAL STANDARD

ISO 8102-6

First edition
2019-01

Electrical requirements for lifts, escalators and moving walks —

Part 6: Programmable electronic systems in safety-related applications for escalators and moving walks (PESSRAE)

Exigences électriques pour ascenseurs, escaliers mécaniques et trottoirs roulants —

Partie 6: Systèmes électroniques programmables dans les applications liées à la sécurité pour escaliers mécaniques et trottoirs roulants

Reference number
ISO 8102-6:2019(E)

COPYRIGHT PROTECTED DOCUMENT

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
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*.

This document cancels and replaces ISO 22201-2:2013.

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

0.1 General

Systems comprised of electrical and/or electronic elements have been used for many years to perform safety functions in most application sectors. Computer-based systems, generically referred to as programmable electronic systems, are being used in many application sectors to perform non-safety functions and, increasingly, to perform safety functions. If computer system technology is to be effectively and safely exploited, it is essential that those responsible for making decisions have sufficient guidance on the safety aspects on which to make these decisions. In most situations, safety is achieved by a number of protective systems that rely on many technologies (for example mechanical, hydraulic, pneumatic, electrical, electronic, programmable electronic). Therefore, any safety strategy needs to consider not only all the components within an individual system (for example sensors, controlling devices and actuators) but also all the safety-related elements making up the total combination of safety-related systems.

This document is based on the guidelines provided in generic standards IEC 62061 and EN 115-1:2008.

The requirements given in this document recognize the fact that the product family covers a total range of escalators and moving walks used in residential buildings, offices, hospitals, hotels, industrial plants, etc. This document is the product family standard for escalators and moving walks and takes precedence over all aspects of the generic standard.

This document sets out the product-specific requirements for systems comprising programmable electronic elements that are used to perform safety functions in escalators and moving walks. This document has been developed so that consistent technical and performance requirements and rationale can be specified for programmable electronic system in safety-related application for escalators (PESSRAE) and moving walks.

Risk analysis, terminology, and technical solutions have been considered, taking into account the methods of the IEC 61508 series. The risk analysis of each safety function specified in Table 1 resulted in the classification of electric safety functions applied to PESSRAE. Tables 1 and 2 give the safety integrity level and functional requirements, respectively, for each electric safety function.

The safety integrity levels (SIL) specified in this document can also be applied to other technologies used to satisfy the safety functions specified in this document.

0.2 Harmonization with national escalator and moving walk standards

The application of this document is intended to be by reference within a national escalator and moving walk standards such as escalator and moving walk codes, standards, or laws. There are three reasons for this.

— to allow selective reference by national standards to specific escalator and moving walk safety functions described in this document. Not all escalator and moving walk safety functions identified in this document are called out in every national standard;

— to allow for future harmonization of national standards with escalator and moving walk safety functions identified in this document. Because some differences exist in the requirements for fulfilment of the safety objective of national escalator and moving walk standards and in national practice of escalator and moving walk use and maintenance, there are instances where the requirements for escalator and moving walk safety functions described in this document are based on the consensus work and agreement by ISO/TC 178. National bodies can choose to selectively harmonize with those escalator and moving walk safety functions that differ in the requirements called for by the existing national standards in future revisions;

— to allow for the application of this document where escalator and moving walk safety functions are new or deviate from those specified in this document. More and more, national escalator and moving walk legislations are moving to performance based requirements. For this reason the development of new or different escalator and moving walk safety functions can be foreseen in

product specific applications. For those who require escalator and moving walk safety functions that are new or different from those specified in this document, this document provides a verifiable method to establish the necessary level of safety integrity for those functions.

Electrical requirements for lifts, escalators and moving walks —

Part 6: Programmable electronic systems in safety-related applications for escalators and moving walks (PESSRAE)

1 Scope

1.1 This document is applicable to the product family of escalators and moving walks used in residential buildings, offices, hospitals, hotels, industrial plants, etc. This document covers those aspects that need to be addressed when programmable electronic systems are used to carry out electric safety functions for escalators and moving walks (PESSRAE). This document is applicable for escalator and moving walk safety functions that are identified in escalator and moving walk codes, standards, or laws that reference this document for PESSRAE application. The safety integrity levels (SILs) specified in this document are understood to be valid for PESSRAE application in the context of the referenced escalator and moving walk codes, standards, and laws in the Bibliography.

1.2 This document is also applicable for the application of PESSRAE that are new or deviate from those described in this document.

1.3 The requirements of this document regarding electrical safety/protective devices are such that it is not necessary to take into consideration the possibility of a failure of an electric safety/protective device complying with all the requirements of this document and other relevant standards.

