IEC 61508-3

Edition 2.0 2010-04

INTERNATIONAL STANDARD

NORME INTERNATIONALE

BASIC SAFETY PUBLICATION

PUBLICATION FONDAMENTALE DE SÉCURITÉ

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

Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 3: Exigences concernant les logiciels

INTERNATIONAL ELECTROTECHNICAL COMMISSION

COMMISSION ELECTROTECHNIQUE INTERNATIONALE

PRICE CODE CODE PRIX XE

ICS 25.040.40

ISBN 978-2-88910-526-7

® Registered trademark of the International Electrotechnical Commission
Marque déposée de la Commission Electrotechnique Internationale

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

INTERNATIONAL ELECTROTECHNICAL COMMISSION

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

Part 3: Software requirements

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
6) All users should ensure that they have the latest edition of this publication.
7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

International Standard IEC 61508-3 has been prepared by subcommittee 65A: System aspects, of IEC technical committee 65: Industrial-process measurement, control and automation.

This second edition cancels and replaces the first edition published in 1998. This edition constitutes a technical revision.

This edition has been subject to a thorough review and incorporates many comments received at the various revision stages.

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

The text of this standard is based on the following documents:

FDIS	Report on voting
65A/550/FDIS	65A/574/RVD

Full information on the voting for the approval of this standard can be found in the report on voting indicated in the above table.

This publication has been drafted in accordance with the ISO/IEC Directives, Part 2.

A list of all parts of the IEC 61508 series, published under the general title *Functional safety of electrical / electronic / programmable electronic safety-related systems*, can be found on the IEC website.

The committee has decided that the contents of this publication will remain unchanged until the stability date indicated on the IEC web site under "http://webstore.iec.ch" in the data related to the specific publication. At this date, the publication will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

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} [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 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.

