
**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)*



PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

STANDARDSISO.COM : Click to view the full PDF of ISO 22201:2009



COPYRIGHT PROTECTED DOCUMENT

© ISO 2009

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester.

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.....	iv
Introduction	v
1 Scope	1
2 Conformance	2
3 Normative references	2
4 Terms and definitions.....	3
5 Symbols and abbreviated terms	6
6 Requirements	6
6.1 General.....	6
6.2 Extended application of this International Standard	6
6.3 Safety function SIL requirements	7
6.4 SIL-relevant and non-SIL-relevant safe-state requirements.....	7
6.5 Implementation and demonstration requirements for verification of SIL compliance.....	15
Annex A (normative) Techniques and measures to implement, verify and maintain SIL compliance	17
Annex B (informative) Applicable lift codes, standards and laws	33
Annex C (informative) Example of a risk-reduction decision table.....	43
Bibliography	44

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*.

STANDARDSISO.COM : Click to view the full PDF of ISO 22201:2009

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.

STANDARDSISO.COM : Click to view the full PDF of ISO 22201:2009

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

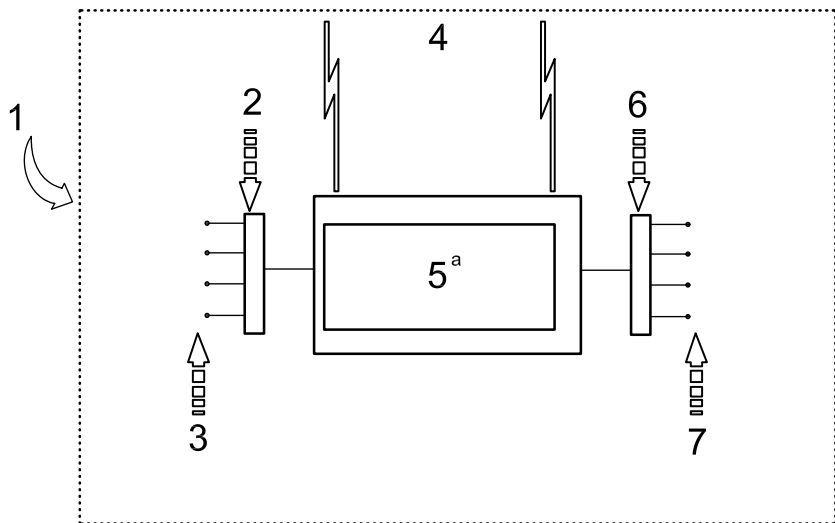
application of a software based PES in a safety-related system for a lift

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)

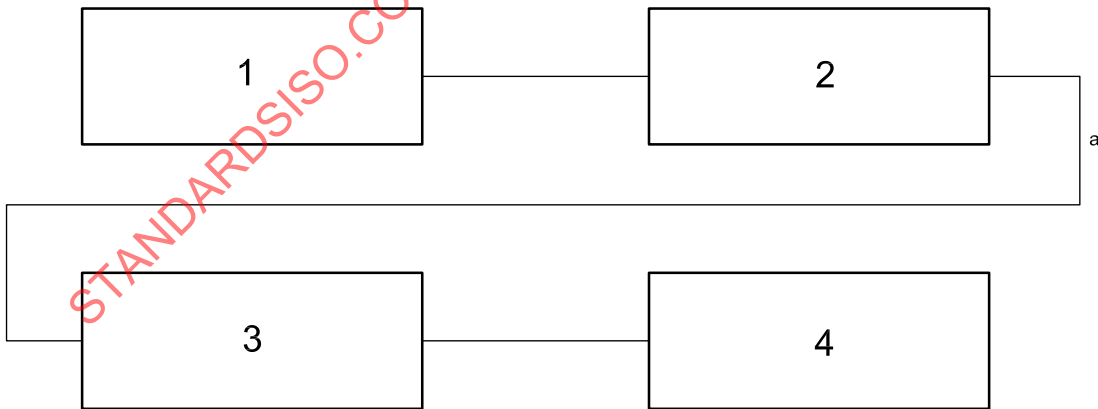
^a The programmable electronics are shown centrally located but could exist at several places in the PES.

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

Table 1 (continued)

Id. number	Lift-safety function	Functional description	Lift type application	SIL
32	Check car/landing door bypass operation	Detects if bypass operation is activated for landing and car door device(s)	All	3
33	Check top of car inspection operation	Detects if top of car inspection operation is enabled	All	3
34	Check in-car inspection operation	Detects if in-car inspection operation is enabled	All	3
35	Check clamping device	Detects engaged clamping device	Hydraulic	1
36	Check emergency electrical operation	Detects if emergency electrical operation (such as machine room, machine space, control room, control space, inspection and test panel, working platform and pit operation) is enabled	All	3
37	Check equipment in-car access panel	Detects if equipment in-car access panel is not closed	All	2
38	Check ascending car over speed	Detects if maximum speed for an ascending car is exceeded	All	2
39	Check uncontrolled car movement	Detects uncontrolled movement of the car	All	2
40	Check pawl device	Detects if the position of the pawl device is not retracted	Hydraulic	1
41	Check buffer position of pawl device	Detects if the buffer is not in normal extended position where the pawl is used	Hydraulic	3
42	Check normal extended position of buffer	Detects if the buffer is not in the normal extended position	All	3
43	Check extended position of buffer mounted to safety device	Detects if the buffer mounted to safety device is not in normal extended position	All	1
44	Check unlocked car door(s)	Detects unlocked car door(s)	All	2
45	Check hoistway access operation	Detects if the hoistway access operation is enabled	All	3
46	Check hoistway inspection and emergency doors and traps	Detects if inspection or emergency hoistway doors or traps are not closed	All	2
47	Check pit door	Detects if pit access door is not closed	All	2
48	Check landing doors and panels	Detects unlocked position of landing doors and panels	All	3
49	Check car and landing doors and car and landing door panels	Detects if car or landing doors, or car or landing door panels are not closed	All	3
50	Check locked in-car inspection and emergency doors and traps	Detects if inspection or emergency doors or traps are unlocked in car or hoistway	All	2
51	Check emergency terminal stopping (ETS)	Detects if car is not decelerating when approaching the terminal landings	All	1

^a The letter designation on 10.x refers to stop switch location.

^b The “.1”, “.2”, “.3” designation on 10 is consistent with the function SIL.

