DRAFT INTERNATIONAL STANDARD

ISO/DIS 22201-2

ISO/TC **178**

Secretariat: **AFNOR**

Voting begins on:
2016-01-04

Voting terminates on:
2016-04-04

Lifts (elevators), escalators and moving walks — Programmable electronic systems in safety related applications —

Part 2:
Escalators and moving walks (PESSRAE)

Ascenseurs, escaliers mécaniques et trottoirs roulants — Systèmes électroniques programmables dans les applications liées à la sécurité —

Partie 2: Escaliers mécaniques et trottoirs roulants

ICS: 91.140.90

Reference number
ISO/DIS 22201-2:2015(E)

COPYRIGHT PROTECTED DOCUMENT

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

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. 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. 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.

The committee responsible for this document is ISO/TC 178, *Lifts, escalators and moving walks*.

ISO 22201 consists of the following parts, under the general title *Lifts (elevators), escalators and moving walks — Programmable electronic systems in safety-related applications*:

— *Part 1: Lifts (elevator) (PESSRAL)*

— *Part 2: Escalators and moving walks (PESSRAE)*

— *Part 3: Life cycle guideline for programmable electronic systems related to PESSRAL and PESSRAE* [Technical Report]

Introduction

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). Any safety strategy must therefore 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 International Standard is based upon the guidelines provided in the generic International Electrotechnical Commission (IEC) Standard IEC 62061 and Comité Européen de Normalisation (CEN) Standard EN 115-1:2008.

The requirements given in this International Standard 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 International Standard is the product family standard for escalators and moving walks and takes precedence over all aspects of the generic standard.

This International Standard sets out the product specific requirements for systems comprised of programmable electronic element that are used to perform safety functions in escalators and moving walks. This International Standard has been developed in order that consistent technical and performance requirements and rational be specified for Programmable Electronic System in Safety-Related Application for Escalators and moving walks (PESSRAE).

Risk analysis, terminology, and technical solutions have been considered taking into account the methods of the IEC 61508 series of standards. 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 International Standard may also be applied to other technologies used to satisfy the safety functions specified in this International Standard.

Harmonization with national escalator and moving walk norms:

Application of this International Standard:

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

— To allow selective reference by national norms to specific escalator and moving walk safety functions described in this International Standard. Not all escalator and moving walk safety functions identified in this International Standard are called out in every national norm.

— To allow for future harmonization of national norms with escalator and moving walk safety functions identified in this International Standard. Because there exist some differences in the requirements for fulfilment of the safety objective of national escalator and moving walk norms 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 International Standard are based on the consensus work and agreement by the ISO committee responsible for this International Standard. National bodies may choose to selectively harmonize with those escalator and moving walk safety functions that differ in the requirements called for by the existing national norm in future norm revisions.

— To allow for the application of this International Standard where escalator and moving walk safety functions are new or deviate from those specified in this International Standard. 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 International Standard, this International Standard provides a verifiable method to establish the necessary level of safety integrity for those functions.

Lifts (elevators), escalators and moving walks — Programmable electronic systems in safety related applications —

Part 2: Escalators and moving walks (PESSRAE)

1 Scope

1.1 This International Standard is applicable to the product family of escalators and moving walks used in residential buildings, offices, hospitals, hotels, industrial plants, etc. This International Standard 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 International Standard is applicable for escalator and moving walk safety functions that are identified in escalator and moving walk codes, standards, or laws that reference this International Standard for PESSRAE application. The safety integrity levels (SILs) specified in this International Standard are understood to be valid for PESSRAE application in the context of the referenced escalator and moving walk codes, standards, and laws in Annex B.

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

1.3 The requirements of this International Standard 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 International Standard and other relevant standards.

In particular, this International Standard:

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 escalator and moving walk laws such as The Japan Building Standard Law Enforcement Order For Elevator and Escalator;

d) defines the relationship between this International Standard and IEC 61508 and defines the relationship between this International Standard and the EMC Standard for Escalators and moving walks on immunity, 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 those 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 PESSR-AE according to this International Standard and defines a minimum level of performance (SIL 1).

