SLOVENSKI STANDARD

SIST EN 81-1:1999/A1:2006

01-marec-2006

Varnostna pravila za konstruiranje in vgradnjo dvigal (liftov) ï 1. del: Elektriļ na dvigala

Safety rules for the construction and installation of lifts - Part 1: Electric lifts

Sicherheitsregeln für die Konstruktion und den Einbau von Aufzügen - Teil 1: Elektrisch betriebene Personen- und Lastenaufzüge

Regles de sécurité pour la construction et l'installation des ascenseurs - Partie 1: Ascenseurs électriques

Ta slovenski standard je istoveten z: EN 81-1:1998/A1:2005

ICS:

91.140.90 Dvigala. Tekoļ e stopnice Lifts. Escalators

SIST EN 81-1:1999/A1:2006 **en**

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 81-1:1998/A1

November 2005

ICS 91.140.90

English Version

Safety rules for the construction and installation of lifts - Part 1: Electric lifts

Règles de sécurité pour la construction et l'installation des ascenseurs - Partie 1: Ascenseurs électriques

Sicherheitsregeln für die Konstruktion und den Einbau von Aufzügen - Teil 1: Elektrisch betriebene Personen- und Lastenaufzüge

This amendment A1 modifies the European Standard EN 81-1:1998; it was approved by CEN on 13 May 2005.

CEN members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for inclusion of this amendment into the relevant national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the Central Secretariat or to any CEN member.

This amendment exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN member into its own language and notified to the Central Secretariat has the same status as the official versions.

CEN members are the national standards bodies of Austria, Belgium, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Slovakia, Slovenia, Spain, Sweden, Switzerland and United Kingdom.

EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

Management Centre: rue de Stassart, 36 B-1050 Brussels

Ref. No. EN 81-1:1998/A1:2005: E

Contents

Foreword

This European Standard (EN 81-1:1998/A1:2005) has been prepared by Technical Committee CEN/TC 10 “Lifts, escalators and moving walks”, the secretariat of which is held by AFNOR.

This Amendment to the European Standard EN 81-1:1998 shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by May 2006, and conflicting national standards shall be withdrawn at the latest by May 2006.

This European Standard has been prepared under a mandate given to CEN by the European Commission and the European Free Trade Association, and supports essential requirements of EU Directive(s).

For relationship with EU Directive(s), see informative Annex ZA, which is an integral part of this European Standard.

The 1998 edition of EN 81-1, under 14.1.2.1.1 b) 3) and Annex H foresees the use of electronic components in safety circuits thus giving hardware provisions. This amendment extends their use to permit the inclusion of software (programmable electronic systems - PESSRAL).

This amendment A1 covers those aspects that need to be addressed when programmable electronic systems (PESSRAL) are used to carry out electric safety functions for lifts within the scope of EN 81-1:1998 and EN 81-1:1998/A2:2004.

This amendment A1 covers the necessary additional precautions by replacing the relevant existing text of EN 81-1:1998 or adding new clauses as indicated.

NOTE Drafting and presentation of the amended text has been arranged to comply with the presentation of EN 81-1:1998.

According to the CEN/CENELEC Internal Regulations, the national standards organizations of the following countries are bound to implement this European Standard: Austria, Belgium, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Slovakia, Slovenia, Spain, Sweden, Switzerland and United Kingdom.

1 Modifications in Clause 0

A new 0.2.6 shall be added as follows:

"**0.2.6** Risk analysis, terminology and technical solutions have been considered taking into account the methods of the EN 61508 series of standards. This led to a necessary classification of safety functions applied to PESSRAL."

0.3.5 shall be amended as follows:

"**0.3.5** The requirements of this European Standard regarding electrical safety devices are such that the possibility of a failure of an electric safety device (see 14.1.2.1.1 b)) complying with all the requirements of this European Standard need not to be taken into consideration."