This document:

a) uses safety integrity levels (SIL) for specifying the target failure rate for the safety functions to be implemented by the PESSRAE;

b) specifies the requirements for achieving safety integrity for a function but does not specify who is responsible for implementing and maintaining the requirements (for example, designers, suppliers, owner/operating company, contractor); this responsibility is assigned to different parties according to safety planning and national regulations;

c) applies to PE systems used in escalator and moving walk applications that meet the minimum requirements of a recognized escalator and moving walk standards, such as EN 115, ASME A17.1/CSA B44 or The Japan Building Standard Law Enforcement Order For Elevator and Escalator;

d) defines the relationship between this document and IEC 61508 and defines the relationship between this document and ISO 22200;

e) outlines the relationship between escalator and moving walk safety functions and their safe-state conditions;

f) applies to phases and activities that are specific to design of hardware and software but not the phases and activities which occur post design, for example sourcing and manufacturing;

h) provides requirements relating to the hardware and software safety validation;

i) establishes the safety integrity levels for specific escalator and moving walk safety functions;

j) specifies techniques/measures required for achieving the specified safety integrity levels;

k) defines a maximum level of performance (SIL 3) which can be achieved for a PESSRAE according to this document and defines a minimum level of performance (SIL 1).

1.4 This document does not cover:

a) hazards arising from the PE systems equipment itself such as electric shock etc.;

b) the concept of fail-safe that can be of value when the failure modes are well defined and the level of complexity is relatively low. The concept of fail-safe was considered inappropriate because of the full range of complexity of PESSRAE that are within the scope of this document;

c) other relevant requirements necessary for the complete application of a PESSRAE in an escalator and moving walk safety function, such as system integration specifications, temperature and humidity, the mechanical construction, mounting and labelling of switches, actuators, or sensors that contain PESSRAE.

d) foreseeable misuse involving security threats related to malevolent or unauthorized action. This document can be used in cases where a security threat analysis needs to be considered, provided that the specified SIL has been reassessed.

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 61508-1:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 1: General Requirements*

IEC 61508-2, *Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems*

IEC 61508-3, *Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 3: Software requirements*

IEC 61508-4, *Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 4: Definitions and abbreviations*

IEC 61508-5, *Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 5: Example of methods for the determination of Safety Integrity Levels*

ISO 22200, *Electromagnetic compatibility — Product family standard for lifts, escalators and moving walks — Immunity*

IEC 62061, *Safety of machinery — Functional safety of safety-related electrical, electronic and programmable electronic control systems*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in IEC 61508-4 and the following apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org/

3.1
non-SIL relevant safe-state requirement
required response to the actuation of a SIL rated safety function where the function performing this response is not required to be SIL-rated

Note 1 to entry: See Figure 4 and Table 2.

3.2
programmable electronic
PE
based on computer technology which can be composed of hardware, software, and of input and/or output units

Note 1 to entry: This term covers microelectronic devices based on one or more central processing units (CPUs) together with associated memories, etc.

EXAMPLE The following are all programmable electronic devices:

— microprocessors;

— micro-controllers;

— programmable controllers;

— field programmable gate array (FPGA);

— application specific integrated circuits (ASICs);

— programmable logic controllers (PLCs);

— other computer-based devices (for example smart sensors, transmitters, actuators).

3.3
programmable electronic system
PE system
system for control, protection or monitoring based on one or more programmable electronic devices, including all elements of the system such as power supplies, sensors and other input devices, data highways and other communication paths, and actuators and other output devices

Note 1 to entry: See Figure 1.

Note 2 to entry: A PE systems may perform functions that fulfil requirements for SIL-rated and non-SIL–rated function(s). The SIL rating of a function is only required to consider that portion of PE systems that perform the SIL relevant functional requirements.

Note 3 to entry: The programmable electronics are shown centrally located but can exist at several places in the PE systems.

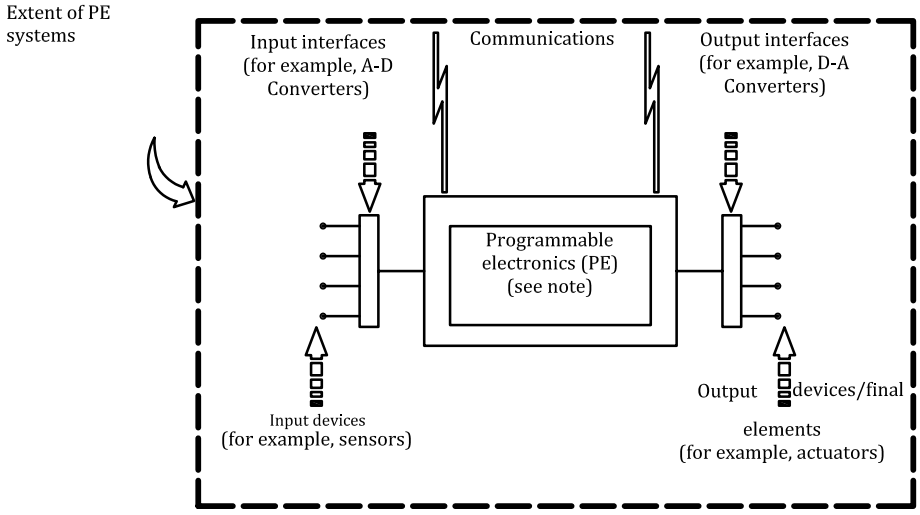

Figure 1 — Basic PE systems structure

3.4
programmable electronic systems in safety-related applications for escalators and moving walks
PESSRAE
application of a software-based PE systems in a safety-related system for escalators and moving walks

4.5
proof test
periodic test performed to detect dangerous hidden failures in a safety-related system so that, if necessary, a repair can restore the system to an “as new” condition or as close as practical to this condition

Note 1 to entry: In this document, the term “proof test” is used but it is recognized that a synonymous term is “periodical test”.