Table 2 — Safe-state requirements

NOTE The definitions of the "Rx" are given at the end of the table.		Removal of power from machine motor and brake (traction lifts), respectively, from motor and/or involved valve(s) (hydraulic lifts)	Block (prevent) automatic operation of lift (R22)	Limit the travel range	Interrupt supply circuit to the coil of the circuit breaker contactor	Transfer to inspection operation	Limit the speed of the car	Limit car movement to a direction	Manual reset required	Ignore "check car door is closed and / or locked"	Ignore "check landing door is closed and / or locked"	Block (prevent) automatic operation of the doors	Block (prevent) docking operation	Block (prevent) emergency electrical operation	Block (prevent) anti-creep (hydraulic only)	Block (prevent) in-car inspection operation	Block (prevent) hoistway access operation	Velocity profile stop and / or profile start permitted	Activate signaling
Id N°	Lift safety functions	SIL relevant				Non-SIL-relevant													
1	Check final stopping limit positive drive	X	—	—	—	—	—	—	X	—	—	—	—	—	—	—	—	—	—
2	Check tension, suspension means	X	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
3	Check for running motor generator	X	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
4	Check tension, compensation means	X	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
5	Check compensation tie-down	X	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
6	Check motor field running current	X	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
7	Check tension, final limit linkage	X	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
8	Check tension, ETSL linkage	X	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
9	Check fully retracted working platform	R26	—	X	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
10	Check manual (and non-manual) stop, stopping device	X	—	—	—	—	—	—	—	—	—	X	—	—	—	—	—	—	—
11	Check car safety gear	X	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
12	Check car over-speed (manual reset)	X	—	—	—	—	—	—	X	—	—	—	—	—	—	—	—	—	—
13	Check reset of governor (manual type)	X	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
14	Check tension in governor rope (or equivalent)	X	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—

Table 2 (continued)

NOTE The definitions of the "Rx" are given at the end of the table.		Removal of power from machine motor and brake (traction lifts), respectively, from motor and/or involved valve(s) (hydraulic lifts) Block (prevent) automatic operation of lift (R22) Limit the travel range Interrupt supply circuit to the coil of the circuit breaker contactor Transfer to inspection operation Limit the speed of the car Limit car movement to a direction Manual reset required Ignore "check car door is closed and / or locked" Ignore "check landing door is closed and / or locked" Block (prevent) automatic operation of the doors Block (prevent) docking operation Block (prevent) emergency electrical operation Block (prevent) anti-creep (hydraulic only) Block (prevent) in-car inspection operation Block (prevent) hoistway access operation Velocity profile stop and / or profile start permitted Activate signaling															
		SIL relevant				Non-SIL-relevant											
Id N°	Lift safety functions																
15	Check car over-speed (automatic reset permitted)	X	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
16	Check final limit (automatic or inspection)	X	—	—	—	—	—	—	R24	—	—	—	—	—	—	—	—
17	Check for emergency terminal speed limit (ETSL)	X	—	—	—	—	—	—	—	—	—	—	—	—	—	X	—
18	Check tension in two-suspension means	X	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
19	Check manual evacuation means	X	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
20	Check the fully retracted position of the mechanical device	X	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
21	Check proper inactive position of pit protection mechanical device	R27	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
22	Check proper full engagement of the pit protection mechanical device	R29	—	X	—	—	—	R5	—	—	—	—	—	—	—	—	—
23	Check movable stops not fully retracted	R28	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
24	Check movable stops not fully extended	R29	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
25	Check doors providing access to equipment inside hoistway	X	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
26	Check doors providing access from working area outside hoistway	X	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—

Table 2 (continued)

NOTE The definitions of the "Rx" are given at the end of the table.		Removal of power from machine motor and brake (traction lifts), respectively, from motor and/or involved valve(s) (hydraulic lifts)	Block (prevent) automatic operation of lift (R22)	Limit the travel range	Interrupt supply circuit to the coil of the circuit breaker contactor	Transfer to inspection operation	Limit the speed of the car	Limit car movement to a direction	Manual reset required	Ignore "check car door is closed and / or locked"	Ignore "check landing door is closed and / or locked"	Block (prevent) automatic operation of the doors	Block (prevent) docking operation	Block (prevent) emergency electrical operation	Block (prevent) anti-creep (hydraulic only)	Block (prevent) in-car inspection operation	Block (prevent) hoistway access operation	Velocity profile stop and / or profile start permitted	Activate signaling
Id N°	Lift safety functions	SIL relevant				Non-SIL-relevant													
27	Check circuit-breaker release device		—	—	X	—	—	—	—	—	—	—	—	—	—	—	—	—	—
28	Check leveling and re-leveling	X	—	R4	—	—	R2	—	—	R3	R3	—	—	—	—	—	—	—	—
29	Check tension, leveling zone position rope or equivalent	X	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
30	Check travel limit for docking operation	X	—	R7	—	—	—	—	—	R3	R3	—	—	—	—	—	—	—	—
31	Check docking operation	—	X	—	—	—	R6	R8	—	—	—	—	—	—	—	—	—	—	—
32	Check car/landing door bypass operation	—	X	—	—	—	R10	—	R9	R11	R12	X	X	—	—	—	—	—	R31
33	Check top of car inspection operation	—	X	R13, R20	—	X	R5	R14	—	—	—	X	X	X	X	X	X	X	—
34	Check in-car inspection operation	—	X	R13	—	X	R5	R14	—	—	—	X	X	X	X	—	X	X	—
35	Check clamping device	R15	—	—	—	—	—	R16	—	—	—	—	—	—	—	—	—	—	—
36	Check emergency electrical operation	R17	X	—	—	X	R5	—	—	—	—	—	X	R21	X	—	—	X	—
37	Check equipment in-car access panel	X	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
38	Check ascending car over-speed	X	—	—	—	—	—	—	X	—	—	—	—	—	—	—	—	—	—
39	Check uncontrolled car movement	X	—	—	—	—	—	—	X	—	—	—	—	—	—	—	—	—	—
40	Check pawl device	R15	—	—	—	—	—	R16	—	—	—	—	—	—	—	—	—	—	—
41	Check buffer position of pawl device	R15	—	—	—	—	—	R16	—	—	—	—	—	—	—	—	—	—	—
42	Check normal extended position of buffer	R25	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—

Table 2 (continued)