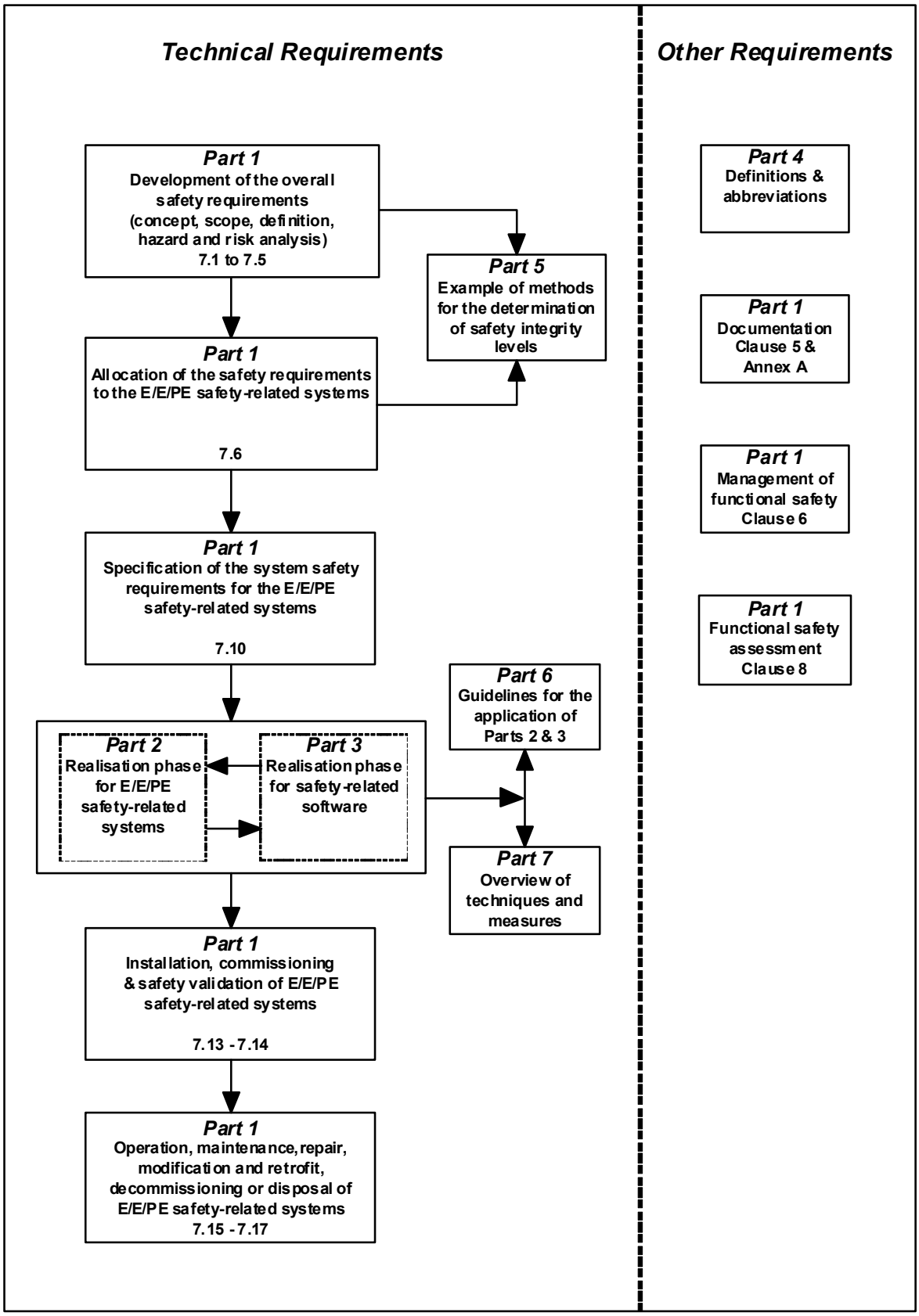


Figure 1 – Overall framework of the IEC 61508 series

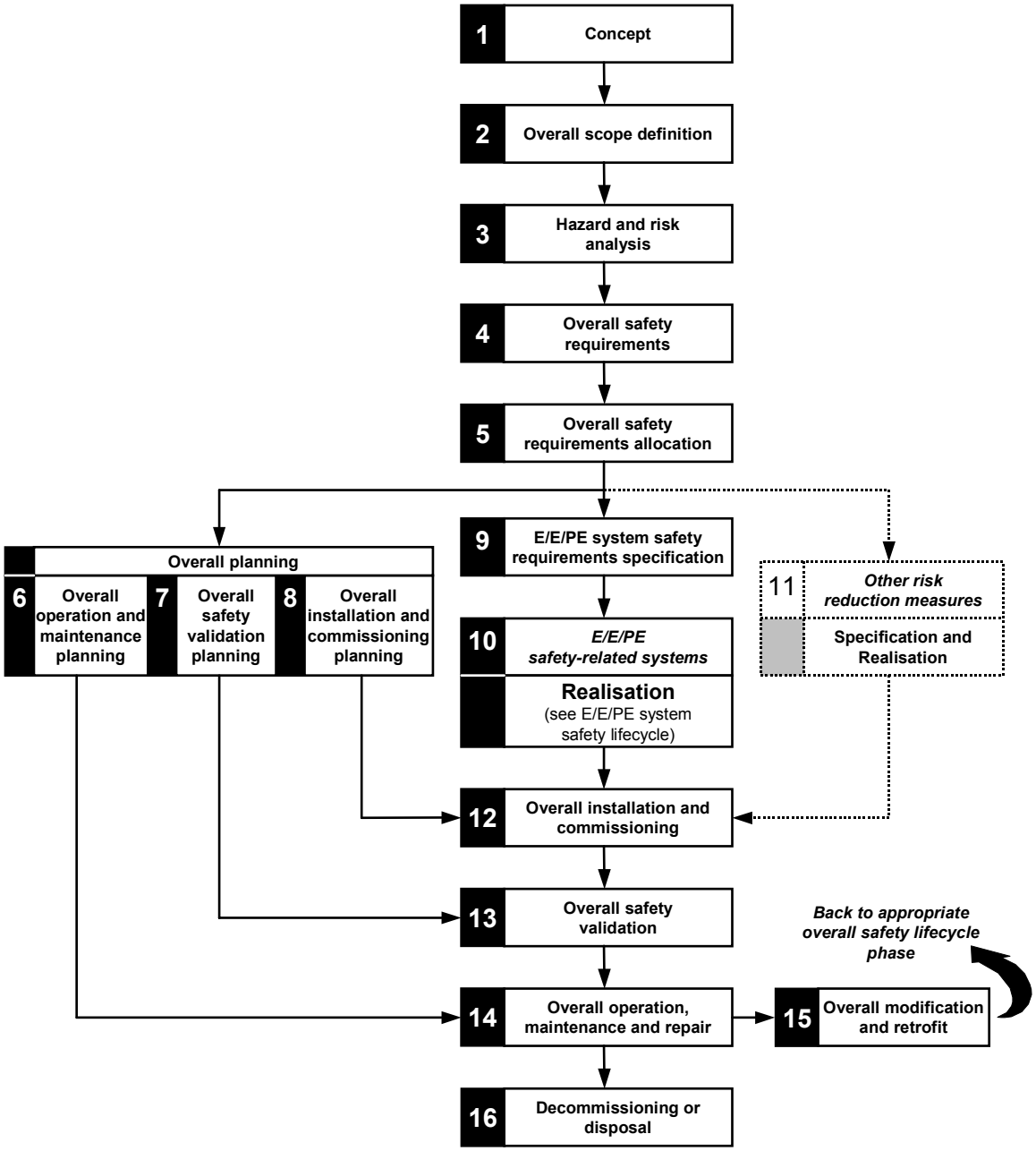


Figure 2 – Overall safety lifecycle

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*

SOMMAIRE

AVANT-PROPOS 115
INTRODUCTION 117
1 Domaine d'application 119
2 Références normatives 122
3 Définitions et abréviations 123
4 Conformité à la présente norme 123
5 Documentation 123
6 Exigences supplémentaires pour la gestion du logiciel de sécurité 123
6.1 Objectifs 123
6.2 Exigences 123
7 Exigences concernant le cycle de vie de sécurité du logiciel 124
7.1 Généralités 124
7.1.1 Objectif 124
7.1.2 Exigences 125
7.2 Spécification des exigences pour la sécurité du logiciel 133
7.2.1 Objectifs 133
7.2.2 Exigences 133
7.3 Planification de la validation de sécurité du logiciel 136
7.3.1 Objectif 136
7.3.2 Exigences 136
7.4 Conception et développement du logiciel 137
7.4.1 Objectifs 137
7.4.2 Exigences générales 138
7.4.3 Exigences concernant la conception de l'architecture du logiciel 142
7.4.4 Exigences concernant les outils de support, y compris les langages de programmation 143
7.4.5 Exigences concernant la conception détaillée et le développement – conception du système logiciel 146
7.4.6 Exigences concernant le codage 147
7.4.7 Exigences concernant l'essai des modules logiciels 148
7.4.8 Exigences concernant l'essai d'intégration du logiciel 148
7.5 Intégration de l'électronique programmable (matériel et logiciel) 149
7.5.1 Objectifs 149
7.5.2 Exigences 149
7.6 Procédures d'exploitation et de modification du logiciel 150
7.6.1 Objectif 150
7.6.2 Exigences 150
7.7 Validation de sécurité du logiciel 151
7.7.1 Objectif 151
7.7.2 Exigences 151
7.8 Modification du logiciel 152
7.8.1 Objectif 152
7.8.2 Exigences 152
7.9 Vérification du logiciel 154
7.9.1 Objectif 154
7.9.2 Exigences 154

8 Evaluation de la sécurité fonctionnelle 158
Annexe A (normative) Guide de sélection de techniques et mesures 159
Annexe B (informative) Tableaux détaillés 168
Annexe C (informative) Propriétés relatives à la capabilité systématique du logiciel 173
