INTERNATIONAL STANDARD

ISO 22201

First edition
2009-01-15

Lifts (elevators) — Design and development of programmable electronic systems in safety-related applications for lifts (PESSRAL)

Ascenseurs — Conception et mise au point des systèmes électroniques programmables dans les applications liées à la sécurité des ascenseurs (PESSRAL)

Reference number
ISO 22201:2009(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web 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.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

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.

ISO 22201 was prepared by Technical Committee ISO/TC 178, *Lifts, escalators and moving walks*.

Introduction

The Working Group ISO/TC 178, WG8 has developed this International Standard as a result of ISO/TC 178 resolution 234/2004, document N 343. Systems comprised of electrical and/or electronic components have been used for many years to perform safety functions in most application sectors. Computer-based systems, generically referred to as programmable electronic systems (PES), are being used in many application sectors to perform non-safety functions and, increasingly, to perform safety functions. In order to effectively and safely exploit computer-system technology, 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). It is necessary that any safety strategy, therefore, consider not only all the elements within an individual system (for example sensors, controlling devices and actuators) but also all the safety-related subsystems making up the total combination of safety-related systems.

This International Standard is based upon the guidelines provided in the generic IEC 61508 series of standards of the International Electro-technical Commission (IEC) and EN 81 (all parts) of the Comité Européen de Normalisation (CEN).

The requirements given in this International Standard recognize the fact that the product family covers a total range of passenger and goods/passenger lifts used in residential buildings, offices, hospitals, hotels, industrial plants, etc. This International Standard is the product family standard for lifts 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 components and programmable electronic systems (PES) that are used to perform safety functions in lifts. This International Standard has been developed in order that consistent technical and performance requirements and rational be specified for programmable electronic systems in safety-related applications for lifts (PESSRAL). Most of the specific measures in Clause A.2 have been copied from EN 81-1.

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 PESSRAL. 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 can also be applied to other technologies used to satisfy the safety functions specified in this International Standard.

Within the context of the harmonization with national standards for lifts, the application of this International Standard is intended to be by reference within a national standard lift such as lift codes, standards, or laws. The reason for this is three-fold:

a) to allow selective reference by national standards to specific lift-safety functions described in this International Standard; not all lift-safety functions identified in this International Standard are called out in every national standard;

b) to allow for future harmonization of national standards with lift-safety functions identified in this International Standard:

— Because there exist some differences in the requirements for fulfilment of the safety objectives of national lift standards and in national practice of lift use and maintenance, there are instances where the requirements for lift-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 chose to selectively harmonize with those lift-safety functions that differ in the requirements called for by the existing national standard in future standard revisions.

— It is important to note that more than 90 % of the safe-state requirements and more than 80 % of the anticipated SIL requirements by the national standards referenced in this International Standard are already harmonized with the requirements of the lift-safety functions specified in this International Standard. The remainder is not harmonized for the reasons given above.

c) to allow for the application of this International Standard where lift-safety functions are new or deviate from those specified in this International Standard. More and more, national lift legislations are moving to performance-based requirements. For this reason, the development of new or different lift-safety functions can be foreseen in product specific applications. For those who require lift-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) — Design and development of programmable electronic systems in safety-related applications for lifts (PESSRAL)

1 Scope

This International Standard is applicable to the product family of passenger and goods/passenger lifts used in residential buildings, offices, hospitals, hotels, industrial plants, etc. This International Standard covers those aspects that it is necessary to address when programmable electronic systems are used to carry out electric safety functions for lifts (PESSRAL). This International Standard is applicable for lift-safety functions that are identified in lift codes, standards or laws that reference this International Standard for PESSRAL. The SILs specified in this International Standard are understood to be valid for PESSRAL in the context of the referenced lift codes, standards and laws in Annex B.

NOTE Within this International Standard, the UK term “lift” is used throughout instead of the US term “elevator”.

This International Standard is also applicable for PESSRAL that are new or deviate from those described in this International Standard.

