

**Functional safety of electrical/electronic/programmable  
electronic safety-related systems - Part 3: Software  
requirements**

## EESTI STANDARDI EESSÕNA

## NATIONAL FOREWORD

<p>Käesolev Eesti standard EVS-EN 61508-3:2010 sisaldab Euroopa standardi EN 61508-3:2010 ingliskeelset teksti.</p> <p>Standard on kinnitatud Eesti Standardikeskuse 31.08.2010 käskkirjaga ja jõustub sellekohase teate avaldamisel EVS Teatajas.</p> <p>Euroopa standardimisorganisatsioonide poolt rahvuslikele liikmetele Euroopa standardi teksti kättesaadavaks tegemise kuupäev on 28.05.2010.</p> <p>Standard on kättesaadav Eesti standardiorganisatsioonist.</p>	<p>This Estonian standard EVS-EN 61508-3:2010 consists of the English text of the European standard EN 61508-3:2010.</p> <p>This standard is ratified with the order of Estonian Centre for Standardisation dated 31.08.2010 and is endorsed with the notification published in the official bulletin of the Estonian national standardisation organisation.</p> <p>Date of Availability of the European standard text 28.05.2010.</p> <p>The standard is available from Estonian standardisation organisation.</p>
----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

ICS 25.040.40

**Võtmesõnad:** computer programs, computers, pr, programming, reliability, safety, safety devices, safety engineering, safety measures, safety requirements, safety studies, safety systems, sample surveys, specification (approval), specifications, surveillance (approval), testing

### Standardite reprodutseerimis- ja levitamiseõigus kuulub Eesti Standardikeskusele

Andmete paljundamine, taastekitamine, kopeerimine, salvestamine elektroonilisse süsteemi või edastamine ükskõik millises vormis või millisel teel on keelatud ilma Eesti Standardikeskuse poolt antud kirjaliku loata.

Kui Teil on küsimusi standardite autorikaitse kohta, palun võtke ühendust Eesti Standardikeskusega:  
Aru 10 Tallinn 10317 Eesti; [www.evs.ee](http://www.evs.ee); Telefon: 605 5050; E-post: [info@evs.ee](mailto:info@evs.ee)

### Right to reproduce and distribute belongs to the Estonian Centre for Standardisation

No part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying, without permission in writing from Estonian Centre for Standardisation.

If you have any questions about standards copyright, please contact Estonian Centre for Standardisation:  
Aru str 10 Tallinn 10317 Estonia; [www.evs.ee](http://www.evs.ee); Phone: 605 5050; E-mail: [info@evs.ee](mailto:info@evs.ee)

English version

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

Sécurité fonctionnelle des systèmes  
électriques/électroniques/électroniques  
programmables relatifs à la sécurité -  
Partie 3: Exigences concernant  
les logiciels  
(CEI 61508-3:2010)

Funktionale Sicherheit sicherheitsbezogener  
elektrischer/elektronischer/programmierbarer  
elektronischer Systeme -  
Teil 3: Anforderungen an Software  
(IEC 61508-3:2010)

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/550/FDIS, future edition 2 of IEC 61508-3, 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 61508-3 on 2010-05-01.

This European Standard supersedes EN 61508-3:2001.

It has the status of a basic safety publication according to IEC Guide 104.

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 61508-3:2010 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 61508-5:2010 | NOTE Harmonized as EN 61508-5:2010 (not modified).    |
| [5] IEC 61508-6:2010 | NOTE Harmonized as EN 61508-6:2010 (not modified).    |
| [6] IEC 61508-7:2010 | NOTE Harmonized as EN 61508-7:2010 (not modified).    |
| [7] IEC 60601 series | NOTE Harmonized in 60601 series (partially modified). |
| [8] IEC 61131-3      | NOTE Harmonized as EN 61131-3.                        |

## 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 61508-1	2010	Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 1: General requirements	EN 61508-1	2010
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 61508-4	2010	Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 4: Definitions and abbreviations	EN 61508-4	2010
IEC Guide 104	1997	The preparation of safety publications and the use of basic safety publications and group safety publications	-	-
ISO/IEC Guide 51	1999	Safety aspects - Guidelines for their inclusion in standards	-	-