NOTE The definitions of the "Rx" are given at the end of the table.		Removal of power from machine motor and brake (traction lifts), respectively, from motor and/or involved valve(s) (hydraulic lifts)	Block (prevent) automatic operation of lift (R22)	Limit the travel range	Interrupt supply circuit to the coil of the circuit breaker contactor	Transfer to inspection operation	Limit the speed of the car	Limit car movement to a direction	Manual reset required	Ignore "check car door is closed and / or locked"	Ignore "check landing door is closed and / or locked"	Block (prevent) automatic operation of the doors	Block (prevent) docking operation	Block (prevent) emergency electrical operation	Block (prevent) anti-creep (hydraulic only)	Block (prevent) in-car inspection operation	Block (prevent) hoistway access operation	Velocity profile stop and / or profile start permitted	Activate signaling
Id N°	Lift safety functions	SIL relevant				Non-SIL-relevant													
43	Check extended position of buffer mounted to safety device	X	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
44	Check unlocked car door(s)	X	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
45	Check hoistway access operation	—	X	X	—	—	X	R19	—	R18	R18	X	—	X	X	—	—	—	—
46	Check hoistway inspection and emergency doors and traps	X	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
47	Check pit door	R30	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
48	Check landing doors and panels	R23	—	—	—	—	X	—	—	—	—	—	—	—	—	—	—	—	—
49	Check car and landing doors and car and landing door panels	R23	—	—	—	—	X	—	—	—	—	—	—	—	—	—	—	—	—
50	Check locked in-car inspection and emergency doors and traps	X	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
51	Check emergency terminal stopping (ETSD)	X	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
R1	If, after release of the safety gear, the over-speed governor does not automatically reset itself, an electric safety device shall prevent the starting of the lift while the over-speed governor is not in the reset position.																		
R2	The car speed is limited to 0,8 m/sec maximum levelling and 0,3 m/sec maximum re-levelling.																		
R3	Ignore this check in the unlocking zone of the target landing.																		
R4	The car travel is limited only to within the unlocking zone (as defined by the national standard).																		
R5	Car speed shall not exceed 0,75 m/s.																		
R6	Car speed is limited to inspection speed.																		
R7	Movement of the car shall be possible only in a zone not exceeding 1,7 m above the corresponding landing level.																		
R8	Movement of the car is only by the use of a constant-pressure direction-dependent button.																		
R9	Activation and reset is only by manual use of a tool.																		

Table 2 (continued)

R10	Car speed shall not to exceed 0,75 m/sec except in a fire-fighting operation.
R11	Ignore this check with car door by-pass actuated.
R12	Ignore this check with landing door by-pass actuated.
R13	Limit car travel to within final terminal limits. For hydraulic, travel in the direction beyond the lower final limit is permitted.
R14	Limit car movement to the direction away from the end of a terminal where the final limit has been reached.
R15	Check only during downward movement.
R16	Limit car movement to up direction.
R17	When enabled, it shall be permitted to render ineffective, independently or as a group, a) the means to check on the actuation of the car safety gear; (Id. no. 11); b) the means to check on over speed; (Id. nos. 12, 15); c) the means to check on ascending car over speed; (Id. no. 38); d) the means to check uncontrolled car movement (Id. no. 39); e) the means to check on the extension of the buffer (Id. no. 31); f) the means to check on the final limit (Id. nos. 1, 16, 30).
R18	Ignore this check at the access landing only.
R19	Limit car movement to opposite direction of the access limit.
R20	It shall be permitted to render ineffective the means to check the top terminal final limit and the means to check the extension of the counter-weight buffer.
R21	Only one emergency electrical operation shall be permitted. Any enabled inspection operation shall have priority over emergency electrical operation, e.g. on the platform, in the car, in the pit, etc.
R22	Any type of automatic operation, including single, selective, group, emergency fire service, hospital emergency, emergency power operation, etc.
R23	Ignoring this check is permitted during preliminary preparation.
R24	Manual reset is required only for hydraulic lifts.
R25	Ignore this check when machine room inspection operation is enabled.
R26	Ignore this check when platform and moveable stops are in fully extended position.
R27	Ignore this check only when the mechanical safety device is fully engaged and inspection operation in the pit is enabled.
R28	Ignore this check only when moveable stops are fully extended.
R29	Ignore this check only when the device is in the fully retracted and disengaged position.
R30	Ignore this check only when inspection operation in the pit is enabled and the pit-protection mechanical device is fully extended (Id. no. 22).
R31	Activate on the car audible and visible signals.

6.5 Implementation and demonstration requirements for verification of SIL compliance

6.5.1 General

The safety-integrity level of a PESSRAL shall be verified in conformance with the requirements of 6.5.

6.5.2 Required techniques and measures to implement and demonstrate PES compliance with specified safety integrity levels

6.5.2.1 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.

6.5.2.2 Where two or more lift-safety functions are implemented with common circuits in a safety chain, the SIL of these common circuits shall be at least as high as the highest SIL rating of the lift-safety functions included in those circuits. (See definition of safety chain.)

6.5.3 Loss of power after a PESSRAL device has actuated

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

6.5.3.2 Where a manual reset is required (see Table 2), the PESSRAL output shall revert to its output state just prior to the power loss.

STANDARDSISO.COM : Click to view the full PDF of ISO 22201:2009

Annex A

(normative)

Techniques and measures to implement, verify and maintain SIL compliance

A.1 General

This Annex addresses the requirements for the implementation, verification and maintenance of PESSRAL SIL compliance.

A.1.1 Techniques and measures to satisfy the SIL requirements

Techniques and measures necessary to implement and demonstrate PESSRAL SIL compliance shall be satisfied by either of the following:

- a) specific application of techniques and measures provided in Clause A.2;
- b) application of techniques and measures provided in Clause A.3 using IEC 61508-2 and IEC 61508-3.

A.1.2 Instruction manual

The manufacturer shall provide an Instruction manual.

Where the functional verification of the PESSRAL is not possible during normal operation of the lift, information shall be provided in the instruction manual to enable carrying out functional verification. The instruction manual shall also provide information about the following activities, 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.1.2.1 General requirements for the instruction manual on maintenance and repair

The instruction manual required from the manufacturer shall provide the following concerning the maintenance and repair of a PESSRAL:

- unique requirements and/or precautions for training maintenance personnel to sustain full functional performance of the PESSRAL to its SIL;
- proof-test, preventive and breakdown maintenance activities;
- unique measures and techniques used for maintenance;
- verification and documentation requirements for adherence to maintenance activities;

- timing intervals of maintenance activities;
- ensuring that test equipment used during normal maintenance activities is properly calibrated and maintained;
- necessary maintenance and repair activities when faults or failures occur in the PESSRAL, 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 PESSRAL shall allow for testing either end-to-end or in parts.

NOTE The term “end-to-end” means from sensor end to safe-state actuation.

