

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

Säkerhetsfordringar på elektriska, elektroniska och programmerbara elektroniska säkerhetskritiska systems funktion – 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 61508-6:2010. Den svenska standarden innehåller den officiella engelska språkversionen av EN 61508-6:2010.

Nationellt förord

Europastandarden EN 61508-6:2010

består av:

- **europastandardens ikraftsättningsdokument**, utarbetat inom CENELEC
- **IEC 61508-6, Second edition, 2010 - Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3**

utarbetad inom International Electrotechnical Commission, IEC.

Tidigare fastställd svensk standard SS-EN 61508-6, utgåva 1, 2002, gäller ej fr o m 2013-05-01.

Standarder underlättar utvecklingen och höjer elsäkerheten

Det finns många fördelar med att ha gemensamma tekniska regler för bl a säkerhet, prestanda, dokumentation, utförande och skötsel av elprodukter, elanläggningar och metoder. Genom att utforma sådana standarder blir säkerhetskraven tydliga och utvecklingskostnaderna rimliga samtidigt som marknadens acceptans för produkten eller tjänsten ökar.

Många standarder inom elområdet beskriver tekniska lösningar och metoder som åstadkommer den elsäkerhet som föreskrivs av svenska myndigheter och av EU.

SEK är Sveriges röst i standardiseringsarbetet inom elområdet

SEK Svensk Elstandard svarar för standardiseringen inom elområdet i Sverige och samordnar svensk medverkan i internationell och europeisk standardisering. SEK är en ideell organisation med frivilligt deltagande från svenska myndigheter, företag och organisationer som vill medverka till och påverka utformningen av tekniska regler inom elektrotekniken.

SEK samordnar svenska intressenters medverkan i SEKs tekniska kommittéer och stödjer svenska experters medverkan i internationella och europeiska projekt.

Stora delar av arbetet sker internationellt

Utformningen av standarder sker i allt väsentligt i internationellt och europeiskt samarbete. SEK är svensk nationalkommitté av International Electrotechnical Commission (IEC) och Comité Européen de Normalisation Electrotechnique (CENELEC).

Standardiseringsarbetet inom SEK är organiserat i referensgrupper bestående av ett antal tekniska kommittéer som speglar hur arbetet inom IEC och CENELEC är organiserat.

Arbetet i de tekniska kommittéerna är öppet för alla svenska organisationer, företag, institutioner, myndigheter och statliga verk. Den årliga avgiften för deltagandet och intäkter från försäljning finansierar SEKs standardiseringsverksamhet och medlemsavgift till IEC och CENELEC.

Var med och påverka!

Den som deltar i SEKs tekniska kommittéarbete har möjlighet att påverka framtida standarder och får tidig tillgång till information och dokumentation om utvecklingen inom sitt teknikområde. Arbetet och kontakterna med kollegor, kunder och konkurrenter kan gynnsamt påverka enskilda företags affärsutveckling och bidrar till deltagarnas egen kompetensutveckling.

Du som vill dra nytta av dessa möjligheter är välkommen att kontakta SEKs kansli för mer information.

SEK Svensk Elstandard

Box 1284
164 29 Kista
Tel 08-444 14 00
www.elstandard.se

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 61508-6:2010)**

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 61508-6:2010)

Funktionale Sicherheit sicherheitsbezogener
elektrischer/elektronischer/programmierbarer
elektronischer Systeme -
Teil 6: Anwendungsrichtlinie für IEC 61508-2
und IEC 61508-3
(IEC 61508-6:2010)

This European Standard was approved by CENELEC on 2010-05-01. 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, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland and the United Kingdom.

CENELEC

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

Management Centre: Avenue Marnix 17, B - 1000 Brussels

Foreword

The text of document 65A/553/FDIS, future edition 2 of IEC 61508-6, prepared by SC 65A, System aspects, of IEC TC 65, Industrial-process measurement, control and automation, was submitted to the IEC-CENELEC parallel vote and was approved by CENELEC as EN 61508-6 on 2010-05-01.

This European Standard supersedes EN 61508-6:2001.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN and CENELEC shall not be held responsible for identifying any or all such patent rights.

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) | 2011-02-01 |
| – latest date by which the national standards conflicting with the EN have to be withdrawn | (dow) | 2013-05-01 |

Annex ZA has been added by CENELEC.