## CONTENTS

FOREWORD.....	5
INTRODUCTION.....	7
1 Scope.....	9
2 Normative references.....	12
3 Definitions and abbreviations.....	13
4 Conformance to this standard.....	13
5 Documentation.....	13
6 Additional requirements for management of safety-related software.....	13
6.1 Objectives.....	13
6.2 Requirements.....	13
7 Software safety lifecycle requirements.....	14
7.1 General.....	14
7.1.1 Objective.....	14
7.1.2 Requirements.....	14
7.2 Software safety requirements specification.....	21
7.2.1 Objectives.....	21
7.2.2 Requirements.....	21
7.3 Validation plan for software aspects of system safety.....	24
7.3.1 Objective.....	24
7.3.2 Requirements.....	24
7.4 Software design and development.....	25
7.4.1 Objectives.....	25
7.4.2 General requirements.....	26
7.4.3 Requirements for software architecture design.....	29
7.4.4 Requirements for support tools, including programming languages.....	30
7.4.5 Requirements for detailed design and development – software system design.....	33
7.4.6 Requirements for code implementation.....	34
7.4.7 Requirements for software module testing.....	35
7.4.8 Requirements for software integration testing.....	35
7.5 Programmable electronics integration (hardware and software).....	36
7.5.1 Objectives.....	36
7.5.2 Requirements.....	36
7.6 Software operation and modification procedures.....	37
7.6.1 Objective.....	37
7.6.2 Requirements.....	37
7.7 Software aspects of system safety validation.....	37
7.7.1 Objective.....	37
7.7.2 Requirements.....	38
7.8 Software modification.....	39
7.8.1 Objective.....	39
7.8.2 Requirements.....	39
7.9 Software verification.....	41
7.9.1 Objective.....	41
7.9.2 Requirements.....	41
8 Functional safety assessment.....	44

Annex A (normative) Guide to the selection of techniques and measures.....	46
Annex B (informative) Detailed tables .....	55
Annex C (informative) Properties for software systematic capability.....	60
Annex D (normative) Safety manual for compliant items – additional requirements for software elements.....	97
Annex E (informative) Relationships between IEC 61508-2 and IEC 61508-3.....	100
Annex F (informative) Techniques for achieving non-interference between software elements on a single computer .....	102
Annex G (informative) Guidance for tailoring lifecycles associated with data driven systems .....	107
Bibliography.....	111
Figure 1 – Overall framework of the IEC 61508 series .....	11
Figure 2 – Overall safety lifecycle .....	12
Figure 3 – E/E/PE system safety lifecycle (in realisation phase).....	16
Figure 4 – Software safety lifecycle (in realisation phase).....	16
Figure 5 – Relationship and scope for IEC 61508-2 and IEC 61508-3 .....	17
Figure 6 – Software systematic capability and the development lifecycle (the V-model) .....	17
Figure G.1 – Variability in complexity of data driven systems .....	108
Table 1 – Software safety lifecycle – overview.....	18
Table A.1 – Software safety requirements specification .....	47
Table A.2 – Software design and development – software architecture design .....	48
Table A.3 – Software design and development – support tools and programming language.....	49
Table A.4 – Software design and development – detailed design .....	50
Table A.5 – Software design and development – software module testing and integration .....	51
Table A.6 – Programmable electronics integration (hardware and software).....	51
Table A.7 – Software aspects of system safety validation .....	52
Table A.8 – Modification .....	52
Table A.9 – Software verification .....	53
Table A.10 – Functional safety assessment .....	54
Table B.1 – Design and coding standards .....	55
Table B.2 – Dynamic analysis and testing.....	56
Table B.3 – Functional and black-box testing.....	56
Table B.4 – Failure analysis.....	57
Table B.5 – Modelling .....	57
Table B.6 – Performance testing.....	58
Table B.7 – Semi-formal methods .....	58
Table B.8 – Static analysis.....	59
Table B.9 – Modular approach .....	59
Table C.1 – Properties for systematic safety integrity – Software safety requirements specification .....	64