Annexe D (normative) Manuel de sécurité d'article conforme – exigences supplémentaires pour les composants logiciels 218
Annexe E (informative) Relation entre la CEI 61508-2 et la CEI 61508-3 221
Annexe F (informative) Techniques de réalisation de non interférence entre les composants logiciels d'un seul ordinateur 223
Annexe G (informative) Indications relatives à la personnalisation des cycles de vie associés aux systèmes dirigés par les données 228
Bibliographie 232

Figure 1 – Structure générale de la série CEI 61508 121
Figure 2 – Cycle de vie de sécurité global 122
Figure 3 – Cycle de vie de sécurité du système E/E/PE (en phase de réalisation) 127
Figure 4 – Cycle de vie de sécurité du logiciel (en phase de réalisation) 127
Figure 5 – Relation et domaine d'application pour la CEI 61508-2 et la CEI 61508-3 128
Figure 6 – Capabilité systématique du logiciel et cycle de vie de développement (modèle en V) 128
Figure G.1 – Variabilité de complexité des systèmes dirigés par les données 229

Tableau 1 – Cycle de vie de sécurité du logiciel – présentation 129
Tableau A.1 – Spécification des exigences pour la sécurité du logiciel 160
Tableau A.2 – Conception et développement du logiciel – conception de l'architecture du logiciel 160
Tableau A.3 – Conception et développement du logiciel – outils de support et langage de programmation 162
Tableau A.4 – Conception et développement du logiciel – conception détaillée 162
Tableau A.5 – Conception et développement du logiciel – essai et intégration des modules logiciels 163
Tableau A.6 – Intégration de l'électronique programmable (matériel et logiciel) 164
Tableau A.7 – Validation de sécurité du logiciel 164
Tableau A.8 – Modification 165
Tableau A.9 – Vérification du logiciel 166
Tableau A.10 – Evaluation de la sécurité fonctionnelle 167
Tableau B.1 – Règles de conception et de codage 168
Tableau B.2 – Analyse dynamique et essai 169
Tableau B.3 – Essais fonctionnels et boîte noire 169
Tableau B.4 – Analyse de défaillance 170
Tableau B.5 – Modélisation 170
Tableau B.6 – Essais de fonctionnement 171
Tableau B.7 – Méthodes semi-formelles 171
Tableau B.8 – Analyse statique 172
Tableau B.9 – Approche modulaire 172