1.4 This International Standard does not cover:

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

b) the concept of fail-safe that may 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 PESSR-AE that are within the scope of this International Standard;

c) other relevant requirements necessary for the complete application of a PESSR-AE in a 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 PESSR-AE. These requirements are to be carried out in accordance with the national escalator and moving walk norm that references this International Standard.

d) foreseeable misuse involving security threats related to malevolent or unauthorized action. In cases where a security threat analysis needs to be considered this standard may be used, provided the specified SIL has been reassessed.

3 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. 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 61508-2:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems*

IEC 61508-3:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 3: Software requirements*

IEC 61508-4:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 4: Definitions and abbreviations*

IEC 61508-5:2010, *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*

4 Terms and definitions

For the purposes of this document, the terms and definitions given in IEC 61508-4 apply, except that the definitions in this International Standard take precedence over those in the generic standard.

4.1
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.

4.2
programmable electronic
PE
based on computer technology which may be comprised of hardware, software, and of input and/or output units

NOTE This term covers microelectronic devices based on one or more central processing units (CPUs) together with associated memories, etc.

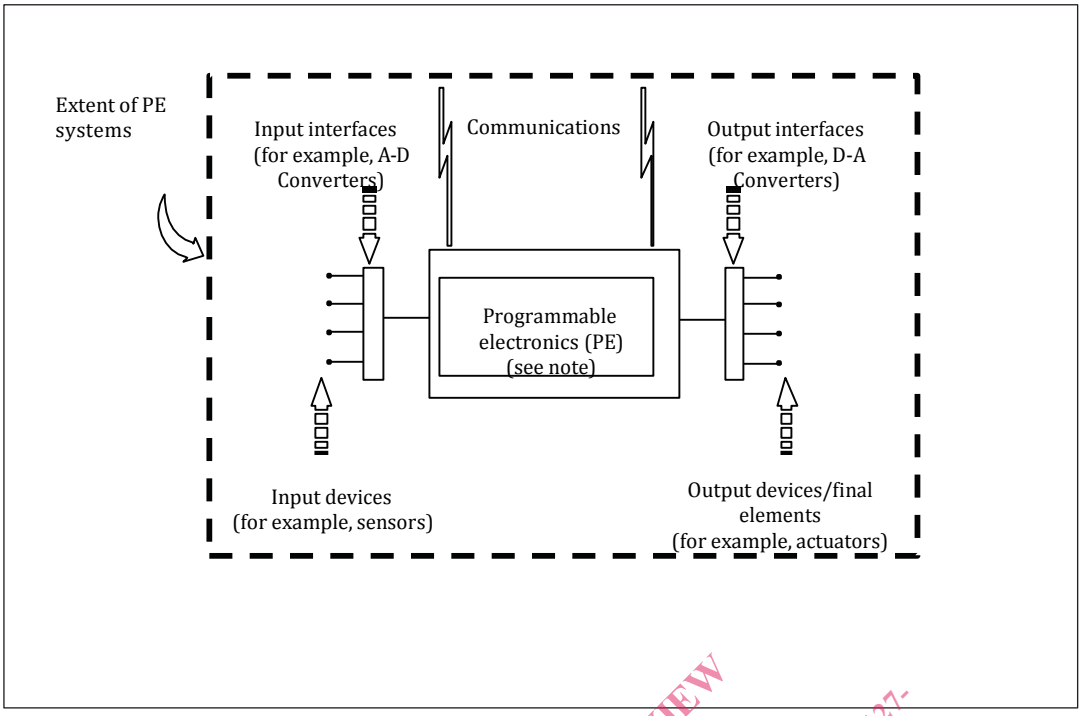
EXAMPLE The following are all programmable electronic devices:

- 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).

4.3
programmable electronic system
PE systems
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 The programmable electronics are shown centrally located but could exist at several places in the PE systems.

