

Svenska Elektriska Kommissionen, SEK

Fastställt	Utgåva	Sida	Ingår i
2002-10-09	1	1 (1+72)	SEK Område 65

© Copyright SEK. Reproduction in any form without permission is prohibited.

## Funktionssäkerhet hos elektriska, elektroniska och programmerbara elektroniska säkerhetskritiska system – Del 6: Vägledning vid tillämpning av IEC 61508-2 och IEC 61508-3

*Functional safety of electrical/electronic/programmable electronic safety-related systems –  
Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3*

Som svensk standard gäller europastandarden EN 61508-6:2001. Den svenska standarden innehåller den officiella engelska språkversionen av EN 61508-6:2001.

### Nationellt förord

Europastandarden EN 61508-6:2001

består av:

- **europastandardens ikraftsättningsdokument**, utarbetat inom CENELEC
- **IEC 61508-6, First edition, 2000 - Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3**

utarbetat inom International Electrotechnical Commission, IEC.

SS-EN 61508-6 skall användas tillsammans med SS-EN 61508-2 och SS-EN 61508-3.



EUROPEAN STANDARD

**EN 61508-6**

NORME EUROPÉENNE

EUROPÄISCHE NORM

December 2001

ICS 25.040.40

English version

**Functional safety of electrical/electronic/programmable electronic  
safety-related systems**  
**Part 6: Guidelines on the application**  
**of IEC 61508-2 and IEC 61508-3**  
**(IEC 61508-6:2000)**

Sécurité fonctionnelle des systèmes  
électriques/électroniques/électroniques  
programmables relatifs à la sécurité  
Partie 6: Lignes directrices pour  
l'application de la CEI 61508-2 et  
de la CEI 61508-3  
(CEI 61508-6:2000)

Funktionale Sicherheit  
sicherheitsbezogener elektrischer/  
elektronischer/programmierbarer  
elektronischer Systeme  
Teil 6: Anwendungsrichtlinie für  
IEC 61508-2 und IEC 61508-3  
(IEC 61508-6:2000)

This European Standard was approved by CENELEC on 2001-07-03. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a 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 CENELEC member.

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

CENELEC members are the national electrotechnical committees of Austria, Belgium, Czech Republic, Denmark, Finland, France, Germany, Greece, Iceland, Ireland, Italy, Luxembourg, Malta, Netherlands, Norway, Portugal, Spain, Sweden, Switzerland and United Kingdom.

**CENELEC**

European Committee for Electrotechnical Standardization  
Comité Européen de Normalisation Electrotechnique  
Europäisches Komitee für Elektrotechnische Normung

**Central Secretariat: rue de Stassart 35, B - 1050 Brussels**

## Foreword

The text of the International Standard IEC 61508-6:2000, prepared by SC 65A, System aspects, of IEC TC 65, Industrial-process measurement and control, was submitted to the Unique Acceptance Procedure and was approved by CENELEC as EN 61508-6 on 2001-07-03 without any modification.

The following dates were fixed:

- latest date by which the EN has to be implemented  
at national level by publication of an identical  
national standard or by endorsement (dop) 2002-08-01
- latest date by which the national standards conflicting  
with the EN have to be withdrawn (dow) 2004-08-01

Annexes designated "normative" are part of the body of the standard.

Annexes designated "informative" are given for information only.

In this standard, annex ZA is normative and annexes A to E are informative.

Annex ZA has been added by CENELEC.

IEC 61508 is a basic safety publication covering the functional safety of electrical, electronic and programmable electronic safety-related systems. The scope states:

"This International Standard covers those aspects to be considered when electrical/electronic/programmable electronic systems (E/E/PESs) are used to carry out safety functions. A major objective of this standard is to facilitate the development of application sector international standards by the technical committees responsible for the application sector. This will allow all the relevant factors associated with the application, to be fully taken into account and thereby meet the specific needs of the application sector. A dual objective of this standard is to enable the development of electrical/electronic/programmable electronic (E/E/PE) safety-related systems where application sector international standards may not exist".