Note 2 to entry: The effectiveness of the proof test is dependent both on failure coverage and repair effectiveness. In practice, detecting 100 % of the hidden dangerous failures is not easily achieved for other than low-complexity E/E/PE safety-related systems. This should be the target. As a minimum, all the safety functions which are executed are checked according to the E/E/PE system safety requirements specification. If separate channels are used, these tests are done for each channel separately. For complex elements, it can be necessary to perform an analysis in order to demonstrate that the probability of hidden dangerous failure not detected by proof tests is negligible over the whole life duration of the E/E/PE safety-related system.

Note 3 to entry: A proof test needs some time to be achieved. During this time, the E/E/PE safety-related system may be inhibited partially or completely. The proof test duration can be neglected only if the part of the E/E/PE safety-related system under test remains available in case of a demand for operation or if the EUC is shut down during the test.

Note 4 to entry: During a proof test, the E/E/PE safety-related system may be partly or completely unavailable to respond to a demand for operation. The MTTR can be neglected for SIL calculations only if the EUC is shut down during repair or if other risk measures are put in place with equivalent effectiveness.

Note 5 to entry: A repair (including replacement) can be considered restoring the system to "as new”.

3.6
safety circuit
total combination of safety devices that fulfil all or a group of escalator and moving walk safety functions

Note 1 to entry: See Figure 2

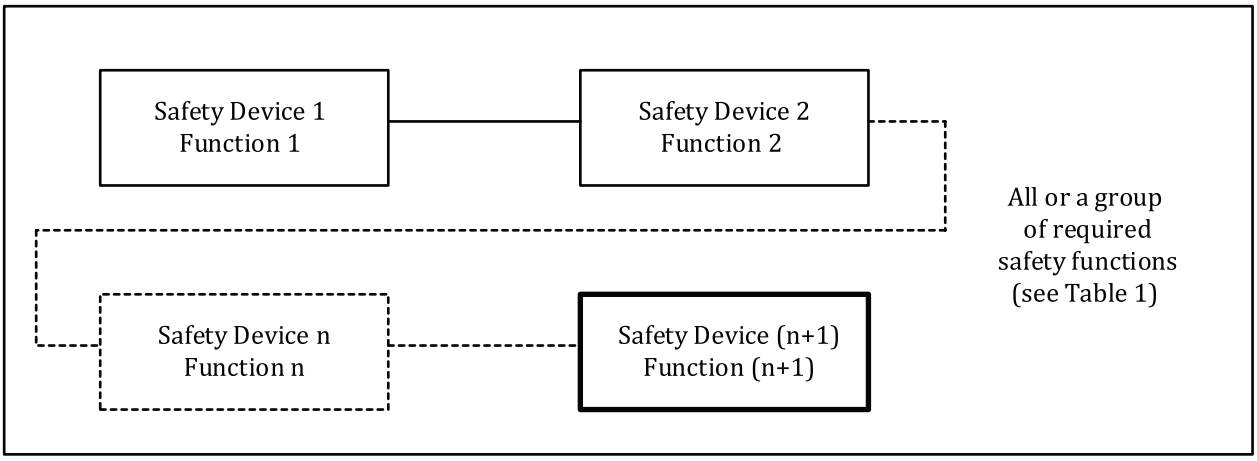

Figure 2 — Safety circuit

3.7
safety device
part of the safety-related system, including necessary control circuits, that has been designated to achieve, in its own right, an escalator and moving walk safety function and can consist of PE system elements and non-PE system elements

Note 1 to entry: See Figure 3 and Table 1.

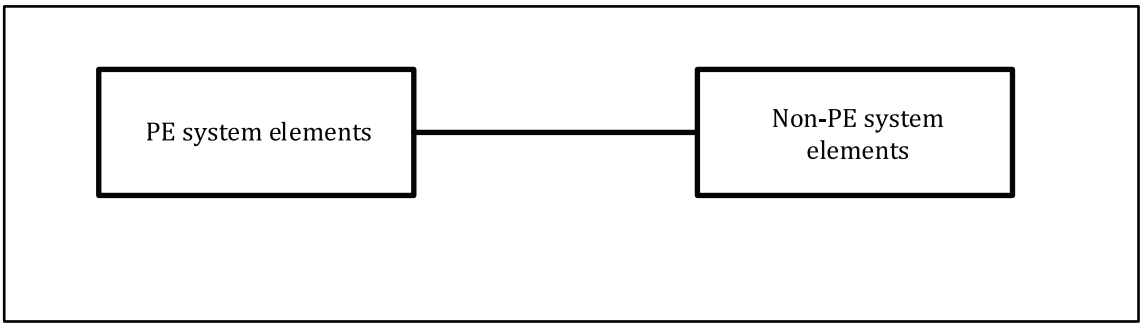

Figure 3 — Safety device

3.8
safety function
function to be implemented by a safety-related system, which is intended to achieve or maintain a safe-state of the escalator and moving walk, with respect to a specific hazardous event

Note 1 to entry: See Table 1.