Tableau C.1 – Propriétés relatives à l'intégrité systématique – Spécification des exigences pour la sécurité du logiciel 178
Tableau C.2 – Propriétés relatives à l'intégrité systématique – Conception et développement du logiciel – Conception de l'architecture logicielle 181
Tableau C.3 – Propriétés relatives à l'intégrité systématique - Conception et développement du logiciel – outils de support et langage de programmation 192
Tableau C.4 – Propriétés relatives à l'intégrité systématique – Conception et développement du logiciel – conception détaillée (comprend la conception du système logiciel, la conception des modules logiciels et le codage) 193
Tableau C.5 – Propriétés relatives à l'intégrité systématique – Conception et développement du logiciel – essai et intégration des modules logiciels 196
Tableau C.6 – Propriétés relatives à l'intégrité systématique – Intégration de l'électronique programmable (matériel et logiciel) 198
Tableau C.7 – Propriétés relatives à l'intégrité systématique – Validation de sécurité du logiciel 199
Tableau C.8 – Propriétés relatives à l'intégrité systématique – Modification du logiciel 200
Tableau C.9 – Propriétés relatives à l'intégrité systématique – Vérification du logiciel 202
Tableau C.10 – Propriétés relatives à l'intégrité systématique – Évaluation de la sécurité fonctionnelle 203
Tableau C.11 – Propriétés détaillées – Conception et règles de codage 205
Tableau C.12 – Propriétés détaillées – Analyse dynamique et essais 207
Tableau C.13 – Propriétés détaillées – Essais fonctionnels et boîte noire 209
Tableau C.14 – Propriétés détaillées – Analyse des défaillances 211
Tableau C.15 – Propriétés détaillées – Modélisation 212
Tableau C.16 – Propriétés détaillées – Essais de fonctionnement 213
Tableau C.17 – Propriétés détaillées – Méthodes semi-formelles 214
Tableau C.18 – Propriétés relatives à l'intégrité systématique – Analyse statique 215
Tableau C.19 – Propriétés détaillées – Approche modulaire 217
Tableau E.1 – Catégories des exigences de la CEI 61508-2 221
Tableau E.2 – Exigences de la CEI 61508-2 pour le logiciel et leur pertinence typique pour certains types de logiciels 221
Tableau F.1 – Couplage de modules – définition des termes 225
Tableau F.2 – Types de couplage de modules 226

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

SÉCURITÉ FONCTIONNELLE DES SYSTÈMES ÉLECTRIQUES/ÉLECTRONIQUES/ÉLECTRONIQUES PROGRAMMABLES RELATIFS À LA SÉCURITÉ –

Partie 3: Exigences concernant les logiciels

AVANT-PROPOS

1) La Commission Electrotechnique Internationale (CEI) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de la CEI). La CEI a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. A cet effet, la CEI – entre autres activités – publie des Normes internationales, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés "Publication(s) de la CEI"). Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec la CEI, participent également aux travaux. La CEI collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.
2) Les décisions ou accords officiels de la CEI concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de la CEI intéressés sont représentés dans chaque comité d'études.
3) Les Publications de la CEI se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de la CEI. Tous les efforts raisonnables sont entrepris afin que la CEI s'assure de l'exactitude du contenu technique de ses publications; la CEI ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.
4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de la CEI s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de la CEI dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de la CEI et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
5) La CEI elle-même ne fournit aucune attestation de conformité. Des organismes de certification indépendants fournissent des services d'évaluation de conformité et, dans certains secteurs, accèdent aux marques de conformité de la CEI. La CEI n'est responsable d'aucun des services effectués par les organismes de certification indépendants.
6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.
7) Aucune responsabilité ne doit être imputée à la CEI, à ses administrateurs, employés, auxiliaires ou mandataires, y compris ses experts particuliers et les membres de ses comités d'études et des Comités nationaux de la CEI, pour tout préjudice causé en cas de dommages corporels et matériels, ou de tout autre dommage de quelque nature que ce soit, directe ou indirecte, ou pour supporter les coûts (y compris les frais de justice) et les dépenses découlant de la publication ou de l'utilisation de cette Publication de la CEI ou de toute autre Publication de la CEI, ou au crédit qui lui est accordé.
8) L'attention est attirée sur les références normatives citées dans cette publication. L'utilisation de publications référencées est obligatoire pour une application correcte de la présente publication.
9) L'attention est attirée sur le fait que certains des éléments de la présente Publication de la CEI peuvent faire l'objet de droits de propriété intellectuelle ou de droits analogues. La CEI ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de propriété et de ne pas avoir signalé leur existence.

La norme internationale CEI 61508-3 a été établie par le sous-comité 65A: Aspects systèmes, du comité d'études 65 de la CEI: Mesure, commande et automation dans les processus industriels.

Cette deuxième édition annule et remplace la première édition publiée en 1998 dont elle constitue une révision technique.

La présente édition a fait l'objet d'une révision approfondie et intègre de nombreux commentaires reçus lors des différentes phases de révision.

Elle a le statut de publication de sécurité de base conformément au Guide CEI 104.

Le texte de cette norme est issu des documents suivants:

FDIS	Rapport de vote
65A/550/FDIS	65A/574/RVD

Le rapport de vote indiqué dans le tableau ci-dessus donne toute information sur le vote ayant abouti à l'approbation de cette norme.

Cette publication a été rédigée selon les Directives ISO/CEI, Partie 2.

Une liste de toutes les parties de la série CEI 61508, présentées sous le titre général *Sécurité fonctionnelle des systèmes électriques / électroniques / électroniques programmables relatifs à la sécurité*, peut être consultée sur le site web de la CEI.

Le comité a décidé que le contenu de cette publication ne sera pas modifié avant la date de stabilité indiquée sur le site web de la CEI sous "http://webstore.iec.ch" dans les données relatives à la publication recherchée. A cette date, la publication sera

- reconduite,
- supprimée,
- remplacée par une édition révisée, ou
- amendée.