2 Modifications in Clause 2

Clause 2 shall be amended as follows:

"EN 61508-1:2001, *Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 1: General requirements (IEC 61508-1:1998 + Corrigendum 1999).*

EN 61508-2:2001, *Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems (IEC 61508-2:2000).*

EN 61508-3:2001, *Functional safety of electrical/electronic/programmable electronic safety related systems - Part 3: Software requirements (IEC 61508-3:1998 + Corrigendum 1999).*

EN 61508-4:2001, *Functional safety of electrical/electronic/programmable electronic safety related systems - Part 4: Definitions and abbreviations (IEC 61508-4:1998 + Corrigendum 1999).*

EN 61508-5:2001, *Functional safety of electrical/electronic/programmable electronic safety related systems - Part 5: Examples of methods for the determination of safety integrity levels (IEC 61508-5:1998 + Corrigendum 1999).*

EN 61508-7:2001, *Functional safety of electrical/electronic/programmable electronic safety related systems – Part 7: Overview of techniques and measures (IEC 61508-7:2000)."*

3 Modifications in Clause 3

Clause 3 shall be amended by the following definitions:

"**programmable electronic system in safety related applications for lifts (PESSRAL)**
(système électronique programmable dans les applications liées à la sécurité des ascenseurs (PESSRAL))
(programmierbares elektronisches System in sicherheitstechnisch relevanten Anwendungen für Aufzüge (PESSRAL))

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, used in safety related applications as listed in Tables A.1 and A.2.

system reaction time
(temps de réaction système)
(Systemreaktionszeit)

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.

safety integrity level (SIL)
(niveau d'intégrité de sécurité)
(Sicherheits-Integritätslevel)

discrete level for specifying the safety integrity requirements of the safety functions to be allocated to the PESSRAL

NOTE In this European Standard SIL 1 is representing the lowest level and SIL 3 the highest."

4 Modifications in Clause 14

14.1.2.1.1 b) shall be amended as follows:

" 4) programmable electronic systems in safety related applications in accordance with 14.1.2.6."

A new 14.1.2.6 shall be added as follows:

"**14.1.2.6 Programmable electronic systems in safety related applications (PESSRAL)**

Tables A.1 and A.2 give the safety integrity level for each electric safety device.

Programmable electronic systems designed in accordance with 14.1.2.6 cover the requirements of 14.1.2.3.2.

The minimum requirements of the safety functions common to all SILs are listed in Tables 6, 7 and 8. In addition specific measures required for SILs 1, 2 and 3 are listed respectively in Tables 9, 10 and 11.

NOTE The EN 61508-7:2001 clauses listed in Tables 6 to 11 refer to the relevant requirements in EN 61508-2:2001 and EN 61508-3:2001.

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

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

If a PESSRAL and a non safety related system share the same PCB, the requirements of 13.2.2.3 shall apply for the separation of the two systems."

The following Tables shall be added:

Table 6 - Common measures to avoid and detect failures - Hardware design

No	Object	Measure	EN 61508-7:2001 reference
1	**Processing unit**	Use of watch dog.	A.9
2	**Component selection**	Use of components only within their specifications.	
3	**I/O units and interfaces incl. communication links**	Defined safe state in the event of 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 7 - Common measures to avoid and detect failures - Software design

No	Object	Measure	EN 61508-7:2001 reference
1	**Structure**	Program structure (i.e. modularity, data handling, interface definition) according to the state of the art (see EN 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 number of loops or checking execution time.	
8	**Program**	Array pointer offset checks, if not included in the used programming language.	C.2.6.6
9	**Program**	Defined handling of exceptions (e.g. divisions by zero, overflow, variable range checking etc.) which 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.	EN 61508-1:2001, 7.7.2.1

Table 7 *(continued)*

No	Object	Measure	EN 61508-7:2001 reference
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 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 being reconfiguration.	C.3.13

Table 8 - Common measures for the design and implementation process

No	Measure	EN 61508-7:2001 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 F.6.1 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 9 - Specific measures according to SIL 1

Components and functions	Requirements	Measures	see No. in Annex P	EN 61508-7:2001 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	M 1.1	A.3.1
		two channels or more with comparison.	M 1.3	A.2.5
Processing units	Failures in processing units, which 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	M 2.1	A.3.4
		self-test by software, or	M 2.2	A.3.1
		comparator for two-channel structure, or	M 2.4	A.1.3
		reciprocal comparison by software for 2-channel structure.	M 2.5	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	M 3.5	A.5.5
		block safety with one-word redundancy.	M 3.1	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	M 3.2	A.5.6
		check via test pattern against static or dynamic faults.	M 4.1	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	M 5.4	A.6.2
		test pattern.	M 5.5	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	M 6.1	A.9.4
		reciprocal monitoring.	M 6.2	
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
NOTE As a consequence of the detection of a failure, a safe state of the lift shall be maintained.				

Table 10 - Specific measures according to SIL 2

Components and functions	Requirements	Measures	see No. in Annex P	EN 61508-7:2001 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, which 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.	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
NOTE As a consequence of the detection of a failure, a safe state of the lift shall be maintained.				