Note 2 to entry: A safety function may include non-SIL relevant requirements, see Table 2.

3.9
safety-related system
system which consists of one or more safety devices performing one or more safety functions that can be based on programmable electronic (PE), electrical, electronic and/or mechanical elements of the escalator and moving walk

Note 1 to entry: The term includes all the hardware, software and supporting services (for example, power supplies) necessary to carry out the specified safety function [sensors, other input devices, final elements (actuators) and other output devices are therefore included in the safety-related system].

3.10
safety integrity level
SIL
discrete level for specifying the safety integrity requirements of the safety functions to be allocated to the programmable electronic safety-related system

Note 1 to entry: There are four SIL: safety integrity level 4 has the highest level of safety integrity and safety integrity level 1 has the lowest.

Note 2 to entry: In the context of this document, SIL 3 is the highest safety integrity level that is applied to escalators and moving walks.

Note 3 to entry: The SIL is indicative of a failure rate that includes all causes of failures (both random hardware failures and systematic failures), which lead to an unsafe state, for example hardware failures, software induced failures and failures due to electrical interference

3.11
SIL relevant safe-state requirement
part of the safety-related system where it is required to meet the specified SIL of the function

Note 1 to entry: See Figure 4 and Table 2.

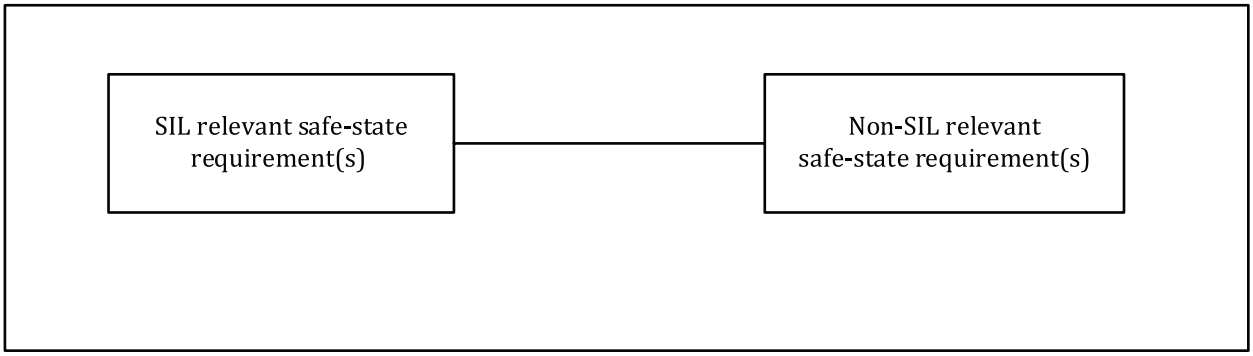

Figure 4 — Escalator and moving walk safety function

3.12
system reaction time
sum of the following two values:

a) the time period between the occurrence of a fault in the PESSRAE and the initiation of the corresponding action on the escalator and moving walk;

b) the time period for the escalator and moving walk to respond to the action, maintaining a safe state.

4 Requirements

4.1 General

4.1.1 Table 1 defines the safety function names, the associated escalator and moving walk functional description, applicable escalator and moving walk type and required SIL for the SIL relevant part of the safety function.

NOTE Safety functions refer to the escalator and moving walk functions that are identified in codes standards and laws that reference this document for PESSRAE application.

4.1.2 Table 2 defines the safe-state requirements when the safety functions in Table 1 are actuated. If a safety function actuates, the safety function shall cause the escalator and moving walk system to revert to the safe-state conditions specified by the requirements of Table 2.

4.1.3 PESSRAE shall consider the reaction time of the escalator and moving walk to respond to the safety function and internal fault detection in the necessary time to achieve the safe-state condition without hazard. Methods that fulfil internal fault detection shall consider the necessary system reaction time required by the SIL.

NOTE For example, if an internal fault is detected by comparison of data in a 2-channel system within the time necessary to meet the system reaction time, then it is not necessary to complete a variable memory range test within the system reaction time because safety integrity is verified by the 2-channel design.

4.2 Extended application of this document

4.2.1 General

The following requirements are provided to verify SILs and safe-state conditions for escalator and moving walk safety functions that:

— are new or deviate from the requirements provided in 6.3 and 6.4; or

— are referenced by codes and standards not harmonized with the requirements of the documents listed in Annex B.

4.2.2 Risk assessment

As an alternative to the requirements of 6.3 and/or 6.4, methods for the determination of the required safety integrity level shall be performed according to IEC 61508-5 or IEC 62061. The same methods shall be used to establish rationale for a new PESSRAE function and corresponding SIL or a revised PESSRAE function and/or SIL that deviate from the requirements of 6.3 and 6.4. The mean target failure frequency for the worst-case severity of any single potential consequence hazard scenario shall not exceed a frequency of 5×10^{-7} per year (see also Annex B).