Table C.2 – Properties for systematic safety integrity – Software design and development – software Architecture Design .....	67
Table C.3 – Properties for systematic safety integrity – Software design and development – support tools and programming language .....	76
Table C.4 – Properties for systematic safety integrity – Software design and development – detailed design (includes software system design, software module design and coding) .....	77
Table C.5 – Properties for systematic safety integrity – Software design and development – software module testing and integration .....	79
Table C.6 – Properties for systematic safety integrity – Programmable electronics integration (hardware and software) .....	81
Table C.7 – Properties for systematic safety integrity – Software aspects of system safety validation .....	82
Table C.8 – Properties for systematic safety integrity – Software modification .....	83
Table C.9 – Properties for systematic safety integrity – Software verification .....	85
Table C.10 – Properties for systematic safety integrity – Functional safety assessment .....	86
Table C.11 – Detailed properties – Design and coding standards .....	87
Table C.12 – Detailed properties – Dynamic analysis and testing .....	89
Table C.13 – Detailed properties – Functional and black-box testing .....	90
Table C.14 – Detailed properties – Failure analysis .....	91
Table C.15 – Detailed properties – Modelling .....	92
Table C.16 – Detailed properties – Performance testing .....	93
Table C.17 – Detailed properties – Semi-formal methods .....	94
Table C.18 – Properties for systematic safety integrity – Static analysis .....	95
Table C.19 – Detailed properties – Modular approach .....	96
Table E.1 – Categories of IEC 61508-2 requirements .....	100
Table E.2 – Requirements of IEC 61508-2 for software and their typical relevance to certain types of software .....	100
Table F.1 – Module coupling – definition of terms .....	104
Table F.2 – Types of module coupling .....	105

This document is a preview generated by EVS



## 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.

NOTE 1 Examples of product and application sector international standards based on the IEC 61508 series are given in the bibliography (see references [1], [2] and [3]).

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  $10^{-9}$  [ $\text{h}^{-1}$ ];

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.

This document is a preview generated by EVS

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

## Part 3: Software requirements

### 1 Scope

1.1 This part of the IEC 61508 series

- a) is intended to be utilized only after a thorough understanding of IEC 61508-1 and IEC 61508-2;
- b) applies to any software forming part of a safety-related system or used to develop a safety-related system within the scope of IEC 61508-1 and IEC 61508-2. Such software is termed safety-related software (including operating systems, system software, software in communication networks, human-computer interface functions, and firmware as well as application software);
- c) provides specific requirements applicable to support tools used to develop and configure a safety-related system within the scope of IEC 61508-1 and IEC 61508-2;
- d) requires that the software safety functions and software systematic capability are specified;

NOTE 1 If this has already been done as part of the specification of the E/E/PE safety-related systems (see 7.2 of IEC 61508-2), then it does not have to be repeated in this part.

NOTE 2 Specifying the software safety functions and software systematic capability is an iterative procedure; see Figures 3 and 6.

NOTE 3 See Clause 5 and Annex A of IEC 61508-1 for documentation structure. The documentation structure may take account of company procedures, and of the working practices of specific application sectors.

NOTE 4 Note: See 3.5.9 of IEC 61508-4 for definition of the term "systematic capability".

- e) establishes requirements for safety lifecycle phases and activities which shall be applied during the design and development of the safety-related software (the software safety lifecycle model). These requirements include the application of measures and techniques, which are graded against the required systematic capability, for the avoidance of and control of faults and failures in the software;
- f) provides requirements for information relating to the software aspects of system safety validation to be passed to the organisation carrying out the E/E/PE system integration;
- g) provides requirements for the preparation of information and procedures concerning software needed by the user for the operation and maintenance of the E/E/PE safety-related system;
- h) provides requirements to be met by the organisation carrying out modifications to safety-related software;
- i) provides, in conjunction with IEC 61508-1 and IEC 61508-2, requirements for support tools such as development and design tools, language translators, testing and debugging tools, configuration management tools;

NOTE 4 Figure 5 shows the relationship between IEC 61508-2 and IEC 61508-3.

- j) Does not apply for medical equipment in compliance with the IEC 60601 series.

1.2 IEC 61508-1, IEC 61598-2, 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 61508-3 plays in the achievement of functional safety for E/E/PE safety-related systems.