Where the expected interval between scheduled testing is greater than the proof-test interval used to determine the SIL rating of the PESSRAL, then appropriate provisions for testing are required. When automatic proof testing is required, provisions for testing shall be an integral part of the SIL rated design to test for undetected failures.

A.1.4 EMC immunity

A PESSRAL shall fulfill the “safety circuit” test levels specified in ISO 22200 for the SIL-relevant safe-state requirements. Non-SIL-relevant safe-state requirements shall fulfill the “general-function circuits” and “all circuits” test levels in accordance with ISO 22200.

A.2 Specific techniques and measures to implement and demonstrate SIL compliance

A.2.1 General

For programmable electronic systems designed in accordance with this annex, no further assessment for the consequence of a combination of two or more faults is necessary.

The minimum requirements of the safety functions common to all SILs are listed in Tables A.1 to A.3. In addition, specific measures required for SILs 1, 2 and 3 are listed, respectively, in Tables A.4, A.5 and A.6.

NOTE The IEC 61508-7:2000 clauses listed in Tables A.1 to A.6 refer to the relevant requirements in IEC 61508-2 and IEC 61508-3.

To avoid unsafe modification, measures to prevent access to the program code and safety-related data of PESSRAL shall be provided, e.g. using EPROM, access code, etc.

A.2.2 Hardware requirements

A.2.2.1 Printed circuit board (PCB)

The short circuit can be excluded provided that

- the general specifications of PCB are in accordance with IEC 62326-1;
- the base material is in accordance with the specifications of IEC 61249-2-1;

- the PCB is constructed according to the above requirements and the minimum values are according to the tables (adapted from IEC 60664-1) with the following conditions:
 - the pollution degree is 3,
 - the material group is III,
 - the field is inhomogeneous.

The column “printed wiring material” of Table A.2.4 of IEC 60664-1:2007 is not used. This means that the creepage distance is 4 mm and the clearance is 3 mm for 250 V_{rms}. For other voltages, refer to IEC 60664-1.

If the protection of the PCB is IP 5X or better, or the material involved is of higher quality, the creepage distances can be reduced to the clearance value, e.g. 3 mm for 250 V_{rms}. For multi-layer boards comprised of at least 3 prepreg or other thin sheet insulating materials, the short circuit can be excluded [see IEC 60950 (all parts)].

A.2.2.2 Shared hardware

If a PESSRAL and a non-safety-related system share the same PCB, the following shall apply for the separation of the two systems.

- If the degree of protection is equal to or less than IP4X, the clearances shall be at least 3 mm and the creepage distances at least 4 mm.
- If the protection is better than IP4X, the creepage distance can be reduced to 3 mm.

If a PESSRAL and a non-safety-related system share the same hardware, the requirements for PESSRAL shall be met.

A.2.2.3 Common measures for avoiding and detecting failures related to hardware design are given in Table A.1.

A.2.3 Software requirements

A.2.3.1 Common measures for avoiding and detecting failures related to software design are given in Table A.2.

A.2.4 Design process requirements

A.2.4.1 Common measures related to the design and implementation process are given in Table A.3.

A.2.5 Specific measures related to SIL category

A.2.5.1 Specific measures for SIL 1 are given in Table A.4.

A.2.5.2 Specific measures for SIL 2 are given in Table A.5.

A.2.5.3 Specific measures for SIL 3 are given in Table A.6.

A.2.6 Tests procedures for verification of conformity

A.2.6.1 General provisions

For the purposes of this International Standard, it is assumed that the laboratory undertakes both the testing and the certification as an approved body. An approved body shall be either

- a) a manufacturer operating an approved, full quality assurance system, or
- b) a certified third party accredited by a national authority for the scope of lifts and corresponding safety devices.

The application for type examination shall be made by the manufacturer of the component or his authorized representative and shall be addressed to an approved test laboratory.

NOTE At the request of the laboratory, the necessary documents can be required in triplicate. The laboratory can, likewise, call for supplementary information necessary for the examination and tests.

The dispatch of samples for examination shall be made by agreement between the laboratory and the applicant. The applicant may attend the tests.

The precision of the instruments shall allow, unless particularly specified, measurements to be made within the following tolerances:

- a) masses, forces, distances, speeds: $\pm 1 \%$;
- b) accelerations, retardations: $\pm 2 \%$;
- c) voltages, currents: $\pm 5 \%$;
- d) temperature: $\pm 5 \text{ }^{\circ}\text{C}$;
- e) recording equipment: detection of signals that vary on the order of 0,01 s.

A.2.6.2 Provisions for printed circuit boards or equivalent assemblies

The applicant shall indicate to the laboratory

- a) the identification of the board/assembly,
- b) working conditions,
- c) listing of components used,
- d) layout of the printed circuit board/assembly,
- e) layout of the hybrids and marks of the tracks used in safety circuits,
- f) function description,
- g) electrical data, inclusive wiring diagram, if applicable, with input and output definitions of the board/assembly,
- h) documents and descriptions relating to the measures listed in Table A.3,
- i) general description of the software used (e.g. programming rules, language, compiler, modules),
- j) function description, including software architecture and hardware/software interaction,
- k) description of blocks, modules, data, variables and interfaces,
- l) software listings.

A.2.6.3 Functional and safety tests

In addition to the verification of the measures defined in Tables A.1 to A.6, the following shall be validated:

- software design and coding: Inspect all code statements using methods such as formal design reviews, FAGAN, test cases, etc.;
- software and hardware inspection: Verify all measures of Tables A.1 and A.2 and the measures chosen, e.g. from Table A.7, by using, for example, fault-insertion testing (based on IEC 61508-2 and IEC 61508-7).

A.2.7 Description of possible measures

A description of possible measures to failure control is given in Table A.7.

A.2.8 Verification of conformity

For the purposes of this International Standard, it is assumed that the laboratory undertakes both the testing and the certification as an approved body. An approved body shall be either

- a) a manufacturer operating a full quality assurance system defined and approved by a national authority, or
- b) a certified third party accredited by a national authority for the scope of lifts and corresponding safety devices. The application for type examination shall be made by the manufacturer of the component or his authorized representative and shall be addressed to an approved test laboratory.