The CENELEC Report R0BT-004, ratified by 103 BT (March 2000) accepts that some IEC standards, which today are either published or under development, are sector implementations of IEC 61508. For example:

- IEC 61511, Functional safety - Safety instrumented systems for the process industry sector;
- IEC 62061, Safety of machinery – Functional safety of electrical, electronic and programmable electronic control systems;
- IEC 61513, Nuclear power plants – Instrumentation and control for systems important to safety – General requirements for systems.

The railways sector has also developed a set of European Standards (EN 50126; EN 50128 and prEN 50129).

NOTE EN 50126 and EN 50128 were based on earlier drafts of IEC 61508. prEN 50129 is based on the principles of the latest version of IEC 61508.

This list does not preclude other sector implementations of IEC 61508 which could be currently under development or published within IEC or CENELEC.

---

### **Endorsement notice**

The text of the International Standard IEC 61508-6:2000 was approved by CENELEC as a European Standard without any modification.

In the official version, for Bibliography, the following notes have to be added for the standards indicated:

IEC 61078      NOTE    Harmonized as EN 61078:1993 (not modified).

IEC 61131-3    NOTE    Harmonized as EN 61131-3:1993 (not modified).

---

## Annex ZA (normative)

### Normative references to international publications with their corresponding European publications

This European Standard incorporates by dated or undated reference, provisions from other publications. These normative references are cited at the appropriate places in the text and the publications are listed hereafter. For dated references, subsequent amendments to or revisions of any of these publications apply to this European Standard only when incorporated in it by amendment or revision. For undated references the latest edition of the publication referred to applies (including amendments).

NOTE When an international publication has been modified by common modifications, indicated by (mod), the relevant EN/HD applies.

<u>Publication</u>	<u>Year</u>	<u>Title</u>	<u>EN/HD</u>	<u>Year</u>
IEC 61508-1 + corr. May	1998 1999	Functional safety of electrical/electronic/programmable electronic safety-related systems Part 1: General requirements	EN 61508-1	2001
IEC 61508-2	2000	Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems	EN 61508-2	2001
IEC 61508-3 + corr. April	1998 1999	Part 3: Software requirements	EN 61508-3	2001
IEC 61508-4 + corr. April	1998 1999	Part 4: Definitions and abbreviations	EN 61508-4	2001
IEC 61508-5 + corr. April	1998 1999	Part 5: Examples of methods for the determination of safety integrity levels	EN 61508-5	2001
IEC 61508-7	2000	Part 7: Overview of techniques and measures	EN 61508-7	2001
IEC Guide 104	1997	The preparation of safety publications and the use of basic safety publications and group safety publications	-	-
ISO/IEC Guide 51	1990	Guidelines for the inclusion of safety aspects in standards	-	-

## CONTENTS

Page

## Clause

1	Scope .....	19
2	Normative references.....	23
3	Definitions and abbreviations .....	23
Annex A (informative) Application of IEC 61508-2 and of IEC 61508-3 .....		25
A.1	General.....	25
A.2	Functional steps in the application of IEC 61508-2.....	29
A.3	Functional steps in the application of IEC 61508-3.....	37
Annex B (informative) Example technique for evaluating probabilities of hardware failure ...		41
B.1	General.....	41
B.2	Average probability of failure on demand (for low demand mode of operation) .....	49
B.3	Probability of failure per hour (for high demand or continuous mode of operation) .....	75
B.4	References .....	91
Annex C (informative) Calculation of diagnostic coverage and safe failure fraction: worked example .....		93
Annex D (informative) A methodology for quantifying the effect of hardware-related common cause failures in E/E/PE systems .....		101
D.1	General.....	101
D.2	Brief overview.....	101
D.3	Scope of the methodology.....	109
D.4	Points taken into account in the methodology .....	109
D.5	Using the $\beta$ -factor to calculate the probability of failure in an E/E/PE safety-related system due to common cause failures .....	111
D.6	Using the tables to estimate $\beta$ .....	113
D.7	Examples of the use of the methodology.....	121
D.8	References .....	123
Annex E (informative) Example applications of software safety integrity tables of IEC 61508-3 .....		125
E.1	General.....	125
E.2	Example for safety integrity level 2 .....	125
E.3	Example for safety integrity level 3 .....	135
Bibliography .....		145