INTRODUCTION

Les systèmes comprenant des composants électriques et/ou électroniques sont utilisés depuis de nombreuses années pour exécuter des fonctions relatives à la sécurité dans la plupart des secteurs d'application. Des systèmes à base d'informatique (dénommés de manière générique systèmes électroniques programmables) sont utilisés dans tous les secteurs d'application pour exécuter des fonctions non relatives à la sécurité, mais aussi de plus en plus souvent relatives à la sécurité. Si l'on veut exploiter efficacement et en toute sécurité la technologie des systèmes informatiques, il est indispensable de fournir à tous les responsables suffisamment d'éléments relatifs à la sécurité pour les guider dans leurs prises de décisions.

La présente Norme internationale présente une approche générique de toutes les activités liées au cycle de vie de sécurité de systèmes électriques et/ou électroniques et/ou électroniques programmables (E/E/PE) qui sont utilisés pour réaliser des fonctions de sécurité. Cette approche unifiée a été adoptée afin de développer une politique technique rationnelle et cohérente concernant tous les systèmes électriques relatifs à la sécurité. Un objectif principal de cette approche est de faciliter le développement de normes internationales de produit et d'application sectorielle basées sur la série CEI 61508.

NOTE 1 Des exemples de normes internationales de produit et d'application sectorielle basées sur la série CEI 61508 sont donnés dans la Bibliographie (voir références [1], [2] et [3]).

Dans la plupart des cas, la sécurité est obtenue par un certain nombre de systèmes fondés sur diverses technologies (par exemple mécanique, hydraulique, pneumatique, électrique, électronique, électronique programmable). En conséquence, toute stratégie de sécurité doit non seulement prendre en compte tous les éléments d'un système individuel (par exemple, les capteurs, les appareils de commande et les actionneurs), mais également prendre en considération tous les systèmes relatifs à la sécurité comme des éléments individuels d'un ensemble complexe. Par conséquent, la présente Norme internationale, bien que traitant des systèmes E/E/PE relatifs à la sécurité, peut aussi fournir un cadre de sécurité susceptible de concerner les systèmes relatifs à la sécurité basés sur d'autres technologies.

Il est admis qu'il existe une grande variété d'applications utilisant des systèmes E/E/PE relatifs à la sécurité dans un grand nombre de secteurs, et couvrant un large éventail de complexité et de potentiel de dangers et de risques. Pour chaque application particulière, les mesures de sécurité requises dépendent de nombreux facteurs propres à l'application. La présente Norme internationale, de par son caractère général, rend désormais possible la prescription de ces mesures dans les futures normes internationales de produit et d'application sectorielle, ainsi que dans les révisions des normes déjà existantes.

La présente Norme internationale

– concerne toutes les phases appropriées du cycle de vie de sécurité global des systèmes E/E/PE et du logiciel (par exemple, depuis le concept initial, en passant par la conception, l'installation, l'exploitation et la maintenance, jusqu'à la mise hors service) lorsque les systèmes E/E/PE permettent d'exécuter des fonctions de sécurité,
– a été élaborée dans le souci de la prise en compte de l'évolution rapide des technologies; le cadre fourni par la présente Norme internationale est suffisamment solide et étendu pour pourvoir aux évolutions futures,
– permet l'élaboration de normes internationales de produit et d'application sectorielle concernant les systèmes E/E/PE relatifs à la sécurité; il convient que l'élaboration de normes internationales de produit et d'application sectorielle dans le cadre de la présente norme, permette d'atteindre un haut niveau de cohérence (par exemple, pour ce qui est des principes sous-jacents, de la terminologie, etc.) à la fois au sein de chaque secteur d'application, et d'un secteur à l'autre. La conséquence en sera une amélioration en termes de sécurité et de gains économiques,
– fournit une méthode de définition d'une spécification des exigences de sécurité nécessaire pour obtenir la sécurité fonctionnelle requise des systèmes E/E/PE relatifs à la sécurité,

– adopte une approche basée sur les risques qui permet de déterminer les exigences en matière d'intégrité de sécurité,

– introduit les niveaux d'intégrité de sécurité pour la spécification du niveau cible d'intégrité de sécurité des fonctions de sécurité devant être réalisées par les systèmes E/E/PE relatifs à la sécurité,

NOTE 2 La norme ne spécifie aucune exigence de niveau d'intégrité de sécurité pour aucune fonction de sécurité, ni comment le niveau d'intégrité de sécurité est déterminé. Elle fournit en revanche un cadre conceptuel basé sur les risques, ainsi que des exemples de méthodes.

– fixe des objectifs chiffrés de défaillance pour les fonctions de sécurité exécutées par les systèmes E/E/PE relatifs à la sécurité, qui sont en rapport avec les niveaux d'intégrité de sécurité,

– fixe une limite inférieure pour les objectifs chiffrés de défaillance pour une fonction de sécurité exécutée par un système E/E/PE relatif à la sécurité unique. Pour des systèmes E/E/PE relatifs à la sécurité fonctionnant

  – en mode de fonctionnement à faible sollicitation, la limite inférieure est fixée pour une probabilité moyenne de défaillance dangereuse de 10^{-5} en cas de sollicitation,

  – en mode de fonctionnement continu ou à sollicitation élevée, la limite inférieure est fixée à une fréquence moyenne de défaillance dangereuse de 10^{-9} [h^{-1}],

NOTE 3 Un système E/E/PE relatif à la sécurité unique n'implique pas nécessairement une architecture à un seul canal.