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 measure for the safety functions implemented by the PESSRAL;

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 PES used in lift applications that meet the minimum requirements of a recognized lift standard such as EN 81, ASME A17.1-2007/CSA B44-07, or lift 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 lifts on immunity, ISO 22200;

e) outlines the relationship between lift-safety functions and their safe-state conditions;

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

g) requires the manufacturer of the PESSRAL to provide instructions that specify what is necessary to maintain the integrity of the PESSRAL (instruction manual) for the organization carrying out the assembly, connections, adjustment and maintenance of the lift;

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

i) establishes the safety-integrity levels for specific lift-safety functions;

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

k) provides risk-reduction decision tables for the application of PESSRALs;

l) defines a maximum level of performance (SIL 3) that can be achieved for a PESSRAL according to this International Standard and defines a minimum level of performance (SIL 1).

This International Standard does not cover

— hazards arising from the PES equipment itself, such as electric shock etc.;

— the concept of fail-safe, which can be of value when the failure modes are well defined and the level of complexity is relatively low; the concept of fail-safe is considered inappropriate because of the full range of complexity of the PESSRAL that are within the scope of this International Standard;

— other relevant requirements necessary for the complete application of a PESSRAL in a lift-safety function, such as the mechanical construction, mounting and labelling of switches, actuators, or sensors that contain the PESSRAL. It is necessary that these requirements be carried out in accordance with the national lift standard that references this International Standard.

2 Conformance

To conform to this International Standard, it shall be shown that each of the requirements outlined in Clause 6 has been satisfied to the defined criteria and, therefore, the clause objective(s) has(have) been met.

3 Normative references

The following referenced documents are indispensable for the application 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 61508-1:1999, *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*

IEC 61508-7:2000, *Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 7: Overview of techniques and measures*

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

IEC 60664-1:2007, *Insulation coordination for equipment within low-voltage systems — Part 1: Principles, requirements and tests*

IEC 61249-2-1, *Materials for printed boards and other interconnecting structures — Part 2-1: Reinforced base materials, clad and unclad — Phenolic cellulose paper reinforced laminated sheets, economic grade, copper clad*

IEC 62326-1, *Printed boards — Part 1: Generic specification*

4 Terms and definitions

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

NOTE The definitions in this International Standard take precedence over those in the generic standard.

4.1
manually operated stopping device
stopping device that is intentionally, by human intervention, actuated and de-actuated (e.g. such as a toggle switch, mushroom type, hand-operated switch)

4.2
non-manually operated stopping device
stopping device that is automatically actuated or de-actuated due to human intervention or detection

4.3
non-SIL-relevant safe-state requirement
required response to the actuation of an SIL-rated safety function where the function performing this response is not required to be SIL rated

NOTE See Figure 4 and Table 2.

4.4
programmable electronic system
PES

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

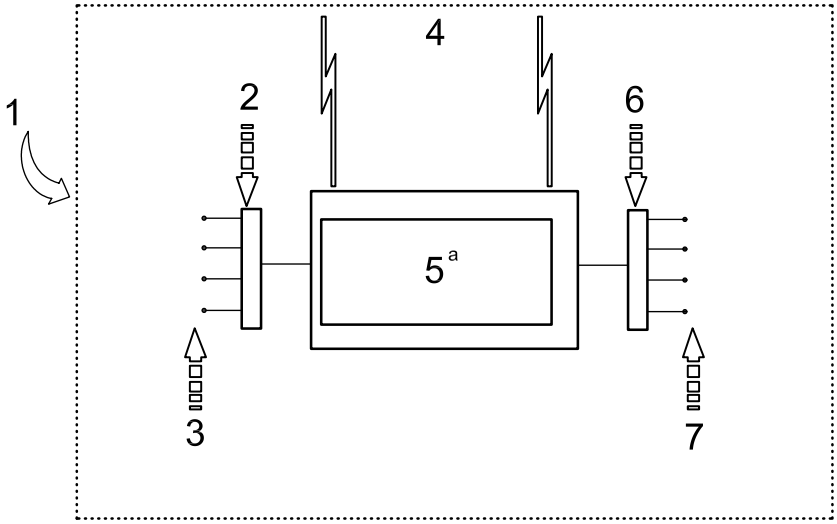
NOTE 1 See Figure 1.

