TECHNICAL REPORT

ISO/TR 22201-3

Second edition
2016-11-15

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

Part 3: Life cycle guideline for programmable electronic systems related to PESSRAL and PESSRAE

Ascenseurs, escaliers mécaniques et trottoirs roulants — Conception et mise au point des systèmes électroniques programmables dans les applications liées à la sécurité —

Partie 3: Lignes directrices pour le cycle de vie des systèmes électroniques programmables liés à PESSRAL et PESSRAE

Reference number
ISO/TR 22201-3:2016(E)

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 (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 on 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 the following URL: www.iso.org/iso/foreword.html.

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

This second edition cancels and replaces the first edition (ISO/TR 22201-3:2013), which has been technically revised.

A list of all parts in the ISO 22201 series can be found on the ISO website.

Introduction

This document addresses phases in the life cycle planning and actions for post-installation activities (e.g. maintenance, repair, and replacement and modification of interface) of PESSRAL and PESSRAE to help ensure the safety integrity level (SIL) over the life cycle of the system.

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

Part 3: Life cycle guideline for programmable electronic systems related to PESSRAL and PESSRAE

1 Scope

This document provides additional information and process for the development of the instruction manual required by ISO 22201-1 (PESSRAL) and ISO 22201-2 (PESSRAE) for programmable electronic systems for use by competent maintenance person(s) that carry out maintenance operations.

2 Normative references

There are no normative references in this document.

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 22201-1, ISO 22201-2 and the following apply.

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

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

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

3.1
competent maintenance person
designated person, suitably trained, qualified by knowledge and practical experience, provided with necessary instructions and supported within their *maintenance organization* (3.4) to enable the required maintenance operations to be safely carried out

Note 1 to entry: The competence of the maintenance person within the *maintenance organization* (3.4) should be continuously updated.

3.2
design equivalent
original equipment manufacturer, or third party certified product, which fulfils same SIL rated element/subsystem design specifications but has different specifications for the non-SIL rated portion of the PE system

3.3
functional equivalent
product which fulfils same functional requirements with different SIL rated element/subsystem design specifications from that of the original certified product

3.4
maintenance organization
company or part of a company where *competent maintenance person(s)* (3.1) carry out maintenance operations on behalf of the *owner* (3.7) of the installation

3.5
manufacturer
natural or legal person who takes responsibility for the design, manufacture and placing on the market safety components for lifts or of machinery (escalator, passenger conveyor, service lift and accessible goods only lift)

3.6
maintenance
post-installation life cycle activities, including preventative, replacement, repair, and alteration (modifications)

3.7
owner
natural or legal person who has the power or disposal of the installation and takes the responsibility for its operation and use

3.8
programmable electronic
PE
based on computer technology which may be comprised 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);