	Page
Figure 1 – Overall framework of IEC 61508 .....	21
Figure A.1 – Application of IEC 61508-2 .....	33
Figure A.2 – Application of IEC 61508-2 (continued) .....	35
Figure A.3 – Application of IEC 61508-3 .....	39
Figure B.1 – Example configuration for two sensor channels .....	45
Figure B.2 – Subsystem structure .....	49
Figure B.3 – 1oo1 physical block diagram .....	51
Figure B.4 – 1oo1 reliability block diagram .....	51
Figure B.5 – 1oo2 physical block diagram .....	53
Figure B.6 – 1oo2 reliability block diagram .....	55
Figure B.7 – 2oo2 physical block diagram .....	55
Figure B.8 – 2oo2 reliability block diagram .....	55
Figure B.9 – 1oo2D physical block diagram .....	57
Figure B.10 – 1oo2D reliability block diagram .....	57
Figure B.11 – 2oo3 physical block diagram .....	59
Figure B.12 – 2oo3 reliability block diagram .....	59
Figure B.13 – Architecture of an example for low demand mode of operation .....	69
Figure B.14 – Architecture of an example for high demand or continuous mode of operation .....	87
Figure D.1 – Relationship of common cause failures to the failures of individual channels..	105
 Table B.1 – Terms and their ranges used in this annex (applies to 1oo1, 1oo2, 2oo2, 1oo2D and 2oo3) .....	 47
Table B.2 – Average probability of failure on demand for a proof test interval of six months and a mean time to restoration of 8 h .....	61
Table B.3 – Average probability of failure on demand for a proof-test interval of one year and mean time to restoration of 8 h .....	63
Table B.4 – Average probability of failure on demand for a proof-test interval of two years and a mean time to restoration of 8 h .....	65
Table B.5 – Average probability of failure on demand for a proof-test interval of 10 years and a mean time to restoration of 8 h .....	67
Table B.6 – Average probability of failure on demand for the sensor subsystem in the example for low demand mode of operation (one year proof-test interval and 8 h MTTR) .....	69
Table B.7 – Average probability of failure on demand for the logic subsystem in the example for low demand mode of operation (one year proof-test interval and 8 h MTTR) .....	71
Table B.8 – Average probability of failure on demand for the final element subsystem in the example for low demand mode of operation (one year proof-test interval and 8 h MTTR) .....	71



Table B.9 – Example for a non-perfect proof test.....	75
Table B.10 – Probability of failure per hour (in high demand or continuous mode of operation) for a proof-test interval of one month and a mean time to restoration of 8 h.....	79
Table B.11 – Probability of failure per hour (in high demand or continuous mode of operation) for a proof test interval of three months and a mean time to restoration of 8 h.....	81
Table B.12 – Probability of failure per hour (in high demand or continuous mode of operation) for a proof test interval of six months and a mean time to restoration of 8 h.....	83
Table B.13 – Probability of failure per hour (in high demand or continuous mode of operation) for a proof-test interval of one year and a mean time to restoration of 8 h.....	85
Table B.14 – Probability of failure per hour for the sensor subsystem in the example for high demand or continuous mode of operation (six month proof-test interval and 8 h MTTR).....	87
Table B.15 – Probability of failure per hour for the logic subsystem in the example for high demand or continuous mode of operation (six month proof-test interval and 8 h MTTR).....	89
Table B.16 – Probability of failure per hour for the final element subsystem in the example for high demand or continuous mode of operation (six month proof-test interval and 8 h MTTR) .....	89
Table C.1 – Example calculations for diagnostic coverage and safe failure fraction .....	97
Table C.2 – Diagnostic coverage and effectiveness for different subsystems .....	99
Table D.1 – Scoring programmable electronics or sensors/final elements.....	115
Table D.2 – Value of Z: programmable electronics .....	119
Table D.3 – Value of Z: sensors or final elements.....	119
Table D.4 – Calculation of $\beta$ or $\beta_D$ .....	121
Table D.5 – Example values for programmable electronics.....	123
Table E.1 – Software safety requirements specification (see 7.2 of IEC 61508-3).....	127
Table E.2 – Software design and development: software architecture design (see 7.4.3 of IEC 61508-3).....	129
Table E.3 – Software design and development: support tools and programming language (see 7.4.4 of IEC 61508-3) .....	129
Table E.4 – Software design and development: detailed design (see 7.4.5 and 7.4.6 of IEC 61508-3) (this includes software system design, software module design and coding) .....	131
Table E.5 – Software design and development: software module testing and integration (see 7.4.7 and 7.4.8 of IEC 61508-3).....	131
Table E.6 – Programmable electronics integration (hardware and software) (see 7.5 of IEC 61508-3).....	131
Table E.7 – Software safety validation (see 7.7 of IEC 61508-3) .....	133
Table E.8 – Software modification (see 7.8 of IEC 61508-3) .....	133
Table E.9 – Software verification (see 7.9 of part 3) .....	133
Table E.10 – Functional safety assessment (see clause 8 of IEC 61508-3) .....	135