NOTE 2 A PES may include elements that perform SI-rated requirements and non-SIL-rated requirements. The SIL rating is only required for those elements that perform the SI-relevant functional requirements.

4.5
programmable electronic systems in safety-related applications for lifts
PESSRAL
application of a software based PES in a safety-related system for a lift

4.6
proof test
periodic test performed to detect failures in a safety-related system

NOTE Where separate channels are used, these tests are done for each channel separately.



Key

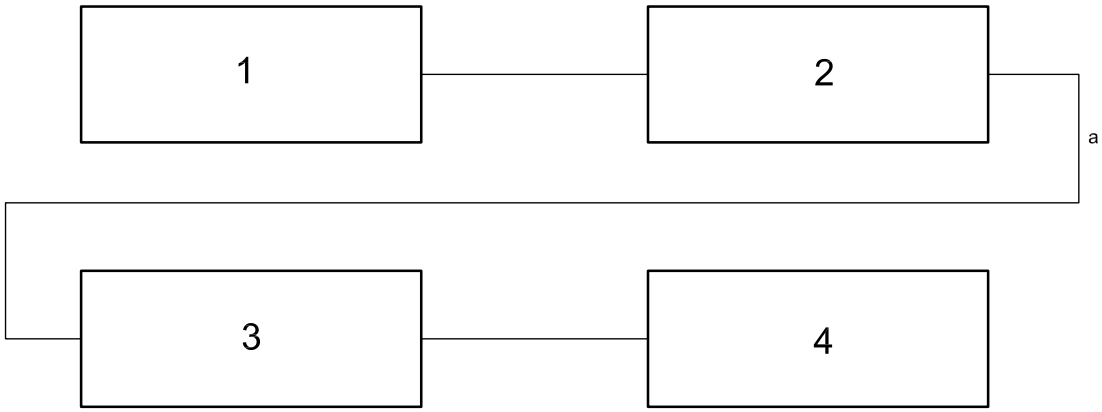
1 extent of PES
2 input interfaces (for example, D-A converters)
3 input devices (for example, sensors)
4 communications
5 programmable electronics (PEs)
6 output interfaces (for example, D-A converters)
7 output devices/final elements (for example, actuators)

[a] The programmable electronics are shown centrally located but could exist at several places in the PES.

Figure 1 — Basic PES structure

4.7
safety chain
total combination of safety devices that fulfil all or a group of lift safety functions

NOTE See Figure 2.



Key

1 safety device 1, function 1
2 safety device 2, function 2
3 safety device n, function n
4 safety device $(n + 1)$, function $(n + 1)$

[a] All or a group of required list-safety functions; see Table 1.

Figure 2 — Safety chain

4.8
safety device
part of the safety-related system, including necessary control circuits, that is designated to achieve, in its own right, a lift-safety function and that may consist of PES elements and non-PES elements

NOTE See Figure 3 and Table 1.

Key

1 PES elements
2 non-PES elements

Figure 3 — Safety device

4.9
safety function
function implemented by a safety-related system that is intended to achieve or maintain a safe state of the lift with respect to a specific hazardous event

NOTE 1 See Table 1.

NOTE 2 A safety function may include non-SIL-relevant requirements; see Table 2.

4.10
safety-related system
one or more safety devices performing one or more safety functions that may be based on programmable electronic systems (PES), electrical, electronic and/or mechanical elements of the lift

4.11
safety integrity level
SIL
discrete level (one out of a possible four) for specifying the safety-integrity requirements of the safety functions allocated to the programmable electronic safety-related system, where safety-integrity level 4 has the highest level of safety integrity and safety-integrity level 1 has the lowest

NOTE 1 The SIL is indicative of a failure rate that includes all causes of failures (both random hardware failures and systematic failures) that lead to an unsafe state, for example hardware failures, software-induced failures and failures due to electrical interference.

NOTE 2 In the context of this International Standard, SIL 3 is the highest safety integrity level that shall be applied to lifts.

4.12
SIL-relevant safe-state requirement
part of the safety-related system where it is necessary that the specified SIL of the function be met

NOTE See Figure 4 and Table 2.