Endorsement notice

The text of the International Standard IEC 61508-6:2010 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:

[1] IEC 61511 series	NOTE Harmonized in EN 61511 series (not modified).
[2] IEC 62061	NOTE Harmonized as EN 62061.
[3] IEC 61800-5-2	NOTE Harmonized as EN 61800-5-2.
[4] IEC 61078:2006	NOTE Harmonized as EN 61078:2006 (not modified).
[5] IEC 61165:2006	NOTE Harmonized as EN 61165:2006 (not modified).
[16] IEC 61131-3:2003	NOTE Harmonized as EN 61131-3:2003 (not modified).
[18] IEC 61025:2006	NOTE Harmonized as EN 61025:2007 (not modified).
[26] IEC 60601 series	NOTE Harmonized in EN 60601 series (partially modified).
[27] IEC 61508-1:2010	NOTE Harmonized as EN 61508-1:2010 (not modified).
[28] IEC 61508-5:2010	NOTE Harmonized as EN 61508-5:2010 (not modified).
[29] IEC 61508-7:2010	NOTE Harmonized as EN 61508-7:2010 (not modified).

Annex ZA (normative)

Normative references to international publications with their corresponding European publications

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.

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 61508-2	2010	Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems	EN 61508-2	2010
IEC 61508-3	2010	Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 3: Software requirements	EN 61508-3	2010
IEC 61508-4	2010	Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 4: Definitions and abbreviations	EN 61508-4	2010

CONTENTS

INTRODUCTION.....	8
1 Scope.....	10
2 Normative references	12
3 Definitions and abbreviations.....	12
Annex A (informative) Application of IEC 61508-2 and of IEC 61508-3.....	13
Annex B (informative) Example of technique for evaluating probabilities of hardware failure	21
Annex C (informative) Calculation of diagnostic coverage and safe failure fraction – worked example.....	76
Annex D (informative) A methodology for quantifying the effect of hardware-related common cause failures in E/E/PE systems.....	80
Annex E (informative) Example applications of software safety integrity tables of IEC 61508-3	95
Bibliography.....	110
Figure 1 – Overall framework of the IEC 61508 series	11
Figure A.1 – Application of IEC 61508-2	17
Figure A.2 – Application of IEC 61508-2 (Figure A.1 <i>continued</i>).....	18
Figure A.3 – Application of IEC 61508-3	20
Figure B.1 – Reliability Block Diagram of a whole safety loop	22
Figure B.2 – Example configuration for two sensor channels.....	26
Figure B.3 – Subsystem structure	29
Figure B.4 – 1oo1 physical block diagram.....	30
Figure B.5 – 1oo1 reliability block diagram.....	31
Figure B.6 – 1oo2 physical block diagram.....	32
Figure B.7 – 1oo2 reliability block diagram.....	32
Figure B.8 – 2oo2 physical block diagram.....	33
Figure B.9 – 2oo2 reliability block diagram.....	33
Figure B.10 – 1oo2D physical block diagram.....	33
Figure B.11 – 1oo2D reliability block diagram	34
Figure B.12 – 2oo3 physical block diagram.....	34
Figure B.13 – 2oo3 reliability block diagram.....	35
Figure B.14 – Architecture of an example for low demand mode of operation.....	40
Figure B.15 – Architecture of an example for high demand or continuous mode of operation	49
Figure B.16 – Reliability block diagram of a simple whole loop with sensors organised into 2oo3 logic	51
Figure B.17 – Simple fault tree equivalent to the reliability block diagram presented on Figure B.1.....	52
Figure B.18 – Equivalence fault tree / reliability block diagram.....	52
Figure B.19 – Instantaneous unavailability $U(t)$ of single periodically tested components	54
Figure B.20 – Principle of PFD_{avg} calculations when using fault trees.....	55