Figure 1 — Basic PE systems structure

4.4
Programmable Electronic Systems in Safety-Related Applications for Escalators and moving walks PESSR-AE
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 In this standard the term “proof test” is used but it is recognised that a synonymous term is “periodical test”.
NOTE 2 The effectiveness of the proof test will be 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, an analysis may need to be performed 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 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 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.

4.6
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

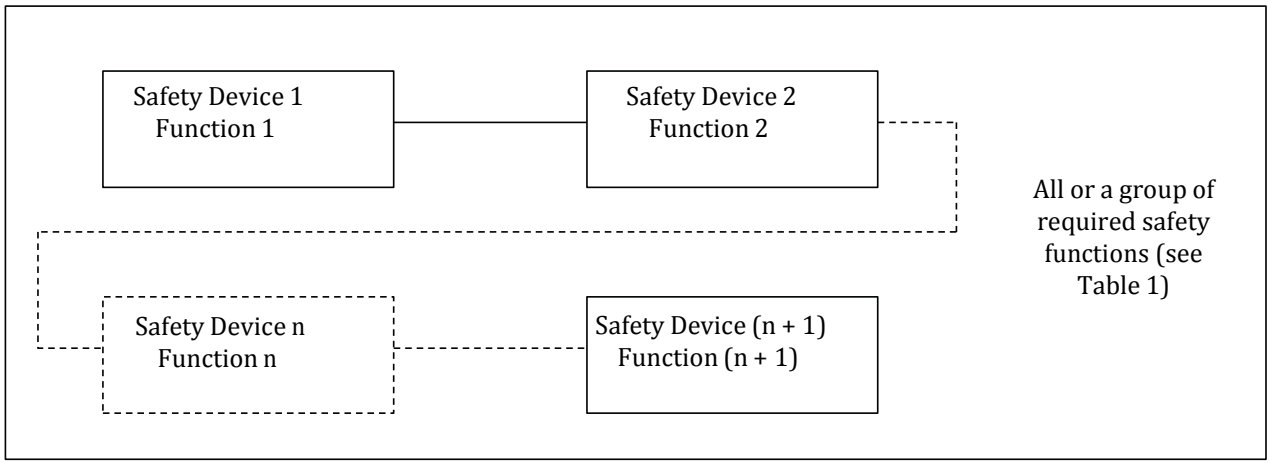


Figure 2 — Safety circuit

4.7
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 may consist of PE system elements and non-PE system elements

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

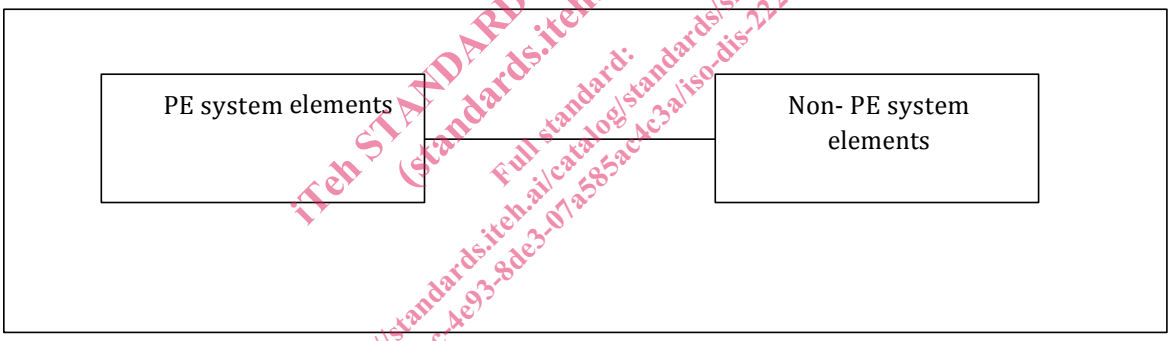


Figure 3 — Safety Device

4.8
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.

4.9
safety-related system
consists of one or more safety devices performing one or more safety functions that may 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).