Key

1 SIL-relevant safe-state requirement(s)
2 non-SIL-relevant safe-state requirement(s)

Figure 4 — Lift-safety function

4.13
system reaction time
sum of the following two values:

a) time period between the occurrence of a fault in the PESSRAL and the initiation of the corresponding action on the lift;

b) time period for the lift to respond to the action, maintaining a safe state.

5 Symbols and abbreviated terms

ETSL Emergency terminal speed limiting

ETS Emergency terminal stopping

PCB Printed circuit board

6 Requirements

6.1 General

6.1.1 Table 1 defines the safety-function names, the associated lift functional description, applicable lift type and required SIL for the SIL-relevant part of the safety function. A lift is permitted to operate without interruption when safety functions are not actuated.

NOTE Safety functions refer to those lift functions that are identified in codes, standards and laws that reference this International Standard for PESSRAL. (See Table B.1.)

6.1.2 Table 2 defines the safe-state requirements when the safety functions in Table 1 are actuated. If a safety function should actuate, the safety function shall cause the lift system to revert to the safe-state conditions specified by the requirements of Table 2.

6.1.3 PESSRAL shall consider the reaction time of the lift to respond to the safety function and internal fault detection in the time necessary 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 (see example).

EXAMPLE If an internal fault is detected by comparison of data in a two-channel system within the time necessary to meet the system's reaction time, then it is not necessary to complete a variable-memory range test within the system reaction time because the safety integrity is verified by the two-channel design.

6.2 Extended application of this International Standard

6.2.1 General

The requirements in 6.2.2 to 6.2.4 are provided to verify SILs and safe-state conditions for lift-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 codes, standards or laws referenced in Table B.1.

6.2.2 Risk assessment

Where alternatives to the requirements of 6.3 and/or 6.4 are sought, methods for the determination of the required safety-integrity level shall be performed in accordance with IEC 61508-5. The same methods shall be used to establish the rationale for a new PESSRAL function and corresponding SIL or a revised PESSRAL 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 the consequence of any single potential hazard scenario shall not exceed a frequency of 5×10^{-7}/year. See also Annex C.

6.2.3 Limits for specifying SIL for PESSRAL

Target failure measures required for specifying a PES in a lift-safety-related function shall be no less than SIL 1 and no greater than SIL 3. If a target failure measure requires a SIL higher than SIL 3, consideration should be given to redesigning the system such that the required target-failure measure is satisfied with SIL 3 or less. If an SIL lower than SIL 1 is required, a non-SIL-rated PES may be used but it shall not be classified as a PESSRAL. No PESSRAL 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 lift 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 a lift-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 the safety-integrity-level requirements for the lift-safety function. If the safety-integrity level cannot be reduced, the target failure measure for the safety function shall be distributed across multiple PESSRAL of SIL 3 or less that are sufficiently independent and certified in the application.

6.2.4 Safe-state requirements

For lift-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 that in which they are described in Table 2.

6.3 Safety function SIL requirements

Table 1 provides the required SIL for each lift safety function. For further information, see Table B.1.

6.4 SIL-relevant and non-SIL-relevant safe-state requirements

Table 2 provides the required response of the lift to the lift safety functions of Table 1 and the SIL and non-SIL relevant requirements for each response from actuation of that function. An “X” indicates the response is required for the safe-state condition when the safety function actuates or where the PESSRAL detects an internal fault condition. See corresponding notes where a numerical note reference value is used in place of an “X” for further clarification of the required response.