Table A.1 — Common measures for avoiding and detecting failures — Hardware design

No.	Object	Measure	IEC 61508-7:2000 reference
1	Processing unit	Use of watchdog	A.9
2	Component selection	Use of components only within their specifications	—
3	I/O units and interfaces including communication links	Defined safe state in the event of a power failure or reset	—
4	Power supply	Defined safe shut-off state in case of over-voltage or under-voltage	A.8.2
5	Variable memory ranges	Use of only solid-state memories	—
6	Variable memory ranges	Read/write test of variable data memory during boot procedure	—
7	Variable memory ranges	Remote access only to informative data (e.g. statistics)	—
8	Invariant memory ranges	No possibility to change the program code, either automatically by the system or remote intervention	—
9	Invariant memory ranges	Test of program-code memory and fixed-data memory during boot procedure with a method at least equivalent to sum check	A.4.2

Table A.2 — Common measures for avoiding and detecting failures — Software design

No.	Object	Measure	IEC 61508-7:2000 reference (unless otherwise indicated)
1	Structure	Program structure (i.e. modularity, data handling, interface definition) according to the state of the art (see IEC 61508-3)	B.3.4/C.2.1 C.2.9/C.2.7
2	Boot procedure	During boot procedures a safe state of the lift shall be maintained	—
3	Interrupts	Limited use of interrupts; use of nested interrupts only if all possible sequences of interrupts are predictable	C.2.6.5
4	Interrupts	No triggering of watchdog by interrupt procedure except in combination with other program sequence conditions	A.9.4
5	Power down	No power-down procedures, such as saving of data, for safety related functions	—
6	Memory management	Stack manager in the hardware and/or software with appropriate reaction procedure	C.2.6.4/ C.5.4
7	Program	Iteration loops shorter than system reaction time, e.g. by limiting the number of loops or checking execution time	—
8	Program	Array pointer offset checks, if not included in the programming language used	C.2.6.6
9	Program	Defined handling of exceptions (e.g. divisions by zero, overflow, variable range checking, etc.) that forces the system into a defined safe state	—
10	Program	No recursive programming, except in well tried standard libraries, in approved operating systems, or in high-level language compilers. For these exceptions, separate stacks for separate tasks shall be provided and controlled by a memory management unit	C.2.6.7
11	Program	Documentation of programming library interfaces and operating systems at least as complete as the user program itself	—
12	Program	Plausibility checks on data relevant to safety functions, e.g. input patterns, input ranges, internal data	C.2.5/C.3.1
13	Program	If any operational mode can be invoked for testing or validation purposes, normal operation of the lift shall not be possible until this mode has been terminated	IEC 61508-1:1999, 7.7.2.1
14	Communication system (external and internal)	Reach a safe state with due consideration to the system reaction time in a bus communication system with safety functions in case of loss of communication or a fault in a bus participant	A.7/A.9
15	Bus system	No reconfiguration of the CPU-bus system, except during the boot procedure NOTE Periodical refresh of the CPU-bus system is not considered as being a reconfiguration.	C.3.13
16	I/O handling	No reconfiguration of I/O lines, except during the boot procedures NOTE Periodical refresh of the I/O configuration registers is not considered as a reconfiguration.	C.3.13

Table A.3 — Common measures for the design and implementation process

No.	Measure	IEC 61508-7:2000 reference
1	Assessment of the functional, environmental and interface aspects of the application	A.14/B.1
2	Requirement specification, including the safety requirements	B.2.1
3	Reviews of all specifications	B.2.6
4	Design documentation as required in A.2.6.2 and in addition — function description, including system architecture and hardware/software interaction; — software documentation, including function and program flow description	C.5.9
5	Design review reports	B.3.7/B.3.8, C.5.16
6	Check of reliability using a method such as failure mode and effect analysis (FMEA)	B.6.6
7	Manufacturer's test specification, manufacturer's test reports and field test reports	B.6.1
8	Instruction documents, including limits for intended use	B.4.1
9	Repeat and update of above-mentioned measures if the product is modified	C.5.23
10	Implementation of version control of hardware and software and its compatibility	C.5.24

Table A.4 — Specific measures for SIL 1

Components and functions	Requirements ^a	Measures	Table A.7 reference	IEC 61508-7:2000 reference
Structure	The structure shall be such that any single random failure is detected and the system shall go into a safe state.	One channel structure with self-test, or two channels or more with comparison	M 1.1 M 1.3	A.3.1 A.2.5
Processing units	Failures in processing units that can lead to incorrect results, shall be detected. If such a failure can lead to a dangerous situation, the system shall go into a safe state.	Failure-correcting hardware, or self-test by software, or comparator for two-channel structure, or reciprocal comparison by software for two-channel structure	M 2.1 M 2.2 M 2.4 M 2.5	A.3.4 A.3.1 A.1.3 A.3.5
Invariant memory ranges	Incorrect information modification, i.e. all odd-bit or 2-bit failures and some 3-bit and multi-bit failures shall be detected, at the latest, before the next travel of the lift.	The following measures refer only to a one-channel structure: one-bit redundancy (parity bit), or block safety with one-word redundancy	M 3.5 M 3.1	A.5.5 A.4.3
Variable memory ranges	Global failures during addressing, writing, storing and reading as well as all odd-bit and 2-bit failures and some 3-bit failures and multi-bit failures shall be detected, at the latest, before the next travel of the lift.	The following measures refer only to a one-channel structure: word-saving with multi-bit redundancy, or check via test pattern against static or dynamic faults	M 3.2 M 4.1	A.5.6 A.5.2
I/O units and interfaces incl. communication links	Static failures and cross talk on I/O lines, as well as random and systematic failures in the data flow, shall be detected, at the latest, before the next travel of the lift.	Code safety, or test pattern	M 5.4 M 5.5	A.6.2 A.6.1
Clock	Failures in clock generation for processing units like frequency modification or break-down shall be detected, at the latest, before the next travel of the lift.	Watchdog with separate time base, or reciprocal monitoring	M 6.1 M 6.2	A.9.4
Program sequence	Wrong program sequence and inappropriate execution time of the safety-related functions shall be detected, at the latest, before the next travel of the lift.	Combination of timing and logical monitoring of program sequence	M 7.1	A.9.4

^a As a consequence of the detection of a failure, a safe state of the lift shall be maintained.