	Page
Table E.11 – Software safety requirements specification (see 7.2 of IEC 61508-3) .....	137
Table E.12 – Software design and development: software architecture design (see 7.4.3 of IEC 61508-3) .....	137
Table E.13 – Software design and development: support tools and programming language (see 7.4.4 of IEC 61508-3) .....	139
Table E.14 – Software design and development: detailed design (see 7.4.5 and 7.4.6 of IEC 61508-3) (this includes software system design, software module design and coding) .....	139
Table E.15 – Software design and development: software module testing and integration (see 7.4.7 and 7.4.8 of IEC 61508-3) .....	141
Table E.16 – Programmable electronics integration (hardware and software) (see 7.5 of IEC 61508-3) .....	141
Table E.17 – Software safety validation (see 7.7 of IEC 61508-3) .....	141
Table E.18 – Modification (see 7.8 of IEC 61508-3) .....	143
Table E.19 – Software verification (see 7.9 of IEC 61508-3) .....	143
Table E.20 – Functional safety assessment (see clause 8 of IEC 61508-3) .....	143

## **FUNCTIONAL SAFETY OF ELECTRICAL/ELECTRONIC/PROGRAMMABLE ELECTRONIC SAFETY-RELATED SYSTEMS –**

### **Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3**

#### **1 Scope**

**1.1** This part of IEC 61508 contains information and guidelines on IEC 61508-2 and IEC 61508-3.

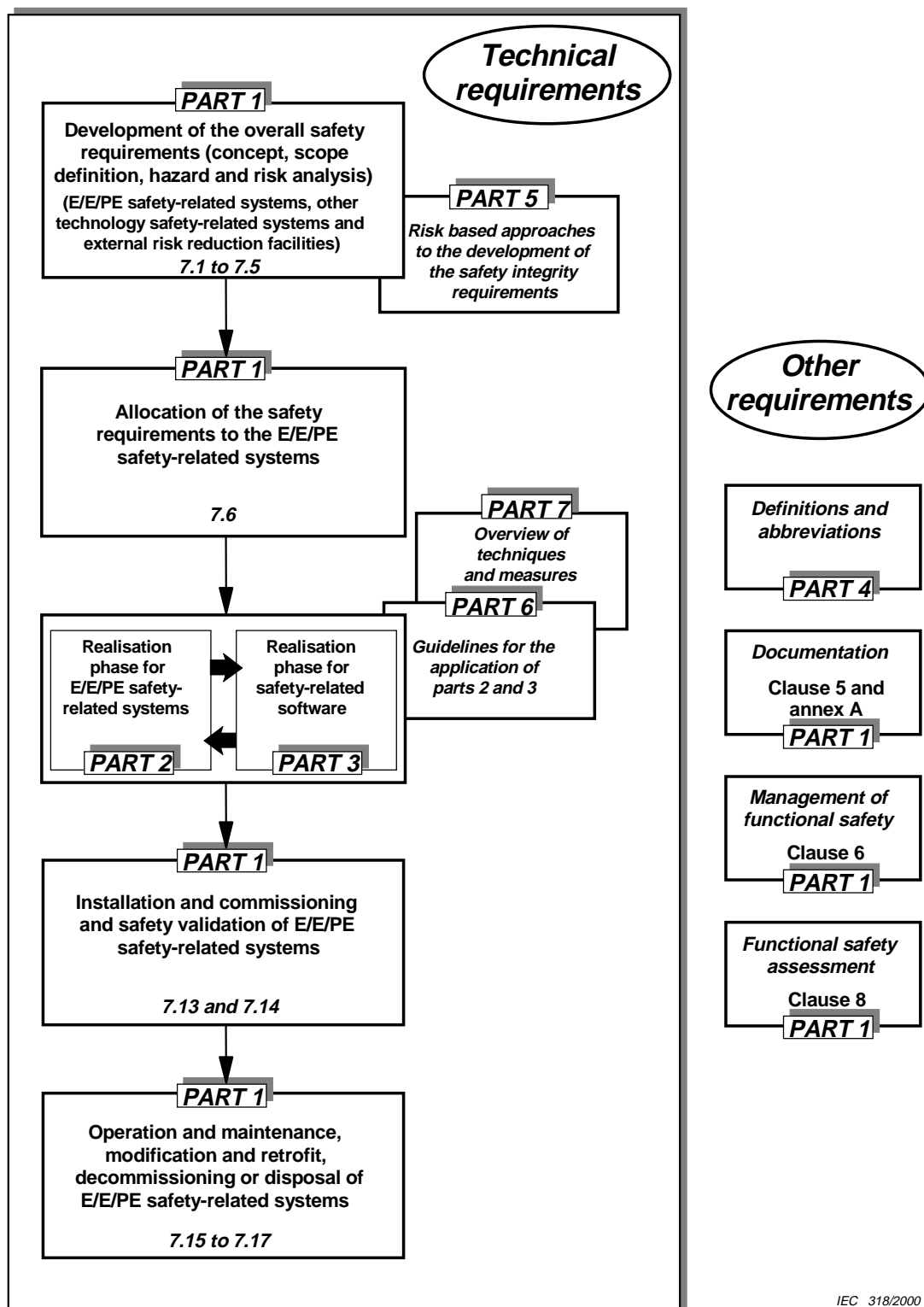
- Annex A gives a brief overview of the requirements of IEC 61508-2 and IEC 61508-3 and sets out the functional steps in their application.
- Annex B gives an example technique for calculating the probabilities of hardware failure and should be read in conjunction with 7.4.3 and annex C of IEC 61508-2 and annex D.
- Annex C gives a worked example of calculating diagnostic coverage and should be read in conjunction with annex C of IEC 61508-2.