This document is a preview generated by EVS

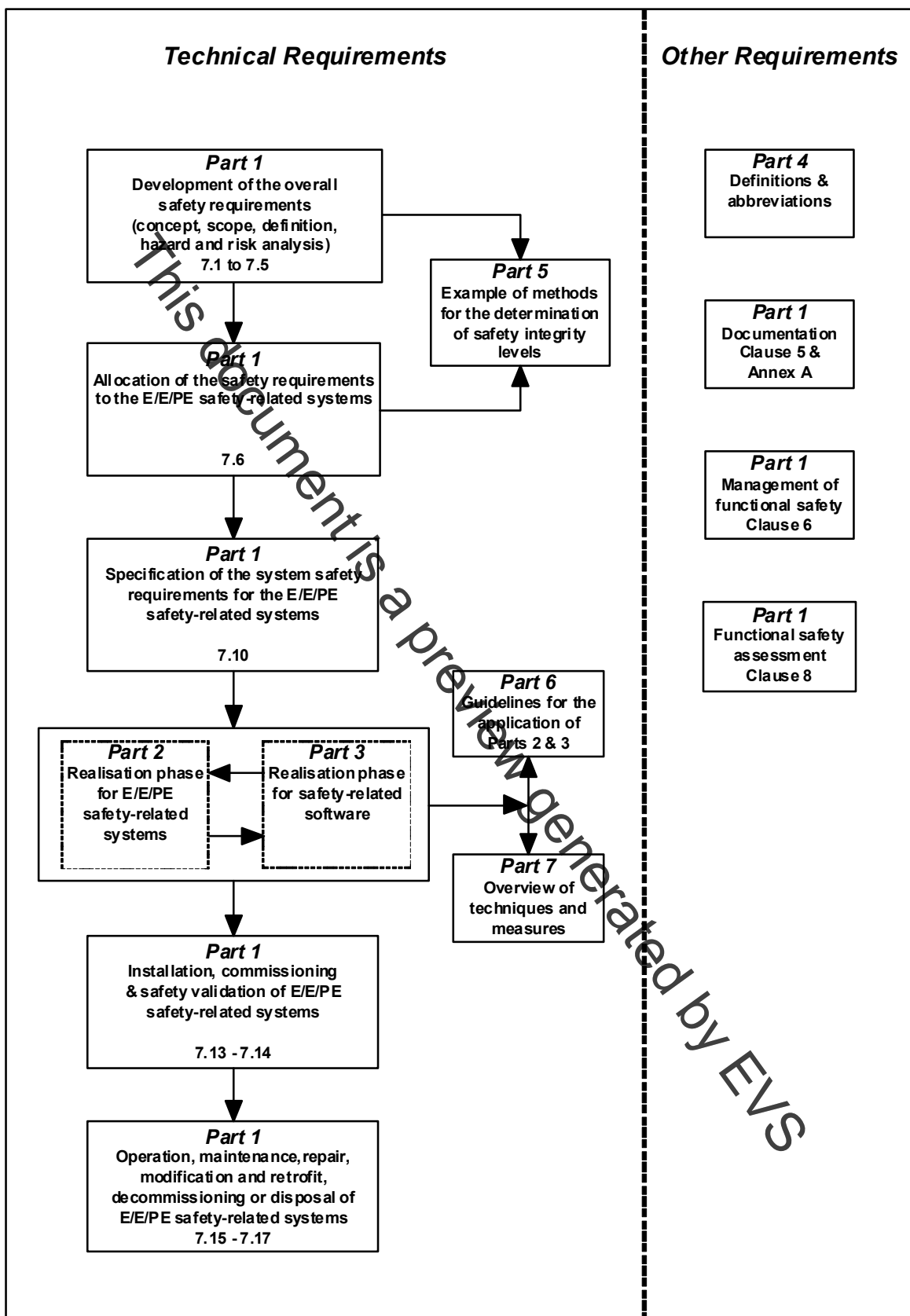


Figure 1 – Overall framework of the IEC 61508 series

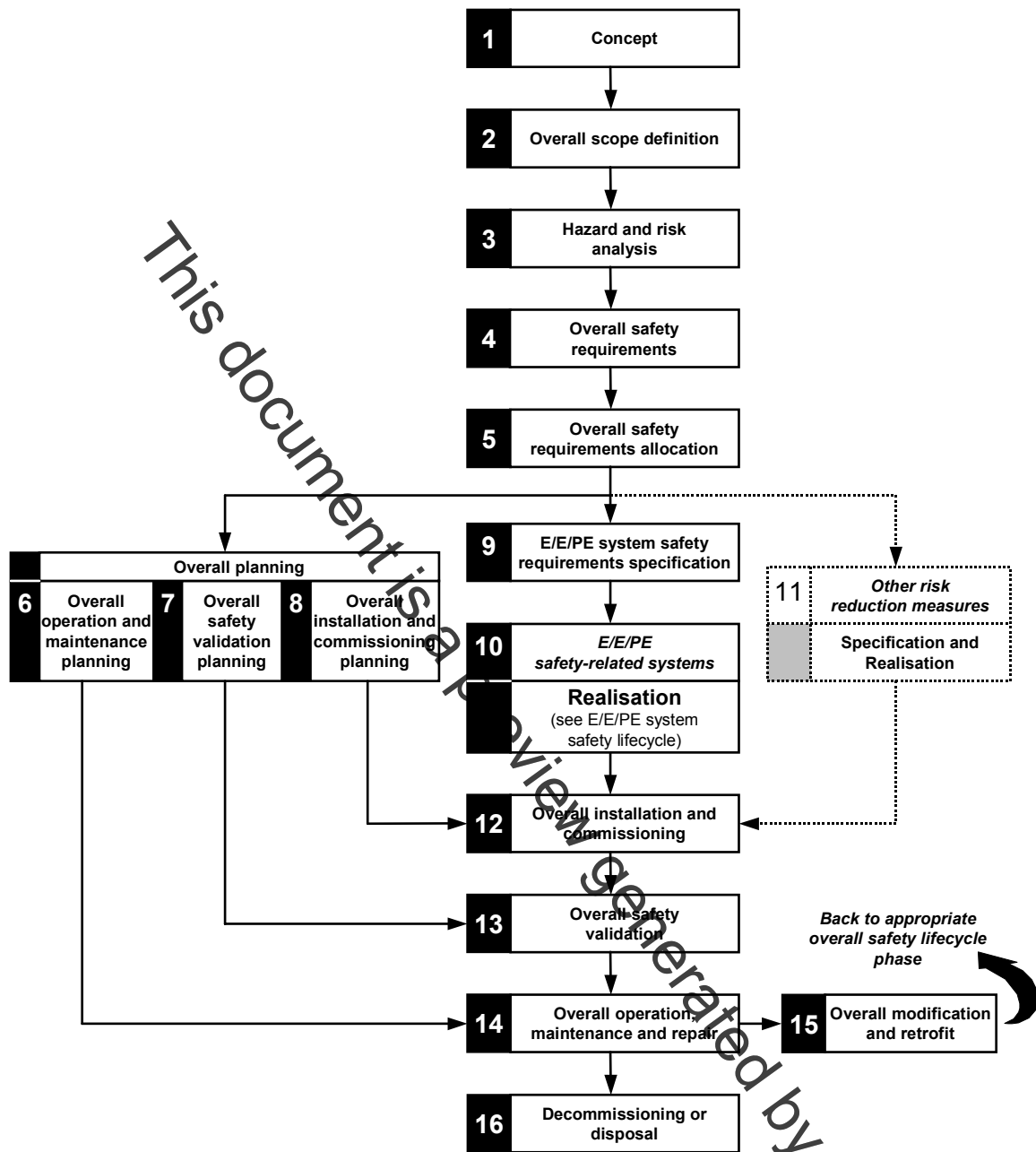


Figure 2 – Overall safety lifecycle

## 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 61508-1: 2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General requirements*

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

IEC Guide 104:1997, *The preparation of safety publications and the use of basic safety publications and group safety publications*

IEC/ISO Guide 51:1999, *Safety aspects – Guidelines for their inclusion in standards*

### **3 Definitions and abbreviations**

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

### **4 Conformance to this standard**

The requirements for conformance to this standard are given in Clause 4 of IEC 61508-1.

### **5 Documentation**

The objectives and requirements for documentation are given in Clause 5 of IEC 61508-1.

### **6 Additional requirements for management of safety-related software**

#### **6.1 Objectives**

The objectives are as detailed in 6.1 of IEC 61508-1.

#### **6.2 Requirements**

**6.2.1** The requirements are as detailed in 6.2 of IEC 61508-1 with the following additional requirements.

**6.2.2** The functional safety planning shall define the strategy for software procurement, development, integration, verification, validation and modification to the extent required by the safety integrity level of the safety functions implemented by the E/E/PE safety-related system.

NOTE The philosophy of this approach is to use the functional safety planning as an opportunity to customize this standard to take account of the required safety integrity for each safety function implemented by the E/E/PE safety-related system.

**6.2.3** Software configuration management shall:

- a) apply administrative and technical controls throughout the software safety lifecycle, in order to manage software changes and thus ensure that the specified requirements for safety-related software continue to be satisfied;
- b) guarantee that all necessary operations have been carried out to demonstrate that the required software systematic capability has been achieved;
- c) maintain accurately and with unique identification all configuration items which are necessary to meet the safety integrity requirements of the E/E/PE safety-related system. Configuration items include at least the following: safety analysis and requirements; software specification and design documents; software source code modules; test plans