Table A.5 — Specific measures for SIL 2

Components and functions	Requirements ^a	Measures	Table A.7 reference	IEC 61508-7:2000 reference
Structure	The structure shall be such that any single random failure is detected with due consideration to the system reaction time and that the system goes into a safe state.	One channel with self-test and monitoring, or two channels or more with comparison	M 1.2 M 1.3	A.3.3 A.2.5
Processing units	Failures in processing units that can lead to incorrect results shall be detected with due consideration to the system reaction time. If such a failure can lead to a dangerous situation, the system shall go into a safe state.	Failure correcting hardware, and software self-test supported by hardware for one-channel structure, or comparator for 2-channel structure, or reciprocal comparison by software for 2-channel structure	M 2.1 M 2.3 M 2.4 M 2.5	A.3.4 A.3.3 A.1.3 A.3.5
Invariant memory ranges	Incorrect information modification, i.e. all odd-bit or 2-bit failures and some 3-bit and multi-bit failures shall be detected with due consideration to the system reaction time.	The following measures refer only to a one-channel structure: block safety with one-word redundancy, or word saving with multi-bit redundancy	M 3.1 M 3.2	A.4.3 A.5.6
Variable memory ranges	Global failures during addressing, writing, storing and reading as well as all odd-bit and 2-bit failures and some 3-bit failures and multi-bit failures shall be detected with due consideration to the system reaction time.	The following measures refer only to a one-channel structure: word-saving with multi-bit redundancy, or check via test pattern against static or dynamic faults	M 3.2 M 4.1	A.5.6 A.5.2
I/O units and interfaces incl. communication links	Static failures and cross talk on I/O lines, as well as random and systematic failures in the data flow, shall be detected with due consideration to the system reaction time. ^b	Code safety, or test pattern	M 5.4 M 5.5	A.6.2 A.6.1
Clock	Failures in clock generation for processing units like frequency modification or break down shall be detected with due consideration to the system reaction time.	Watchdog with separate time base, or reciprocal monitoring	M 6.1 M 6.2	A.9.4
Program sequence	Wrong program sequence and inappropriate execution time of the safety function shall be detected with due consideration to the system reaction time.	Combination of timing and logical monitoring of program sequence	M 7.1	A.9.4
^a As a consequence of the detection of a failure, a safe state of the lift shall be maintained. ^b This does not apply to actuators, such as safety relays or equivalent electronic means, e.g. in the safety chain.				

Table A.6 — Specific measures according to SIL 3

Components and functions	Requirements ^a	Measures	Table A.7 reference	IEC 61508-7:2000 reference
Structure	The structure shall be such that any single random failure is detected with due consideration to the system reaction time and that then the system goes into a safe state.	2 channels or more with comparison	M 1.3	A.2.5
Processing units	Failures in processing units that can lead to incorrect results shall be detected with due consideration to the system reaction time. If such a failure can lead to a dangerous situation, the system shall go into a safe state.	Comparator for two channels, or reciprocal comparison by software for 2-channel structure	M 2.4 M 2.5	A.1.3 A.3.5
Invariant memory ranges	Incorrect information modification, i.e. all 1-bit or multi-bit failures, shall be detected with due consideration to the system reaction time.	Block safety procedure with block replication, or block safety with multi-word redundancy	M 3.3 M 3.4	A.4.5 A.4.4
Variable memory ranges	Global failures during addressing, writing, storing and reading as well as static bit failures and dynamic couplings shall be detected with due consideration to the system reaction time.	Block safety procedure with block replication, or inspection checks such as "Galpat"	M 4.2 M 4.3	A.5.7 A.5.3
I/O units and interfaces incl. communication links	Static failures and cross talk on I/O lines as well as random and systematic failures in the data flow, shall be detected with due consideration to the system reaction time. ^b	Multi-channel parallel input and multi-channel parallel output, or output read back, or code safety, or test pattern	M 5.1 M 5.3 M 5.2 M 5.4 M 5.5	A.6.5 A.6.3 A.6.4 A.6.2 A.6.1
Clock	Failures in clock generation for processing units like frequency modification or break-down shall be detected with due consideration to the system reaction time.	Watchdog with separate time base, or reciprocal monitoring	M 6.1 M 6.2	A.9.4
Program sequence	Wrong program sequence and inappropriate execution time of the safety function shall be detected with due consideration to the system reaction time.	Combination of timing and logical monitoring of program sequence	M 7.1	A.9.4
^a As a consequence of the detection of a failure, a safe state of the lift shall be maintained. ^b This does not apply to actuators, such as safety relays or equivalent electronic means, e.g. in the safety chain.				

Table A.7 — Description of possible measures of failure control

Components and functions	Measure no.	Description of measures
Structure	M 1.1	One-channel structure with self-test <u>Description:</u> Even though the structure consists of a single channel, redundant output paths shall be provided to ensure a safe shutdown. Self-tests (cyclical) are applied to the sub-units of the PESSRAL at time intervals that may be application-dependent. These tests (e.g. CPU tests or memory tests) are designed to detect latent failures that are independent of the data flow. A detected failure shall cause the system to go into a safe state.
	M.1.2	One-channel structure with self-test and monitoring <u>Description:</u> A one-channel structure with self-test and monitoring consists of a separate hardware-monitoring unit which, independent of the application, periodically receives test data from the system that can result from self-test procedures. In case of incorrect data, the system shall go into a safe state. At least two independent shut-down paths are needed so that a shut-down can be caused either by the processing unit itself or by the monitoring unit.
	M.1.3	Two or more channels with comparison <u>Description:</u> Two-channel safety-related design consists of two independent and feedback-free functional units. This allows the specified functions to be processed independently in each channel. For a two-channel PESSRAL exclusively designed for the function of one safety device, the design of the channels may be identical in terms of hardware and software. In the case of a two-channel PESSRAL used for complex solutions (e.g. combinations of several safety functions) and where the processes or conditions are not definitely verifiable, diversity of hardware and software should be considered. The structure includes a function that compares internal signals (e.g. bus comparison) and/or output signals that are relevant to safety functions in order to aid failure detection. At least two independent shut-down paths are needed so that a shut-down can be caused either by the channels themselves or by the comparator. It is necessary that the comparison itself also be subject to failure recognition.

Table A.7 (continued)

Components and functions	Measure no.	Description of measures
Processing units	M 2.1	Failure-correcting hardware <u>Description:</u> Such units can be realized using special failure-recognizing or failure-correcting circuit techniques. These techniques are known for simple structures.
	M 2.2	Self-test by software <u>Description:</u> All the functions of the processing unit that are used in the safety-related application shall be tested cyclically. These tests can be combined with the test of the sub-components, e.g. memories, I/O's, etc.
	M.2.3	Software self-test supported by hardware <u>Description:</u> A special hardware facility is used for the failure detection that supports the self-test functions, for example, a monitoring unit which checks the periodic output of certain bit patterns.
	M 2.4	Comparator for two-channel structures <u>Description:</u> <pre> graph LR 1[1] --- C[Comparator] 2[2] --- C </pre> Two channels with hardware comparator: - The signals of both processing units are compared using a hardware unit cyclically or continuously. The comparator can be an externally tested unit or designed as a self-monitoring device. Or - The signals of both channels are compared using a processing unit. The comparator can be an externally tested unit or designed as a self-monitoring device.
	M.2.5	Reciprocal comparison of two channels <u>Description:</u> <pre> graph LR C1[1 Comparator] --- C2[Comparator 2] C2 --- C1 </pre> Two redundant processing units are used that exchange safety-relevant data reciprocally. A comparison of the data is carried out by each unit.