4.2.3 Limits for specifying SIL for PESSRAE

Target failure measures required for specifying a PE systems in an escalator and moving walk safety-related function shall be no less than a SIL 1 and no greater than SIL 3. If a target failure measure requires higher than SIL 3, the system should be redesigned such that the required target failure measure shall be satisfied with SIL 3 or less. If an SIL lower than SIL 1 is required, a non-SIL rated PE systems may be used but shall not be classified as a PESSRAE. No PESSRAE shall have a SIL of less than SIL 1, even if it is applied to a safety function requiring less than SIL 1.

Applications that require the use of a single safety function of safety integrity level 4 are not typically required in the escalator and moving walk industry. Such applications shall be avoided because of the difficulty of achieving and maintaining such high levels of performance throughout the life cycle of the safety device. If the analysis results in a safety integrity level of 4 or higher being assigned to an escalator and moving walk safety function, consideration shall be given to changing the process design in such a way that it becomes more inherently safe or by adding additional layers of protection. These enhancements can perhaps then reduce safety integrity level requirements for the escalator and moving walk safety function. If the safety integrity level cannot be reduced, the target failure measure for the safety function shall be distributed across multiple PESSRAE of SIL 3 or less that are sufficiently independent, and certified in the application.

4.2.4 Safe-state requirements

For escalator and moving walk safety functions that are new or differ from those specified in 6.3 and 6.4, the designer shall identify the safe-state requirements in a manner similar to how they are described in Table 2.

4.3 Safety function SIL requirements

Table 1 provides the required SIL for each escalator and moving walk safety function.

Table 1 — Safety function SIL requirements

Id. No.	Escalator and moving walk safety function	Functional description	SIL
1	Check for excessive speed	Detect overspeed of the escalator or moving walk and remove power from machine motor and brake before the speed exceeds 20 % of rated speed	2
2	Check for unintentional reversal of the direction of travel	Detect unintended reversal of travel when operated in the ascending direction	2
3	Check for the closing of the auxiliary brake	Detect that the auxiliary brake has actuated	1
4	Check broken step-chain device	Detect the step chain is broken	1
5	Check extension or reduction of the distance between the driving and return devices	Detect extension or reduction of the distance between the driving and return devices	1
6	Check comb-step impact devices	Detect displacement of comb	1
7	Check for egress restriction device	Detect obstruction or barrier at the egress	2
8	Check for objects entrapped in the handrail entry	Detect objects or body parts entering the handrail entry	1
9	Check for the sagging of step or pallet	Detect a downward displacement of step or pallet at the transitions and before entering the comb	2
10	Check for a missing step or pallet	Check for missing step, pallet or dynamic skirt	2
11	Check for non-lifting of the operational braking system	Detect the machine brake has not lifted	1
12	Check for hand rail speed deviation	Detect a speed deviation of more than 15 % between the handrail and the steps or pallet	1
13	Check for opened inspection cover and open floor plate	Detect access cover and floor plates to inspection area are open	1
14	Check manual hand winding means	Detect before or when a winding means to move the rack will be used on the machine	1
15	Check actuation of stopping switch for emergency situations	Detect the actuation of the emergency stopping device at landings	1
16	Check broken drive-chain device	Detect a broken drive chain	1
17	Check escalator skirt obstruction device	Detect an obstruction between skirt and step	1
18	Check maintenance and repair stop switch	Detect actuation of stop switch in the maintenance area	2

Table 1 *(continued)*

Id. No.	Escalator and moving walk safety function	Functional description	SIL
19	Check step up thrust device	Detect an upward force on the step in the lower transition	1
20	Check disconnected motor safety device	Detect the motor is disconnected from the gearbox	1
21	Check step lateral displacement device	Detect excessive lateral displacement of steps	2
22	Check stop switch in inspection controls	Detect actuation of the stopping device on the inspection control panel	2
23	Check dynamic skirt panel obstruction device	Detect an entrapment between the dynamic skirt panel and the dynamic skirt panel cover	1
24	Check dynamic skirt panel in place	Detect missing dynamic skirt panel	1
25	Check inspection control actuation	Detect actuation of inspection control	2
26	Control and operating circuits		No less than the highest safety function applied in the safety circuit

4.4 SIL relevant and non-SIL relevant safe state requirements

Table 2 provides the required response of the escalator and moving walk to the escalator and moving walk safety functions of Table 1 and the SIL and non-SIL relevant requirements for each response from actuation of that function.

Table 2 — Safe state requirements

[References in Matrix (R#) appended to this table]		Remove motor and operational brake power	Remove power from main drive shaft brake	Block all other starting	Block other inspection control devices	Manual reset to start (see R6)	Bypass safety function	Block normal operation starting	Remove motor and operational brake power	Remove power from main drive shaft brake	Audible signal
Id.	**Escalator and moving walk safety function**	**SIL relevant**							**Non-SIL relevant**		
1	Check for excessive speed or unintentional reversal of the direction of travel	R1				X				X	
2	Check for the unintentional reversal of the direction of travel	X				X				X	
3	Check for the closing of the auxiliary brake								X		
4	Broken step-Chain Device	X				X					
5	Extension or reduction of the distance between the driving and return devices	X									

X The response is required for the safe-state condition when the safety function actuates or, where the PESSRAE detects an internal fault condition.