Figure B.21 – Effect of staggering the tests	56
Figure B.22 – Example of complex testing pattern	56
Figure B.23 – Markov graph modelling the behaviour of a two component system	58
Figure B.24 – Principle of the multiphase Markovian modelling	59
Figure B.25 – Saw-tooth curve obtained by multiphase Markovian approach.....	60
Figure B.26 – Approximated Markovian model	60
Figure B.27 – Impact of failures due to the demand itself.....	61
Figure B.28 – Modelling of the impact of test duration.....	61
Figure B.29 – Multiphase Markovian model with both DD and DU failures	62
Figure B.30 – Changing logic (2oo3 to 1oo2) instead of repairing first failure	63
Figure B.31 – "Reliability" Markov graphs with an absorbing state	63
Figure B.32 – "Availability" Markov graphs without absorbing states	65
Figure B.33 – Petri net for modelling a single periodically tested component.....	66
Figure B.34 – Petri net to model common cause failure and repair resources.....	69
Figure B.35 – Using reliability block diagrams to build Petri net and auxiliary Petri net for <i>PFD</i> and <i>PFH</i> calculations	70
Figure B.36 – Simple Petri net for a single component with revealed failures and repairs	71
Figure B.37 – Example of functional and dysfunctional modelling with a formal language.....	72
Figure B.38 – Uncertainty propagation principle.....	73
Figure D.1 – Relationship of common cause failures to the failures of individual channels	82
Figure D.2 – Implementing shock model with fault trees.....	93
 Table B.1 – Terms and their ranges used in this annex (applies to 1oo1, 1oo2, 2oo2, 1oo2D, 1oo3 and 2oo3)	27
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	36
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.....	37
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	38
Table B.5 – Average probability of failure on demand for a proof test interval of ten years and a mean time to restoration of 8 h	39
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 <i>MTTR</i>)	40
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 <i>MTTR</i>)	41
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 <i>MTTR</i>)	41
Table B.9 – Example for a non-perfect proof test	42
Table B.10 – Average frequency of a dangerous failure (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	45

Table B.11 – Average frequency of a dangerous failure (in high demand or continuous mode of operation) for a proof test interval of three month and a mean time to restoration of 8 h	46
Table B.12 – Average frequency of a dangerous failure (in high demand or continuous mode of operation) for a proof test interval of six month and a mean time to restoration of 8 h	Error! Bookmark not defined.
Table B.13 – Average frequency of a dangerous failure (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	Error! Bookmark not defined.
Table B.14 – Average frequency of a dangerous failure for the sensor subsystem in the example for high demand or continuous mode of operation (six month proof test interval and 8 h <i>MTTR</i>)	49
Table B.15 – Average frequency of a dangerous failure for the logic subsystem in the example for high demand or continuous mode of operation (six month proof test interval and 8 h <i>MTTR</i>)	50
Table B.16 – Average frequency of a dangerous failure for the final element subsystem in the example for high demand or continuous mode of operation (six month proof test interval and 8 h <i>MTTR</i>)	50
Table C.1 – Example calculations for diagnostic coverage and safe failure fraction	78
Table C.2 – Diagnostic coverage and effectiveness for different elements	79
Table D.1 – Scoring programmable electronics or sensors/final elements	88
Table D.2 – Value of Z – programmable electronics	89
Table D.3 – Value of Z – sensors or final elements	89
Table D.4 – Calculation of β_{int} or $\beta_{\text{D int}}$	90
Table D.5 – Calculation of β for systems with levels of redundancy greater than 1oo2	91
Table D.6 – Example values for programmable electronics	92
Table E.1 – Software safety requirements specification	96
Table E.2 – Software design and development – software architecture design	97
Table E.3 – Software design and development – support tools and programming language	98
Table E.4 – Software design and development – detailed design	99
Table E.5 – Software design and development – software module testing and integration	100
Table E.6 – Programmable electronics integration (hardware and software)	100
Table E.7 – Software aspects of system safety validation	101
Table E.8 – Modification	101
Table E.9 – Software verification	102
Table E.10 – Functional safety assessment	102
Table E.11 – Software safety requirements specification	104
Table E.12 – Software design and development – software architecture design	104
Table E.13 – Software design and development – support tools and programming language	105
Table E.14 – Software design and development – detailed design	106
Table E.15 – Software design and development – software module testing and integration	106
Table E.16 – Programmable electronics integration (hardware and software)	107
Table E.17 – Software aspects of system safety validation	108
Table E.18 – Modification	108

Table E.19 – Software verification	109
Table E.20 – Functional safety assessment	109

INTRODUCTION

Systems comprised of electrical and/or electronic elements have been used for many years to perform safety functions in most application sectors. Computer-based systems (generically referred to as programmable electronic systems) are being used in all application sectors to perform non-safety functions and, increasingly, to perform safety functions. If computer system technology is to be effectively and safely exploited, it is essential that those responsible for making decisions have sufficient guidance on the safety aspects on which to make these decisions.