Table A.7 (continued)

Components and functions	Measure no.	Description of measures
Invariant memory ranges (ROM, EPROM...)	M 3.1	Block-safety procedure with one-word-redundancy (e.g. signature formation via ROM with single word width) <u>Description:</u> In this test, the contents of the ROM are compressed by a certain algorithm to at least one memory word. The algorithm, e.g. cyclic redundancy check (CRC), can be realized using hardware or using software.
	M 3.2	Word-saving with multi-bit-redundancy (e.g. modified hamming code) <u>Description:</u> Every word of the memory is extended by several redundant bits to produce a modified hamming code with a hamming distance of at least four. Every time a word is read, one can determine whether a corruption has taken place by checking the redundant bits. If a difference is found, it is necessary that the system go into a safe state.
	M 3.3	Block-safety procedure with block replication <u>Description:</u> The address space is equipped with two memories. The first memory is operated in the normal manner. The second memory contains the same information and is accessed in parallel to the first. The outputs are compared and a failure is assumed if a difference is detected. In order to detect certain kinds of bit errors, the data shall be stored inversely in one of the two memories and inverted once again when read. In the software procedure, the contents of both memory areas are compared cyclically using a program.
	M 3.4	Block-safety procedure with multiword redundancy <u>Description:</u> This procedure calculates a signature using a CRC algorithm, but the resulting value is at least two words in size. The extended signature is stored, recalculated and compared as in a single-word case. A failure message is produced if a difference occurs.
	M.3.5	Word-saving one bit redundancy (e.g. ROM monitoring with parity bit) <u>Description:</u> Every word of the memory is extended by one bit (the "parity" bit) that completes each word to an even or odd number of logical 1's. The parity of the data word is checked each time it is read. If the wrong number of 1's is found, a failure message is produced. The choice of even or odd parity should be made such that whichever of zero word (nothing but 0's) and the one word (nothing but 1's) is the more unfavourable in the event of failure, then that word is not a valid code. Parity can also be used to detect addressing failure when the parity is calculated for the concatenation of the data word and its address.

Table A.7 (continued)

Components and functions	Measure no.	Description of measures
Variable memory ranges	M 4.1	Check via test pattern against static or dynamic faults, e.g. RAM test “walkpath” <u>Description:</u> The memory range being tested is initialized by a uniform bit stream. The first cell is then inverted and the remaining memory area is inspected to ensure that the background is correct. After this, the first cell is re-inverted to return to its original value and the whole process is repeated for the next. A second run of the “wandering bit model” is carried out with an inverse background pre-assignment. If a difference occurs, it is necessary that the system go into a safe state.
	M.4.2	Block-safety procedures with block replication, e.g. double RAM with hardware or software comparison <u>Description:</u> The address space is equipped with two memories. The first memory is operated in the normal manner. The second memory contains the same information and is accessed in parallel to the first. The outputs are compared and a failure is assumed if a difference is detected. In order to detect certain kinds of bit errors, the data shall be stored inversely in one of the two memories and inverted once again when read. In the software procedure, the contents of both memory areas are compared cyclically using a program.
	M.4.3	Inspection to check for static and dynamic failures, e. g. “GALPAT” <u>Description:</u> a) RAM test “galpat”: An inverse element is written into the standard pre-assigned memory and then all the remaining cells are inspected to ensure that their contents are correct. After every reading access to one of the remaining cells, the inversely described cell is also inspected and read in addition to this. This process is repeated for every cell. A second run is carried out with an inverse pre-assignment. A failure is assumed if there is a difference. Or b) Transparent “galpat” test: At the beginning of the test, a “signature” is formed using software or also hardware regarding the content of the memory range being tested and this is stored in the register. This corresponds to the pre-assignment of the memory in the galpat test. The contents are now written into the test cell in an inverted way and inspect the contents of the remaining cells. The contents of the test cell are also read after every reading access to one of these cells. Since the contents of the remaining cells are indeed unknown, their contents are not inspected individually, but by forming a signature once again. After this first run for the first cell, a second run for this cell takes place with contents that have been inverted several times: i.e., contents that are real again. Thus, the original contents of the memory are re-established. All the other memory cells are tested in the same manner. A failure is assumed if there is a difference.

Table A.7 (continued)

Components and functions	Measure no.	Description of measures
I/O units and interfaces	M 5.1	Multi-channel parallel input <u>Description:</u> This is a data-flow-dependent comparison of independent inputs complying with a defined tolerance area (time value).
	M.5.2	Output read back (monitored output) <u>Description:</u> This is a data-flow-dependent comparison of outputs with independent inputs complying with a defined tolerance area (time, value). The failure cannot always be related to the defective output.
	M.5.3	Multi-channel parallel output <u>Description:</u> This is a data-flow-dependent output redundancy. Failure recognition takes place directly via the technical process or via external comparators.
	M.5.4	Code safety <u>Description:</u> This procedure protects the input and output information with regard to coincident failures and systematic failures. It provides data-flow-dependent failure recognition of the input and output units with information redundancy or/and time redundancy.
	M.5.5	Test pattern (model) <u>Description:</u> This is a data flow independent cyclical test of input and output units carried out with the aid of a defined testing pattern to compare observations with the corresponding expected values. The testing pattern information, the testing pattern reception and testing pattern evaluation have to be independent from each other. It has to be assumed that all possible input patterns are tested.
Clock	M 6.1	Watchdog with separate time base <u>Description:</u> Hardware timer with a separate time base is triggered by correct operation of the program.
	M.6.2	Reciprocal monitoring <u>Description:</u> Hardware timer with a separate time base is triggered by the correct operation of the program of the other processor.
Program sequence	M 7.1	Combination of timing and logical monitoring of program sequence <u>Description:</u> A time-based facility monitoring the program sequence is re-triggered only if the sequence of the program sections is executed correctly.

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

A.3.1 General requirements

The requirements for the application of IEC 61508 where it is used for the implementation and demonstration of PESSRAL SIL compliance are provided in Clause A.3.