NOTE 4 Dans le cas de systèmes non complexes, il peut être possible de concevoir des systèmes relatifs à la sécurité ayant des valeurs plus basses pour l'intégrité de sécurité cible. Il est toutefois considéré que ces limites représentent ce qui peut être réalisé à l'heure actuelle pour des systèmes relativement complexes (par exemple, des systèmes électroniques programmables relatifs à la sécurité).

– établit des exigences fondées sur l'expérience et le jugement acquis dans le domaine des applications industrielles afin d'éviter des anomalies systématiques ou pour les maintenir sous contrôle. Même si, en général, la probabilité d'occurrence des défaillances systématiques ne peut être quantifiée, la norme permet cependant pour une fonction de sécurité spécifique, de déclarer que l'objectif chiffré de défaillance associé à cette fonction de sécurité peut être réputé atteint si toutes les exigences de la norme sont remplies,

– introduit une capabilité systématique s'appliquant à un élément du fait qu'il permet d'assurer que l'intégrité de sécurité systématique satisfait aux exigences du niveau d'intégrité de sécurité spécifié,

– adopte une large gamme de principes, techniques et mesures pour la réalisation de la sécurité fonctionnelle des systèmes E/E/PE relatifs à la sécurité, mais n'utilise pas de manière explicite le concept de sécurité intrinsèque. Les principes de « sécurité intrinsèque » peuvent toutefois être applicables, l'adoption de ces concepts étant par ailleurs acceptable sous réserve de la satisfaction aux exigences des articles concernés de la norme.

SÉCURITÉ FONCTIONNELLE DES SYSTÈMES ÉLECTRIQUES/ÉLECTRONIQUES/ÉLECTRONIQUES PROGRAMMABLES RELATIFS À LA SÉCURITÉ –

Partie 3: Exigences concernant les logiciels

1 Domaine d'application

1.1 La présente partie de la série CEI 61508

a) est destinée à n'être utilisée qu'après s'être assuré d'une compréhension parfaite de la CEI 61508-1 et de la CEI 61508-2;

b) s'applique à tout logiciel faisant partie intégrante d'un système relatif à la sécurité ou utilisé pour développer un système relatif à la sécurité entrant dans le domaine d'application de la CEI 61508-1 et de la CEI 61508-2. Ce type de logiciel est désigné par le terme "logiciel de sécurité" (comprenant les systèmes d'exploitation, les logiciels système, les logiciels des réseaux de communication, les fonctions d'interface homme-machine et les micrologiciels, ainsi que les logiciels d'application);

c) fournit des exigences spécifiques applicables aux outils de support utilisés pour développer et configurer un système relatif à la sécurité dans le cadre du domaine d'application de la CEI 61508-1 et de la CEI 61508-2;

d) nécessite que les fonctions de sécurité du logiciel et la capabilité systématique du logiciel soient précisées;

NOTE 1 Si cela a déjà été réalisé dans le cadre de la spécification des systèmes E/E/PE relatifs à la sécurité (voir 7.2 de la CEI 61508-2), il n'est alors pas nécessaire de le répéter dans la présente partie.

NOTE 2 Spécifier les fonctions de sécurité du logiciel et la capabilité systématique du logiciel constitue une procédure itérative; voir les Figures 3 et 6.

NOTE 3 Voir l'Article 5 et l'Annexe A de la CEI 61508-1 pour la structure de la documentation. Cette structure peut tenir compte des procédures de l'entreprise et des pratiques professionnelles de secteurs d'application spécifiques.

e) établit des exigences concernant les phases et activités du cycle de vie de sécurité qui doivent être appliquées durant la conception et le développement du logiciel de sécurité (modèle de cycle de vie de sécurité du logiciel). Ces exigences comprennent l'application de mesures et de techniques qui suivent une gradation basée sur la capabilité systématique requise, afin d'éviter et de maîtriser les anomalies et défaillances du logiciel;

f) fournit les exigences pour les informations relatives aux aspects du logiciel applicables à la validation de la sécurité du système et devant être transmises à l'organisation en charge de l'intégration du système E/E/PE;

g) fournit les exigences pour la préparation des informations et procédures concernant le logiciel requises par l'utilisateur pour le fonctionnement et la maintenance d'un système E/E/PE relatif à la sécurité;

h) fournit les exigences devant être observées par l'organisation en charge des modifications du logiciel de sécurité;

i) fournit, en accord avec la CEI 61508-1 et la CEI 61508-2, les exigences pour les outils de support tels que les outils de conception et développement, les traducteurs de langage, les outils d'essai et de mise au point et les outils de gestion de configuration;

NOTE 4 La Figure 5 montre la relation entre la CEI 61508-2 et la CEI 61508-3.

j) ne s'applique pas aux appareils médicaux conformes à la série CEI 60601.