R1 Actuate before speed exceeds 120 % of nominal speed (no load speed). Note this is more stringent than at rated speed, rated load.

R2 Detects impact (no displacement required).

R4 All other starting includes all other inspection operating devices.

R5 When enabled, the following means shall be permitted to be rendered ineffective:

1) tandem and egress protection;

2) step levelling device;

3) missing step pallet;

4) non-lifting of braking system;

5) hand rail speed;

6) open the inspection cover and floor plates.

R6 Manual reset (of Failure Lock) to enable start: Requires restricted human intervention to reset the safety function in order to start or restart the escalator or moving walk. The escalator or moving walk start key does not perform a restricted reset. Note that the requirement for manual reset is not a function of the SIL; it is a function of possible hazardous situations after an event.

Table 2 *(continued)*

[References in Matrix (R#) appended to this table]		Remove motor and operational brake power	Remove power from main drive shaft brake	Block all other starting	Block other inspection control devices	Manual reset to start (see R6)	Bypass safety function	Block normal operation starting	Remove motor and operational brake power	Remove power from main drive shaft brake	Audible signal
Id.	**Escalator and moving walk safety function**	**SIL relevant**							**Non-SIL relevant**		
6	Comb-step impact devices	R2									
7	Escalator egress restriction device	X									
8	Check for foreign bodies being trapped in the handrail	X									
9	Check for the sagging of step or pallet	X				X					
10	Check for a missing step, pallet or dynamic skirt	X				X					
11	Check for the non-lifting of the operational brake	X				X					

X The response is required for the safe-state condition when the safety function actuates or, where the PESSRAE detects an internal fault condition.

R1 Actuate before speed exceeds 120 % of nominal speed (no load speed). Note this is more stringent than at rated speed, rated load.

R2 Detects impact (no displacement required).

R4 All other starting includes all other inspection operating devices.

R5 When enabled, the following means shall be permitted to be rendered ineffective:

1) tandem and egress protection;

2) step levelling device;

3) missing step pallet;

4) non-lifting of braking system;

5) hand rail speed;

6) open the inspection cover and floor plates.

R6 Manual reset (of Failure Lock) to enable start: Requires restricted human intervention to reset the safety function in order to start or restart the escalator or moving walk. The escalator or moving walk start key does not perform a restricted reset. Note that the requirement for manual reset is not a function of the SIL; it is a function of possible hazardous situations after an event.

Table 2 *(continued)*

[References in Matrix (R#) appended to this table]		Remove motor and operational brake power	Remove power from main drive shaft brake	Block all other starting	Block other inspection control devices	Manual reset to start (see R6)	Bypass safety function	Block normal operation starting	Remove motor and operational brake power	Remove power from main drive shaft brake	Audible signal
Id.	**Escalator and moving walk safety function**	**SIL relevant**							**Non-SIL relevant**		
12	Check for handrail speed deviation	R3									X
13	Check for opened inspection cover	X									
14	Check manual hand winding means	X									
15	Stopping switch for emergency situations	X									
16	Drive chain device	X	X			X					
17	Escalator skirt obstruction device	X									

X The response is required for the safe-state condition when the safety function actuates or, where the PESSRAE detects an internal fault condition.

R1 Actuate before speed exceeds 120 % of nominal speed (no load speed). Note this is more stringent than at rated speed, rated load.

R2 Detects impact (no displacement required).

R4 All other starting includes all other inspection operating devices.

R5 When enabled, the following means shall be permitted to be rendered ineffective:

1) tandem and egress protection;

2) step levelling device;

3) missing step pallet;

4) non-lifting of braking system;

5) hand rail speed;

6) open the inspection cover and floor plates.

R6 Manual reset (of Failure Lock) to enable start: Requires restricted human intervention to reset the safety function in order to start or restart the escalator or moving walk. The escalator or moving walk start key does not perform a restricted reset. Note that the requirement for manual reset is not a function of the SIL; it is a function of possible hazardous situations after an event.

Table 2 *(continued)*

[References in Matrix (R#) appended to this table]		Remove motor and operational brake power	Remove power from main drive shaft brake	Block all other starting	Block other inspection control devices	Manual reset to start (see R6)	Bypass safety function	Block normal operation starting	Remove motor and operational brake power	Remove power from main drive shaft brake	Audible signal
Id.	**Escalator and moving walk safety function**	**SIL relevant**							**Non-SIL relevant**		
18	Maintenance and repair stop switch	X									
19	Step up thrust device	X									
20	Disconnected motor safety device	X				X					
21	Step lateral displacement device	X				X					
22	Stop switch in inspection controls	X									

X The response is required for the safe-state condition when the safety function actuates or, where the PESSRAE detects an internal fault condition.

R1 Actuate before speed exceeds 120 % of nominal speed (no load speed). Note this is more stringent than at rated speed, rated load.

R2 Detects impact (no displacement required).

R4 All other starting includes all other inspection operating devices.