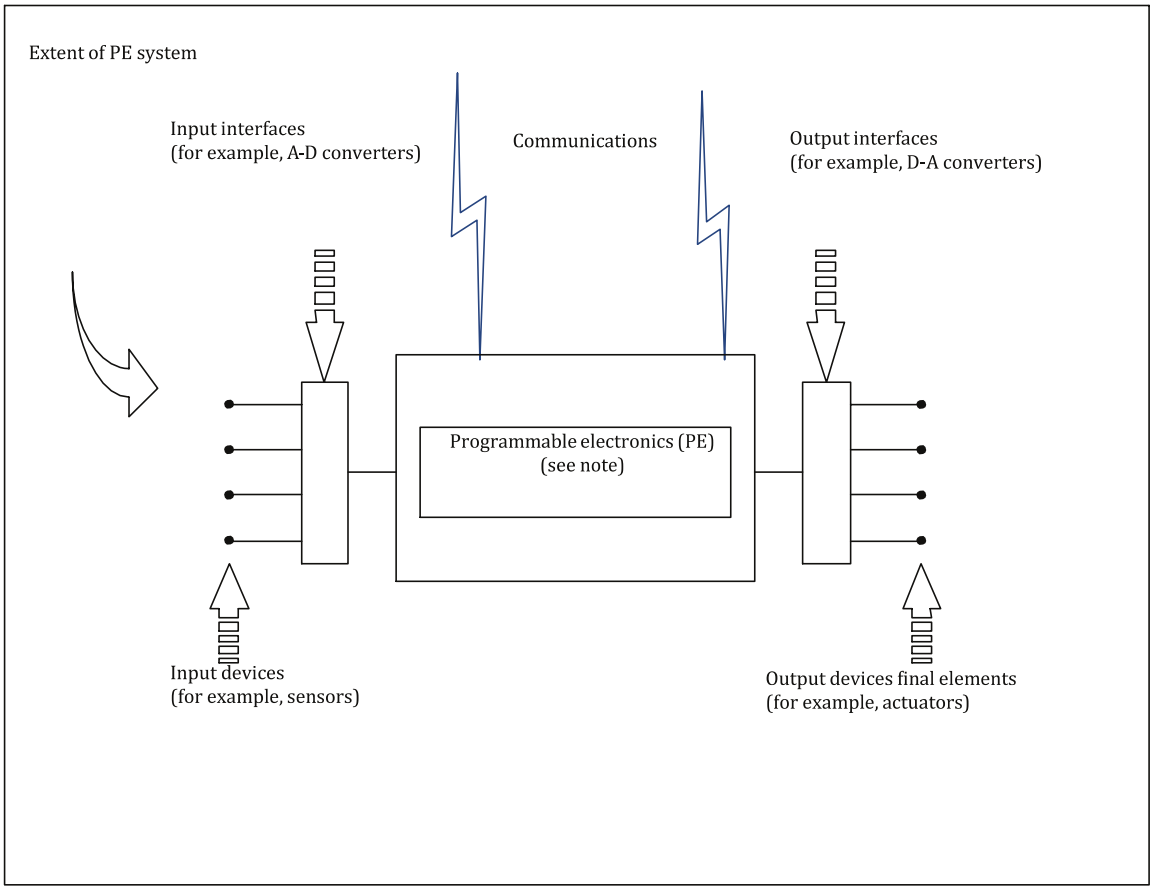
— programmable logic controllers (PLCs);

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

3.9
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 system 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 the PE system that performs the SIL relevant functional requirements.



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

Figure 1 — Basic PE system structure

3.10
product equivalent
original equipment manufacturer or third party certified product that is a direct replacement in design, make, model, and version (built to the same production drawings) of the original certified product

4 Instruction manual content

This clause addresses special considerations for process and additional content of instruction manuals applied to PE system as described in ISO 22201-1 and ISO 22201-2.

4.1 Safety precautions

In creating an instruction manual, the developer should carry out a risk assessment to identify and address possible hazards for this phase of the life cycle of PE system. (See ISO 14798 for possible hazard assessment methodology).

4.2 Markings, signs, pictograms and written warnings

Assemblies containing SIL rated devices should be labelled or tagged with identification information, in accordance with national requirements, and indicate that the maintainer should refer to the

instruction manual for detail instructions and precautions. Where possible, readily understandable signs and pictograms taken from applicable ISO standards should be used, for example, ISO 7000:2014, symbol 1640.

If the risk assessment indicates that additional specific warnings are required for the purpose of maintenance, these will be affixed directly on the installation/component or, when this is not possible, in the close vicinity. Markings, signs, pictograms and written warnings should be readily understandable and unambiguous. Signs or written warnings carrying only “DANGER” should not be used. Information affixed directly on the installation/component should be permanent and legible.