This International Standard sets out a generic approach for all safety lifecycle activities for systems comprised of electrical and/or electronic and/or programmable electronic (E/E/PE) elements that are used to perform safety functions. This unified approach has been adopted in order that a rational and consistent technical policy be developed for all electrically-based safety-related systems. A major objective is to facilitate the development of product and application sector international standards based on the IEC 61508 series.

In most situations, safety is achieved by a number of systems which rely on many technologies (for example mechanical, hydraulic, pneumatic, electrical, electronic, programmable electronic). Any safety strategy must therefore consider not only all the elements within an individual system (for example sensors, controlling devices and actuators) but also all the safety-related systems making up the total combination of safety-related systems. Therefore, while this International Standard is concerned with E/E/PE safety-related systems, it may also provide a framework within which safety-related systems based on other technologies may be considered.

It is recognized that there is a great variety of applications using E/E/PE safety-related systems in a variety of application sectors and covering a wide range of complexity, hazard and risk potentials. In any particular application, the required safety measures will be dependent on many factors specific to the application. This International Standard, by being generic, will enable such measures to be formulated in future product and application sector international standards and in revisions of those that already exist.

This International Standard

- considers all relevant overall, E/E/PE system and software safety lifecycle phases (for example, from initial concept, through design, implementation, operation and maintenance to decommissioning) when E/E/PE systems are used to perform safety functions;
- has been conceived with a rapidly developing technology in mind; the framework is sufficiently robust and comprehensive to cater for future developments;
- enables product and application sector international standards, dealing with E/E/PE safety-related systems, to be developed; the development of product and application sector international standards, within the framework of this standard, should lead to a high level of consistency (for example, of underlying principles, terminology etc.) both within application sectors and across application sectors; this will have both safety and economic benefits;
- provides a method for the development of the safety requirements specification necessary to achieve the required functional safety for E/E/PE safety-related systems;
- adopts a risk-based approach by which the safety integrity requirements can be determined;
- introduces safety integrity levels for specifying the target level of safety integrity for the safety functions to be implemented by the E/E/PE safety-related systems;

NOTE 2 The standard does not specify the safety integrity level requirements for any safety function, nor does it mandate how the safety integrity level is determined. Instead it provides a risk-based conceptual framework and example techniques.

- sets target failure measures for safety functions carried out by E/E/PE safety-related systems, which are linked to the safety integrity levels;

- sets a lower limit on the target failure measures for a safety function carried out by a single E/E/PE safety-related system. For E/E/PE safety-related systems operating in
 - a low demand mode of operation, the lower limit is set at an average probability of a dangerous failure on demand of 10^{-5} ;
 - a high demand or a continuous mode of operation, the lower limit is set at an average frequency of a dangerous failure of 10^{-9} [h^{-1}];

NOTE 3 A single E/E/PE safety-related system does not necessarily mean a single-channel architecture.

NOTE 4 It may be possible to achieve designs of safety-related systems with lower values for the target safety integrity for non-complex systems, but these limits are considered to represent what can be achieved for relatively complex systems (for example programmable electronic safety-related systems) at the present time.

- sets requirements for the avoidance and control of systematic faults, which are based on experience and judgement from practical experience gained in industry. Even though the probability of occurrence of systematic failures cannot in general be quantified the standard does, however, allow a claim to be made, for a specified safety function, that the target failure measure associated with the safety function can be considered to be achieved if all the requirements in the standard have been met;
- introduces systematic capability which applies to an element with respect to its confidence that the systematic safety integrity meets the requirements of the specified safety integrity level;
- adopts a broad range of principles, techniques and measures to achieve functional safety for E/E/PE safety-related systems, but does not explicitly use the concept of fail safe. However, the concepts of “fail safe” and “inherently safe” principles may be applicable and adoption of such concepts is acceptable providing the requirements of the relevant clauses in the standard are met.

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 3.4.3 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 ISO/IEC Guide 51. IEC 61508-1, IEC 61508-2, IEC 61508-3 and IEC 61508-4 are also intended for use as stand-alone publications. The horizontal safety function of this international standard does not apply to medical equipment in compliance with the IEC 60601 series.