A.3.1.1 For the purpose of this International Standard, the SIL represents the requirement for a device operating in the low-demand mode and the probability of failure to perform its safety function on demand (refer to IEC 61508-1:1999, Table 2). However, where a PESSRAL is used for continuous control to maintain functional safety, the SIL shall represent the requirement for a PESSRAL considered operating in the high-demand mode and the dangerous failure rate shall be used (refer to IEC 61508-1:1999, 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.3.1.2 Device(s) and software used to fulfil non-SIL-rated requirements shall not be used to implement SIL-relevant requirements of a PESSRAL unless these device(s) and software have also been included in the rating of the SIL for the safety-related function.

A.3.1.3 The detection of a dangerous fault (by diagnostic tests, proof tests or any other means) in any PESSRAL 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 PESSRAL and maintain the safe-state condition prior to a second fault in the same subsystem that can lead to a dangerous condition, a manual reset shall be required to remove the PESSRAL from the safe-state condition.

Where the above actions depend on an operator or remote subsystem 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 PESSRAL.

A.3.2 Implementation and SIL compliance

Implementation of SIL compliance for a PESSRAL 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 that they are certified for the application.

A.3.3 Verification of conformity

For the purposes of this International Standard, it is assumed that the laboratory undertakes both the testing and the certification as an approved body. An approved body shall be a certified third party accredited by a national authority for the scope of lifts and corresponding safety devices.

The application for type examination shall be made by the manufacturer of the component or his authorized representative and shall be addressed to an approved test laboratory.

Annex B

(informative)

Applicable lift codes, standards and laws

Safety functions refer to those lift functions that are identified in other standards, i.e., codes and laws that reference this International Standard for PESSRAL. For the purposes of records and cross-references, Table B.1 indicates the relationship between the following editions of lift codes, standards and laws and the safety functions set forth in Table B.1.

ASME A17.1-2007/CSA B44-07, *Safety Code for Elevators and Escalators*

EN 81-1:1998 + A1:2005 + A2:2003, *Safety rules for the construction and installation of lifts — Part 1: Electric lifts*

EN 81-2:1998 + A1:2005 + A2:2003, *Safety rules for the construction and installation of lifts — Part 2: Hydraulic lifts*

The Building Standards Law of Japan, Enforcement Order (For Elevator and Escalator): 2002

Table B.1 — Cross-reference to applicable lift codes, standards and laws

Table 1		Cross-reference					
		EN 81, Parts 1 and 2		ASME A17.1-2007/CSA B44-07		Japan building law	
Id. No.	Lift-safety function	Part/Clause	Table A1 text	Clause	Text	Law number	Japan implementation
1	Check final stopping limit positive drive	NA	NA	2.25.3.5	Additional requirements for winding drum machines, final stopping NOTE Not required where final terminal stopping that meets this requirement is provided.	1423.2.7	Winding drum machine final stopping. Limit switch shall be provided to stop winding drum when 1,5 turns of rope remains on the sheave or when the car reaches the top or bottom travel limit in the shaft and to prevent unwinding in the reverse direction.
2	Check tension, suspension means	1/12.9 2/12.13	Check for slack rope or slack chain for positive drive lifts Check for slack rope or slack chain	2.26.2.1	Slack-rope switch on winding drum machines	129.10.2 1423.2.7	Winding drum machine is a device with an automatic switch to turn off the power when the main rope is slack.
3	Check for running motor generator	NA	—	2.26.2.2	Motor-generator running switch	NA	NA
4	Check tension, compensation means	1/9.6.1e	Check on the tension in the compensation ropes	2.26.2.3	Compensating-rope sheave switch	NA	NA
5	Check compensation tie-down	1/9.6.2	Check on the anti-rebound device	2.21.4.2	Tie-down compensation means	NA	NA
6	Check motor field running current	NA	NA	2.26.2.4	Motor field sensing means	NA	NA
7	Check tension, final limit linkage	1/10.5.2.3 b) 2/10.5.2.2 b) 2/10.5.2.3 b)	Check on the tension in the device for transmission of the car position (final limit switches) Check on the tension in the device for transmission of the car position in case of direct acting lift (final limit switches) Check on the tension in the device for transmission of the car position in case of indirect acting lift (final limit switches)	2.26.2.6	Broken rope, tape, or chain switches	NA	NA

Table B.1 (continued)

Table 1		Cross-reference					Japan building law	
		EN 81, Parts 1 and 2		ASME A17.1-2007/CSA B44-07		Text		
Id. No.	Lift-safety function	Part/Clause	Table A1 text	Clause	Text		Law number	Japan implementation
8	Check tension, ETSL linkage	1/12.8.4 c)	Check on the tension in the device for transmission of the car position (slowdown checking device)	2.26.2.6	Broken rope, tape, or chain switches	NA	NA	
9	Check fully retracted working platform	6.4.5.4 a)	Check on the fully retracted position of the retractable platform	2.26.2.36	Working platform electrical device	NA	NA	
10(a)	Check manually operated stopping device	1/5.7.3.4 a) 2/5.7.2.5 a)	Stopping device in the pit Stopping device in the pit	2.26.2.7	Stop switch in pit	1413.1.4.d	If machine and/or controller are placed at the pit, pit emergency switch should be provided.	
10(a).2	Check non-manually operated stopping device	1/5.7.3.4 a) 2/5.7.2.5 a)	Stopping device in the pit Stopping device in the pit	NA	NA	NA	NA	
10(b)	Check manually operated stopping device	NA	NA	2.26.2.5	Stop switch	NA	NA	
10(c)	Check manually operated stopping device	NA	NA	2.26.2.33	Fire-fighter's stop switch	NA	NA	
10(d)	Check manually operated stopping device	14.2.2.1 f)	Stopping device at lift machine Stopping	2.26.2.24 2.26.2.33	2.26.2.24 stop switch for machinery spaces and control spaces 2.26.2.33 Fire-fighter's stop switch	NA	NA	
10(d).2	Check non-manually operated stopping device	1/14.2.2.1 f) 2/14.2.2.1 f)	Stopping device at lift machine	NA	NA	NA	NA	
10(e)	Check manually operated stopping device	14.2.1.3 c) 8.15 b)	Stopping device with inspection operation Stopping device on the car roof	2.26.1.4.2e(1) with 2.26.2.8	Stopping device with inspection operating device	129.8.2	The elevator operation devices or switches, etc., for maintenance shall be provided in order that maintenance persons can work safely.	
						1429.1.1	The equipment by which power can be cut inside a car and on a car-roof shall be provided.	