4.3 Elements to consider for content of the instruction manual

Listed below are elements to consider for contents of the instruction manual. See also A.1 for additional elements of consideration.

a) All the necessary operations to ensure the safe and intended functioning of the installation and its components after the completion of the installation and throughout its life cycle.

b) Repair or changing of components which may occur due to wear or tear and does not affect the characteristics of the installation.

c) Modernization of the installation, including the changing of any characteristic of the installation (speed, load, etc.).

d) Rescue operations carried out by fire brigades and emergency personnel.

e) The specifications and the intended use of the installation (type of installation, performance, type of goods to be transported, type of users, etc.).

f) The environment in which the installation and its components are installed (weather conditions, vandalism, etc.).

g) Any restriction of use.

h) The result of the risk assessment (see 4.1) for every working area and for every task to be undertaken.

i) The specific maintenance instructions provided by the manufacturer of the safety elements.

5 Procedure

The instructions for maintenance of PE system are provided by the manufacturer when placed on the market. They should be the result of a risk assessment and written in the official language(s) of the country for the location of the installation. When preparing the content of the maintenance instructions, the following elements should be taken into account in the manual.

a) Control documents — Control documents are identified and maintained for the life of a PE system that includes SIL rated hardware or software. These documents include:

    1) Functional requirements:

        i) design specifications (system and element/subsystem);

        ii) production specification;

iii) version identification and version control.

b) Maintenance activity and record keeping of maintenance activity — The following maintenance activities, date and explanation of reason for the activity of PE system are recorded and retained by the owner for the life of the PE system installation:

1) preventative maintenance of the safety device (scheduled safety function actuation, proof test, etc.);

2) failure event of the safety device;

3) modification in the PE system device (obsolescence, upgrade, reliability improvement, etc.);

4) modification of the interfaces to the safety device or its environment.

c) Validation of replacement or modification process — Replacements or modifications that result from the maintenance activities in (b) should be made according to the process outlined in A.2 and should not modify the minimum required SIL for the function. Where SIL relevant and non-SIL relevant functions (those indicated in ISO 22201-1 and ISO 22201-2 are in circuits driven by or communicating with SIL rated parts) are included in the design of the SIL rating of the PE system, changes made to software or hardware of the non-SIL relevant functions are treated in the same manner as a change to the SIL relevant portion of the PE system.

Annex A
(informative)

Elements of instruction manual and validation process

A.1 Additional elements for creating instruction manual

See Table A.1.

Table A.1 — Additional elements for creating instruction manual

ID	Element to consider
1	Consideration of diagnostics and failure modes identified
2	Clarity in how to perform the proof test
3	Clarity in gaining access to PE elements
4	Clarity in replacing PE elements
5	Identification of the physical elements including software
6	Identification of PE elements in documentation
7	Version and configuration management of PE system devices and related software
8	Version and configuration management of system interfaces with PE system devices
9	Precautions concerning sensitivity to changes in external environmental condition of the installation (e.g. air pressure, temperature, humidity, ESD, EMI, and grounding)
10	Frequency for maintenance action including proof test
11	Precautions related to introduction of unintended faults due to test simulation setup/parameters
12	Precautions related to unintended faults due to test conditions
13	Precautions related to unintended faults due to software tools (configuration, programming, and testing tools) or incompatibility of software tools
14	Precautions related to misleading results due to misuse of software tools (configuration, programming, and testing tools) or incompatibility of software tools

A.2 Process for validating PE system device replacement or modification

See Figure A.1.