- Annex D gives a methodology for quantifying the effect of hardware-related common cause failures on the probability of failure.
- Annex E gives worked examples of the application of the software safety integrity tables specified in annex A of IEC 61508-3 for safety integrity levels 2 and 3.

**1.2** IEC 61508-1, IEC 61508-2, IEC 61508-3 and IEC 61508-4 are basic safety publications, although this status does not apply in the context of low complexity E/E/PE safety-related systems (see 3.4.4 of IEC 61508-4). As basic safety publications, they are intended for use by technical committees in the preparation of standards in accordance with the principles contained in IEC Guide 104 and IEC/ISO Guide 51. IEC 61508 is also intended for use as a stand-alone standard.

**1.3** One of the responsibilities of a technical committee is, wherever applicable, to make use of basic safety publications in the preparation of its publications. In this context, the requirements, test methods or test conditions of this basic safety publication do not apply unless specifically referred to or included in the publications prepared by those technical committees.

**NOTE** In the USA and Canada, until the proposed process sector implementation of IEC 61508 (i.e. IEC 61511) is published as an international standard, existing national process safety standards based on IEC 61508 (i.e. ANSI/ISA S84.01-1996) can be applied to the process sector instead of IEC 61508.

**1.4** Figure 1 shows the overall framework for parts 1 to 7 of this standard and indicates the role that IEC 61508-6 plays in the achievement of functional safety for E/E/PE safety-related systems.



IEC 318/2000

Figure 1 – Overall framework of IEC 61508