1.2 Les CEI 61508-1, CEI 61508-2, CEI 61508-3 et CEI 61508-4 sont des publications fondamentales de sécurité, bien que ce statut ne soit pas applicable dans le contexte des

systèmes E/E/PE de faible complexité relatifs à la sécurité (voir 3.4.3 de la CEI 61508-4). En tant que publications fondamentales de sécurité, ces normes sont destinées à être utilisées par les comités d'études pour la préparation des normes conformément aux principes contenus dans le Guide CEI 104 et le Guide ISO/CEI 51. Les CEI 61508-1, CEI 61508-2, CEI 61508-3 et CEI 61508-4 sont également destinées à être utilisées comme publications autonomes. La fonction de sécurité horizontale de la présente norme internationale ne s'applique pas aux appareils médicaux conformes à la série CEI 60601.

1.3 Une des responsabilités incombant à un comité d'études consiste, dans toute la mesure du possible, à utiliser les publications fondamentales de sécurité pour la préparation de ses publications. Dans ce contexte, les exigences, les méthodes ou les conditions d'essai de cette publication fondamentale de sécurité ne s'appliquent que si elles sont indiquées spécifiquement ou incluses dans les publications préparées par ces comités d'études.

1.4 La Figure 1 illustre la structure générale de la série CEI 61508 et montre le rôle que la CEI 61508-3 joue dans la réalisation de la sécurité fonctionnelle pour les systèmes E/E/PE relatifs à la sécurité.