R5 When enabled, the following means shall be permitted to be rendered ineffective:

1) tandem and egress protection;

2) step levelling device;

3) missing step pallet;

4) non-lifting of braking system;

5) hand rail speed;

6) open the inspection cover and floor plates.

R6 Manual reset (of Failure Lock) to enable start: Requires restricted human intervention to reset the safety function in order to start or restart the escalator or moving walk. The escalator or moving walk start key does not perform a restricted reset. Note that the requirement for manual reset is not a function of the SIL; it is a function of possible hazardous situations after an event.

Table 2 *(continued)*

[References in Matrix (R#) appended to this table]		Remove motor and operational brake power	Remove power from main drive shaft brake	Block all other starting	Block other inspection control devices	Manual reset to start (see R6)	Bypass safety function	Block normal operation starting	Remove motor and operational brake power	Remove power from main drive shaft brake	Audible signal
Id.	**Escalator and moving walk safety function**	**SIL relevant**							**Non-SIL relevant**		
23	Dynamic skirt panel obstruction device	X				X					
24	Check dynamic skirt panel in place	X				X					
25	Inspection station actuation			R4			R5				

X The response is required for the safe-state condition when the safety function actuates or, where the PESSRAE detects an internal fault condition.

R1 Actuate before speed exceeds 120 % of nominal speed (no load speed). Note this is more stringent than at rated speed, rated load.

R2 Detects impact (no displacement required).

R4 All other starting includes all other inspection operating devices.

R5 When enabled, the following means shall be permitted to be rendered ineffective:

1) tandem and egress protection;

2) step levelling device;

3) missing step pallet;

4) non-lifting of braking system;

5) hand rail speed;

6) open the inspection cover and floor plates.

R6 Manual reset (of Failure Lock) to enable start: Requires restricted human intervention to reset the safety function in order to start or restart the escalator or moving walk. The escalator or moving walk start key does not perform a restricted reset. Note that the requirement for manual reset is not a function of the SIL; it is a function of possible hazardous situations after an event.

4.5 Implementation and demonstration requirements for verification of SIL compliance

4.5.1 General

The Safety Integrity Level of a PESSRAE shall be verified in conformance with the requirements of this subclause.

4.5.2 Required techniques and measures to implement and demonstrate PE systems compliance with specified safety integrity levels in this document

4.5.2.1 Techniques and measures necessary to implement and demonstrate compliance with SIL 1 to SIL 3 shall be satisfied by the techniques and measures of Annex A.

4.5.2.2 Where two or more safety functions are implemented with a common safety circuit, the SIL of this common circuit shall be at least as high as the highest SIL rating of the escalators and moving walk safety functions included in that circuit (see definition of safety circuit).

4.5.3 Loss of power after a PESSRAE device has actuated

4.5.3.1 Where a manual reset is not required for the function, a PESSRAE may revert to a normal operating mode after a power recovery condition and the device output state shall be determined by input conditions that exist after the power recovery.

4.5.3.2 Where a manual reset is required (see Table 2), the PESSRAE output shall revert to its output state just before the power loss.

Annex A
(normative)

Techniques and measures to implement, verify, and maintain SIL compliance

A.1 General

A.1.1 Techniques and measures to be used to satisfy the SIL requirements of this document

Techniques and measures necessary to implement and demonstrate PESSRAE SIL compliance shall be satisfied by the techniques and measures provided in A.2 using IEC 61508-2 and IEC 61508-3.

A.1.2 Instruction manual

A.1.2.1 General

The manufacturer shall provide an instruction manual.

Where the functional verification of the PESSRAE is not possible during normal operation of the escalators and moving walks, information shall be provided in the instruction manual to enable functional verification to be carried out. The instruction manual shall also inform about the following so that they can be carried out effectively and without danger:

— assembly;

— connection;

— adjustment;

— maintenance and repair;

— identification, marking, labelling, certification and listing;

— frequency of functional verification.

A.1.2.2 General requirements on maintenance and repair for the instruction manual

As required by the manufacturer, the instruction manual shall provide the following concerning maintenance and repair of a PESSRAE:

— unique requirements and/or precautions for training of maintenance personnel to sustain full functional performance of the PESSRAE to its SIL;

— proof-test, preventive and breakdown maintenance activities;

— the unique measures and techniques to be used for maintenance;

— verification and documentation requirements of adherence to maintenance activities;

— when maintenance activities shall take place;

— ensuring that test equipment used during normal maintenance activities is properly calibrated and maintained;

— the maintenance and repair activities to be followed when faults or failures occur in the PESSRAE including:

  — activities for fault diagnostics and repair;

  — activities for revalidation;

  — maintenance and failure reporting requirements.

A.1.3 Maintenance or maintainability design requirements

The design of a PESSRAE shall allow for testing either end-to-end or in parts. Where the expected interval between scheduled testing is greater than the proof-test interval used to maintain the SIL rating of the PESSRAE, then appropriate provisions for testing are required.

NOTE The term end-to-end means from sensor end to safe-state actuation. When automatic proof testing is required, provisions for testing are an integral part of the SIL rated design to test for undetected failures.