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 will not apply unless specifically referred to or included in the publications prepared by those technical committees.

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

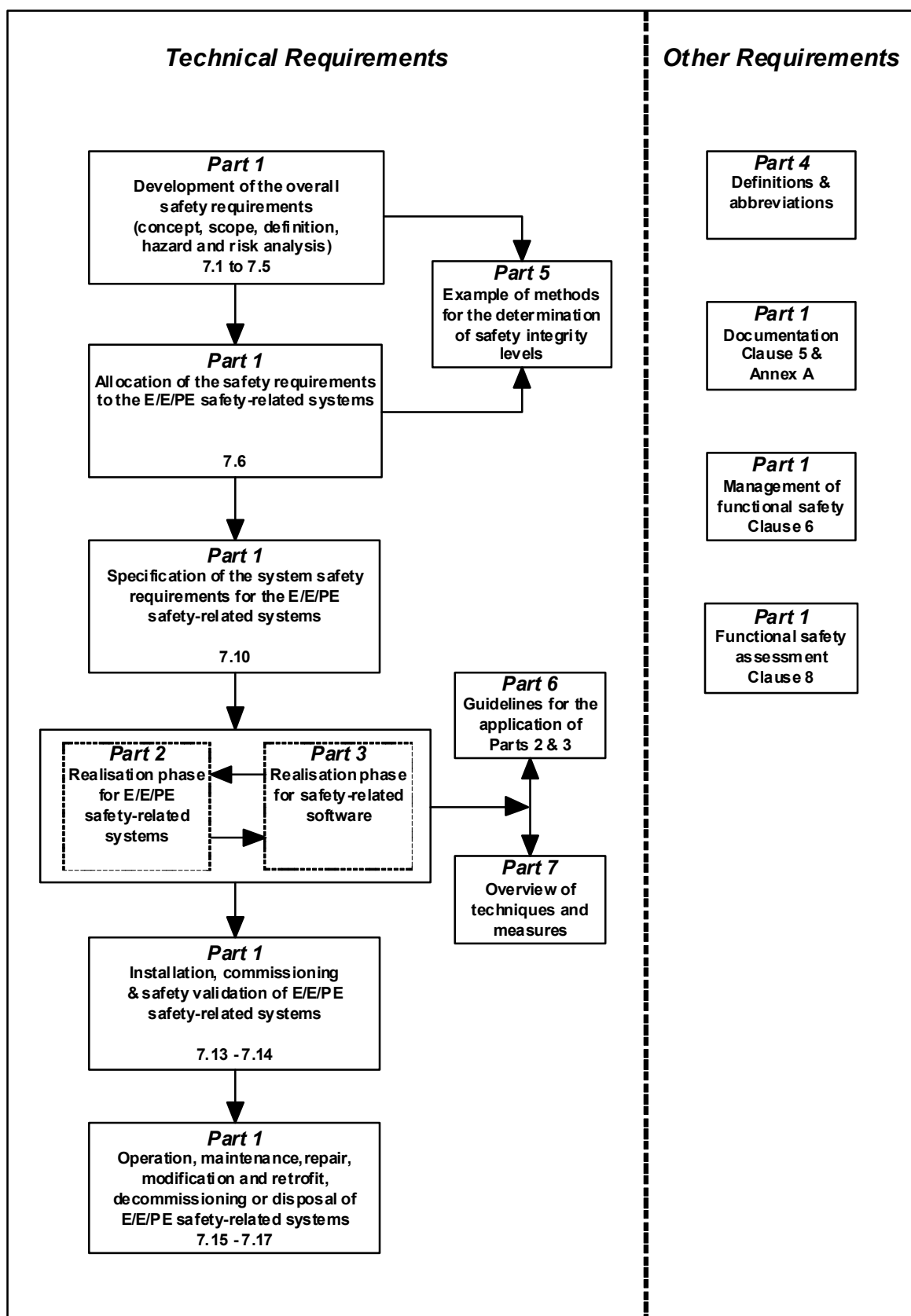


Figure 1 – Overall framework of the IEC 61508 series

2 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 61508-2:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems*

IEC 61508-3:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 3: Software requirements*

IEC 61508-4:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 4: Definitions and abbreviations*