Table 1 — Safety function SIL requirements

Id. number	Lift-safety function	Functional description	Lift type application	SIL
1	Check final stopping limit positive drive	Detects that fewer than 1,5 turns of rope remain on the sheave or when the car has not reached top or bottom travel limit in the shaft and or that the rope is unwinding in the reverse direction	Positive drive (winding drum)	1
2	Check tension, suspension means	Detects loss of tension in the suspension means (e.g. rope or chain)	Positive drive (winding drum) hydraulic	2
3	Check for running motor generator	Detects loss of motor generator running condition	Traction	1
4	Check tension, compensation means	Detects loss of tension in the compensation means	Traction	3
5	Check compensation tie-down	Detects if the travel limits have been exceeded for the compensation tie-down means (anti-rebound)	Traction	3
6	Check motor field running current	Detects loss of DC hoist motor field running current	Traction	1
7	Check tension, final limit linkage	Detects loss of tension in the means for the linkage of transmission of car position for the final limit	Traction hydraulic	1
8	Check tension, ETSL linkage	Detects loss of tension in the means for the linkage of transmission of car position for emergency terminal speed limiting (ETSL)	Traction	2
9	Check fully retracted working platform	Detects if working platform is fully retracted	All	3
10 (a,b,c,…i) [a]	Check manually operated stopping device	Detects if a manually operated stopping device (e.g. emergency stop switch) is actuated as applicable at car-top, pit, pulley room, docking operation, passenger/goods (freight) in-car, in-car, machine remote from the motion controller disconnect, machine spaces, control spaces, machine rooms, control rooms, equipment inspection and test access panels and inspection station	All	3
10(i).1 [b]	Check non-manually operated stopping device	Detects if non-manually operated stopping device (e.g. switch) is actuated as applicable at pulley room	All	1
10(a,d,g,h).2 [b]	Check non-manually operated stopping device	Detects if non-manually operated stopping device (e.g. switch) is actuated as applicable at passenger/goods (freight) in-car, pit, machinery spaces, equipment inspection, emergency and test panels	All	2
10(e).3 [b]	Check non-manually operated stopping device	Detects if non-manually operated stopping device (e.g. switch) is actuated as applicable at inspection station	All	3
11	Check car safety gear	Detects if car safety gear has actuated	All	1
12	Check car over-speed (manual reset)	Detects car speed exceeding maximum limit set prior to or up to governor tripping speed; requires manual reset	All	2
13	Check reset of governor (manual type)	Detects if the governor is not in the reset position	All	3

Table 1 (*continued*)

Id. number	Lift-safety function	Functional description	Lift type application	SIL
14	Check tension in governor rope (or equivalent)	Detects loss of tension in the governor rope or car safety rope	All	3
15	Check car over-speed (automatic reset permitted)	Detects car speed exceeding the maximum limit set prior to or up to governor tripping speed; may be automatically reset	All	2
16	Check final limit (automatic or inspection)	Detects if car exceeds the final limit	All	1
17	Check for emergency terminal speed limit (ETSL)	Detects insufficient speed reduction in terminal zone where reduced stroke buffers are applied	Traction	2
18	Check tension in two suspension means	Detects loss of tension in a rope or chain in case of two ropes or a two-chain-type suspension	All	1
19	Check manual evacuation means	Detects that the manual means (e.g. wheel) for emergency evacuation is engaged with the machine	Traction winding drum	1
20	Check the fully retracted position of the mechanical device	Detects the fully retracted (inactive) position of the mechanical device	All	3
21	Check proper inactive position of pit protection mechanical device	Detects proper full disengagement of inactive position of the mechanical device that provides clearance protection in pit	All	3
22	Check proper full engagement of the pit protection mechanical device	Detects proper full engagement of the mechanical device that provides clearance protection in pit	All	3
23	Check movable stops not fully retracted	Detects movable stops not fully retracted	All	3
24	Check movable stops not fully extended	Detects movable stops not fully extended	All	3
25	Check doors providing access to equipment inside hoistway	Detects open access doors providing access to equipment inside the hoistway	All	2
26	Check doors providing access from working area outside hoistway	Detects open access doors, access from working area outside hoistway	All	2
27	Check circuit-breaker release device	Detects activation of the device to release the circuit breaker contactor (replacement of main switch)	All	2
28	Check leveling and re-leveling	Detects if car position is outside the leveling zone, with open doors, during leveling, re-leveling, or electrical anti-creeping	All	2
29	Check tension, leveling zone position rope or equivalent	Detects loss of tension in the means for the linkage of transmission of car position for leveling zone	All	2
30	Check travel limit for docking operation	Detects if the car exceeds the position limits for docking operation	All	2
31	Check docking operation	Detects if docking operation is enabled	All	2