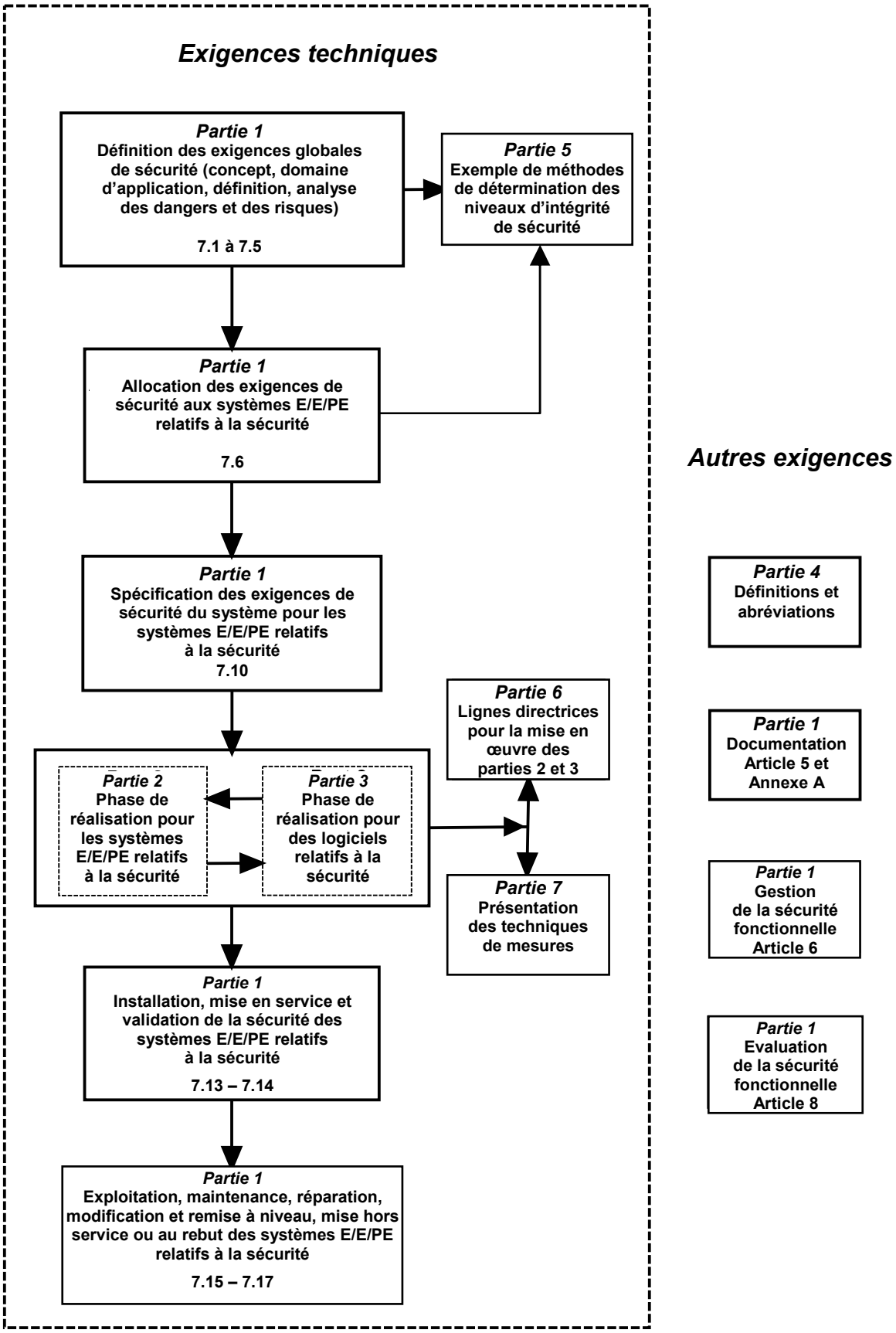


Figure 1 – Structure générale de la série CEI 61508

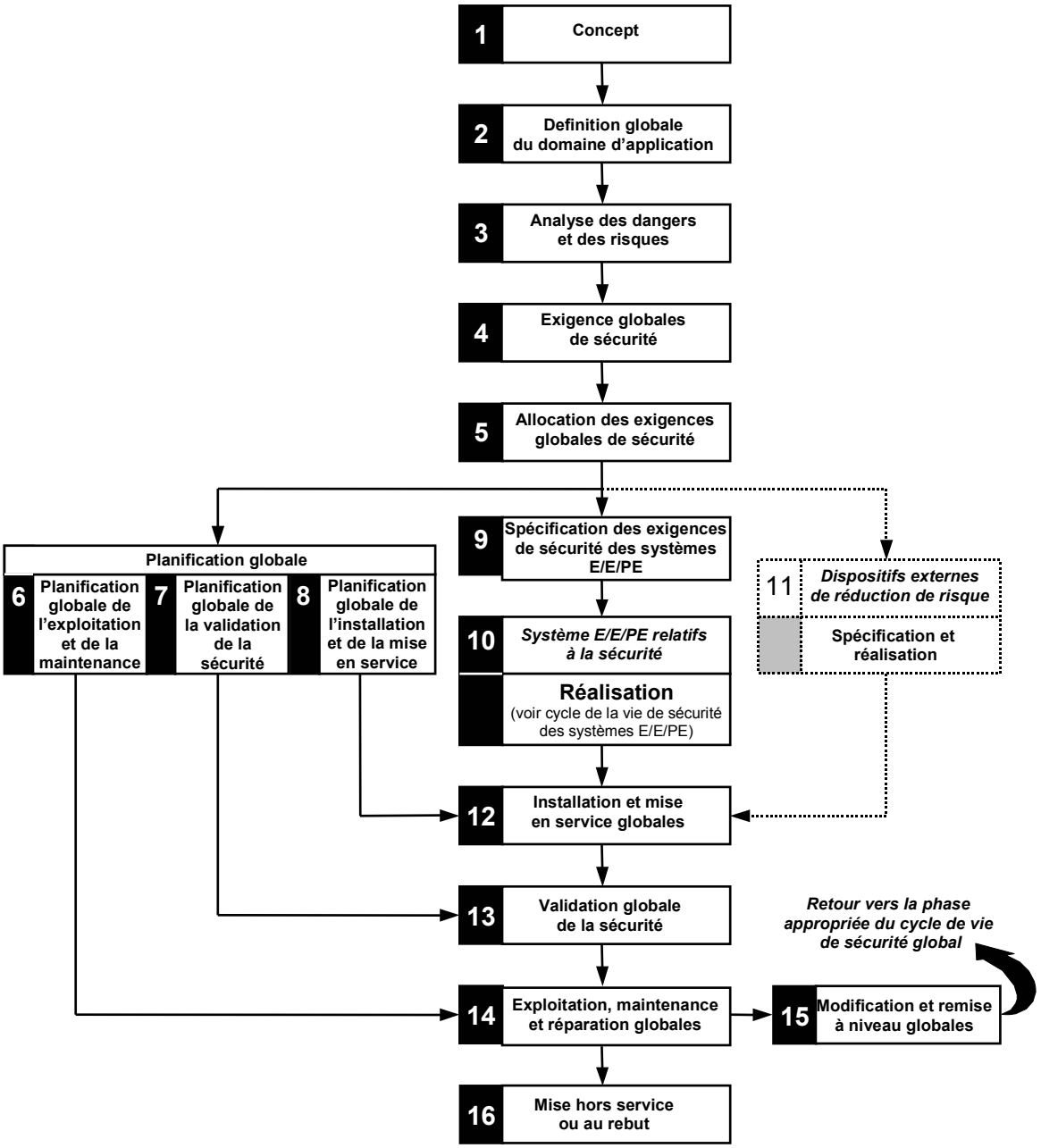


Figure 2 – Cycle de vie de sécurité global

2 Références normatives

Les documents de référence suivants sont indispensables pour l'application du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

CEI 61508-1: 2010, *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 1: Exigences générales*

CEI 61508-2: 2010, *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 2: Exigences concernant les systèmes électriques/ électroniques/électroniques programmables relatifs à la sécurité*

CEI 61508-4: 2010, *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 4: Définitions et abréviations*

Guide CEI 104:1997, *Elaboration des publications de sécurité et utilisation des publications fondamentales de sécurité et publications groupées de sécurité*

Guide ISO/CEI 51:1999, *Aspects liés à la sécurité – Principes directeurs pour les inclure dans les normes*