A.1.4 EMC immunity

A PESSRAE shall fulfil the “safety circuit” test levels specified in ISO 22200 for the SIL relevant safe-state requirements. Non-SIL relevant safe-state requirements shall fulfil “general function circuits” and “all circuits” test levels in ISO 22200. Local radio telecommunications regulations apply where radio frequency is intentionally used for PESSRAE.

A.2 Techniques and measures to implement and demonstrate SIL compliance using IEC 61508-2 and IEC 61508-3

A.2.1 General requirements

A.2.1.1 This clause provides the requirements for the application of the IEC 61508 series where it is used for the implementation and demonstration of PESSRAE SIL compliance.

A.2.1.2 For the purposes of this document, the SIL shall represent the requirement for a device operating in the low demand mode and the probability of failure to perform its safety function on demand as specified in IEC 61508-1:2010, Table 2. However, where a PESSRAE is used for continuous control to maintain functional safety, the SIL shall represent the requirement for a PESSRAE considered operating in the high demand mode and the dangerous failure rate shall be used (see IEC 61508-1:2010, Table 3).

When there is a possibility that some combination of output states of a subsystem can directly cause a hazardous event, then it should be necessary to regard the detection of dangerous faults in the subsystem as a safety function operating in the continuous mode.

A.2.1.3 Device(s) and software used to perform non-SIL rated requirements shall not be used to implement a SIL relevant requirement of a PESSRAE unless these device(s) and software have also been included in the rating of the SIL for the safety-related function.

A.2.1.4 The detection of a dangerous fault (by diagnostic tests, proof tests or by any other means) in any PESSRAE subsystem that can tolerate a single fault shall result in the specified safe-state of Table 2. If necessary, to maintain the integrity of the PESSRAE and maintain the safe-state condition before a second fault in the same subsystem that can lead to a dangerous condition, a manual reset shall be required to remove the PESSRAE from the safe-state condition.

Where the above actions depend on an operator or remote sub-system taking specific actions in response to an alarm of a dangerous fault, then the alarm shall be considered part of the SIL relevant function of the PESSRAE.

A.2.2 Implementation and SIL compliance

Implementation of SIL compliance for a PESSRAE shall be in accordance with the guidelines and measures of IEC 61508-2 for hardware and IEC 61508-3 for software.

NOTE It is possible to use several lower safety integrity level systems to satisfy the need for a higher safety integrity level function provided that adequate levels of independence are achieved, and certified in the application.

Annex B
(informative)

Example of risk reduction decision table

An example of a risk-reduction decision table for the application of PESSRAL is given as Table B.1 and the associated corrective action is summarized in Table B.2. The definitions of the "Potential safety hazard consequences" are as follows:

a) Catastrophic: Total loss of the safety objective within the scope of the document.

b) Critical: Permanent partial loss of the safety objective within the scope of the document.

c) Marginal: Temporary loss of the safety objective within the scope of the document.

d) Negligible: Negligible or no loss of the safety objective within the scope of the document.

Table B.1 — Risk-reduction decision table

Frequency of consequence per year per unit (escalator or moving walk) ***F***		**Potential safety hazard consequence**			
Range	**Mean value**	**1** Catastrophic	**2** Critical	**3** Marginal	**4** Negligible
$F \geq 0{,}01$	0,01	IA	IIA	IIIA	IV
$0{,}001 \leq F < 0{,}01$	0,005	IB	IIB	IIIB	IV
$0{,}000\ 1 \leq F < 0{,}001$	0,000 5	IC	IIC	IIIC	IVC
$0{,}000\ 01 \leq F < 0{,}000\ 1$	0,000 05	ID	IID	IIID	IVD
$0{,}000\ 001 \leq F < 0{,}000\ 01$	0,000 005	IE	IIE	IIIE	IVE
$F < 0{,}000\ 001$	4,7619E-07	IF	IIF	IIIF	IVF

Table B.2 — Corrective action — Risk reduction requirements

IA, IB, IC, ID, IE, IIA, IIB, IIC, IIIA, IIIB	Corrective action required to mitigate the effect and if practicable, eliminate it
IID, IIE, IIIC, IIID, IVA, IVB	Review and determine if any further mitigation is technically practicable
IF, IIF, IIIE, IIIF, IVC, IVD, IVE, IVF	No action required

Bibliography

[1] ISO 690, *Information and documentation — Guidelines for bibliographic references and citations to information resources*

[2] ISO 80000 (all parts), *Quantities and units*

[3] ISO/IEC TR 10000-1, *Information technology — Framework and taxonomy of International Standardized Profiles — Part 1: General principles and documentation framework*

[4] IEC 27 (all parts), *Letter symbols to be used in electrical technology*

[5] IEC 60664-1, *Insulation coordination for equipment within low-voltage systems — Part 1: Principles, requirements and tests*

[6] IEC 60950, *Information technology equipment — Safety*

[7] IEC 61508-6, *Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3*

[8] IEC 61508-7, *Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 7: Overview of techniques and measures*

[9] EN 115-1, *Safety of escalators and moving walks — Part 1: Construction and installation*

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

[11] The Building Standards Law of Japan. *Enforcement Order (for Elevator and Escalator)*

ICS 91.140.90

Price based on 20 pages