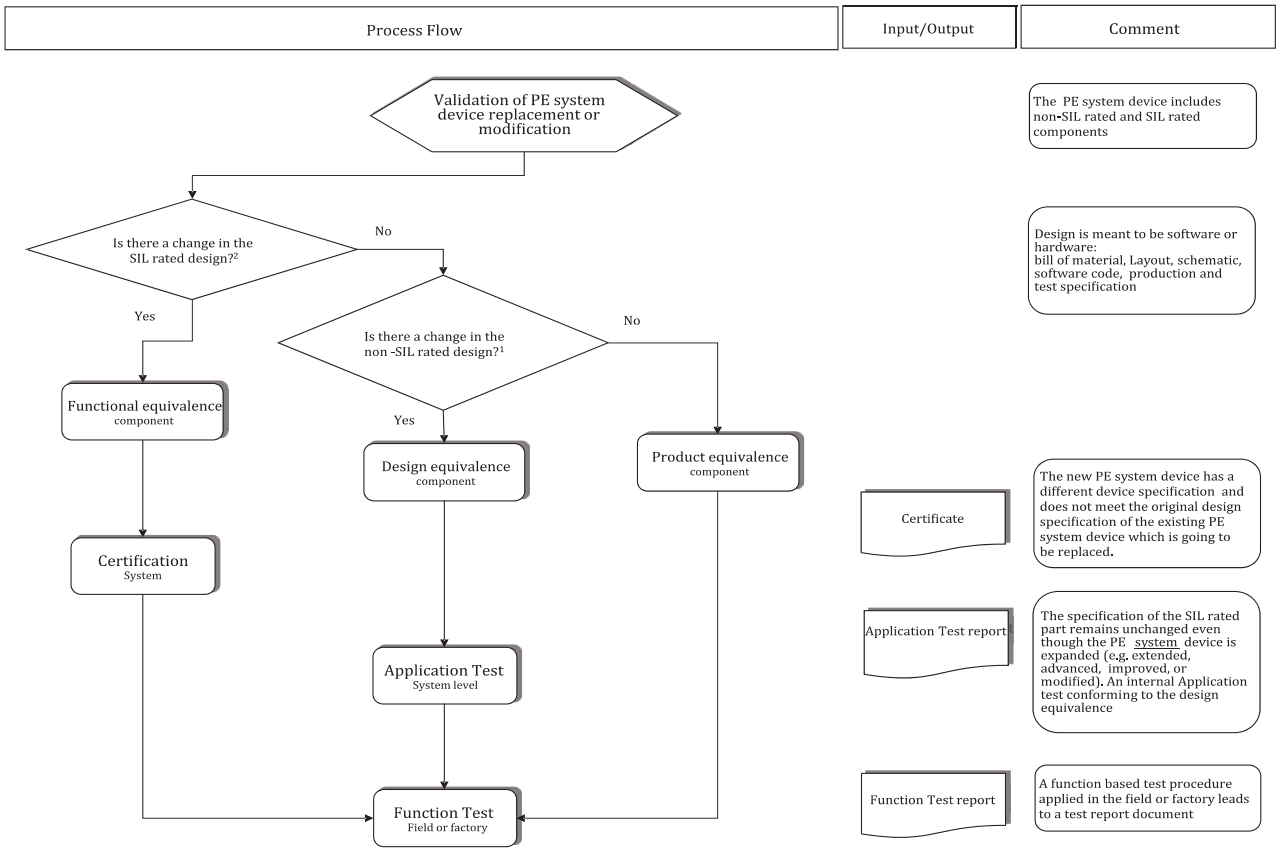


Figure A.1 — Process for validating PE system device replacement or modification

A.3 Verification/certification categories for the SIL rating of the PE system device in the applied safety function

Application test (system level): a test carried out by or witnessed by a registered or licenced professional engineer, testing laboratory, or certifying organization to ensure conformance to code requirements. These tests do not address conformity to certifications that may be required by other standards, e.g. EMC.

Certification (system): a process carried out by an independent organization which is authorized to evaluate the conformity with the appropriate standards.

Function test (field or factory): verification that field installation does not introduce a failure. These tests do not address conformity to certifications that may be required by other standards, e.g. EMC.

Bibliography

[1] ISO 3864-1, *Graphical symbols — Safety colours and safety signs — Part 1: Design principles for safety signs and safety markings*

[2] ISO 14798, *Lifts (elevators), escalators and moving walks — Risk assessment and reduction methodology*

[3] ISO 22201-1, *Lifts (elevators), escalators and moving walks — Programmable electronic systems in safety related applications — Part 1: Lifts (elevators) (PESSRAL)*

[4] ISO 22201-2, *Lifts (elevators), escalators and moving walks — Programmable electronic systems in safety related applications — Part 2: Escalators and moving walks (PESSRAE)*

ICS 91.140.90
Price based on 8 pages