IEC 61508-1

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 1: General requirements

Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 1: Exigences générales

INTERNATIONAL ELECTROTECHNICAL COMMISSION

COMMISSION ELECTROTECHNIQUE INTERNATIONALE

PRICE CODE XB
CODE PRIX

ICS 13.110; 25.040; 29.020

ISBN 978-2-88910-524-3

® 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 12
4 Conformance to this standard 12
5 Documentation 13
5.1 Objectives 13
5.2 Requirements 13
6 Management of functional safety 14
6.1 Objectives 14
6.2 Requirements 14
7 Overall safety lifecycle requirements 17
7.1 General 17
7.1.1 Introduction 17
7.1.2 Objectives and requirements – general 20
7.1.3 Objectives 25
7.1.4 Requirements 25
7.2 Concept 25
7.2.1 Objective 25
7.2.2 Requirements 26
7.3 Overall scope definition 26
7.3.1 Objectives 26
7.3.2 Requirements 26
7.4 Hazard and risk analysis 27
7.4.1 Objectives 27
7.4.2 Requirements 27
7.5 Overall safety requirements 28
7.5.1 Objective 29
7.5.2 Requirements 29
7.6 Overall safety requirements allocation 30
7.6.1 Objectives 30
7.6.2 Requirements 31
7.7 Overall operation and maintenance planning 35
7.7.1 Objective 35
7.7.2 Requirements 35
7.8 Overall safety validation planning 37
7.8.1 Objective 37
7.8.2 Requirements 37
7.9 Overall installation and commissioning planning 38
7.9.1 Objectives 38
7.9.2 Requirements 38
7.10 E/E/PE system safety requirements specification 38
7.10.1 Objective 39
7.10.2 Requirements 39
7.11 E/E/PE safety-related systems – realisation 41

7.11.1 Objective 41
7.11.2 Requirements 41
7.12 Other risk reduction measures – specification and realisation 41
7.12.1 Objective 41
7.12.2 Requirements 41
7.13 Overall installation and commissioning 41
7.13.1 Objectives 41
7.13.2 Requirements 42
7.14 Overall safety validation 42
7.14.1 Objective 42
7.14.2 Requirements 42
7.15 Overall operation, maintenance and repair 43
7.15.1 Objective 43
7.15.2 Requirements 43
7.16 Overall modification and retrofit 46
7.16.1 Objective 46
7.16.2 Requirements 47
7.17 Decommissioning or disposal 48
7.17.1 Objective 48
7.17.2 Requirements 48
7.18 Verification 49
7.18.1 Objective 49
7.18.2 Requirements 49
8 Functional safety assessment 50
8.1 Objective 50
8.2 Requirements 50
Annex A (informative) Example of a documentation structure 54
Bibliography 60

Figure 1 – Overall framework of the IEC 61508 series 11
Figure 2 – Overall safety lifecycle 18
Figure 3 – E/E/PE system safety lifecycle (in realisation phase) 19
Figure 4 – Software safety lifecycle (in realisation phase) 19
Figure 5 – Relationship of overall safety lifecycle to the E/E/PE system and software safety lifecycles 20
Figure 6 – Allocation of overall safety requirements to E/E/PE safety-related systems and other risk reduction measures 32
Figure 7 – Example of operations and maintenance activities model 45
Figure 8 – Example of operation and maintenance management model 46
Figure 9 – Example of modification procedure model 48
Figure A.1 – Structuring information into document sets for user groups 59

Table 1 – Overall safety lifecycle – overview 21
Table 2 – Safety integrity levels – target failure measures for a safety function operating in low demand mode of operation 33
Table 3 – Safety integrity levels – target failure measures for a safety function operating in high demand mode of operation or continuous mode of operation 34

Table 4 – Minimum levels of independence of those carrying out functional safety assessment (overall safety lifecycle phases 1 to 8 and 12 to 16 inclusive (see Figure 2)) 53

Table 5 – Minimum levels of independence of those carrying out functional safety assessment (overall safety lifecycle phases 9 and 10, including all phases of E/E/PE system and software safety lifecycles (see Figures 2, 3 and 4)) 53

Table A.1 – Example of a documentation structure for information related to the overall safety lifecycle 56

Table A.2 – Example of a documentation structure for information related to the E/E/PE system safety lifecycle..... 57

Table A.3 – Example of a documentation structure for information related to the software safety lifecycle 58

INTERNATIONAL ELECTROTECHNICAL COMMISSION

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

Part 1: General 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 61508-1 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/548/FDIS	65A/572/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 maintenance result 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 1: General requirements

1 Scope

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

1.2 In particular, this standard

a) applies to safety-related systems when one or more of such systems incorporates electrical/electronic/programmable electronic elements;

NOTE 1 In the context of low complexity E/E/PE safety-related systems, certain requirements specified in this standard may be unnecessary, and exemption from compliance with such requirements is possible (see 4.2, and the definition of a low complexity E/E/PE safety-related system in 3.4.3 of IEC 61508-4).

NOTE 2 Although a person can form part of a safety-related system (see 3.4.1 of IEC 61508-4), human factor requirements related to the design of E/E/PE safety-related systems are not considered in detail in this standard.

b) is generically-based and applicable to all E/E/PE safety-related systems irrespective of the application;

c) covers the achievement of a tolerable risk through the application of E/E/PE safety-related systems, but does not cover hazards arising from the E/E/PE equipment itself (for example electric shock);

d) applies to all types of E/E/PE safety-related systems, including protection systems and control systems;

e) does not cover E/E/PE systems where

   – a single E/E/PE system is capable on its own of meeting the tolerable risk, and

   – the required safety integrity of the safety functions of the single E/E/PE system is less than that specified for safety integrity level 1 (the lowest safety integrity level in this standard).

f) is mainly concerned with the E/E/PE safety-related systems whose failure could have an impact on the safety of persons and/or the environment; however, it is recognized that the consequences of failure could also have serious economic implications and in such cases this standard could be used to specify any E/E/PE system used for the protection of equipment or product;

NOTE 3 See 3.1.1 of IEC 61508-4.

g) considers E/E/PE safety-related systems and other risk reduction measures, in order that the safety requirements specification for the E/E/PE safety-related systems can be determined in a systematic, risk-based manner;

h) uses an overall safety lifecycle model as the technical framework for dealing systematically with the activities necessary for ensuring the functional safety of the E/E/PE safety-related systems;

NOTE 4 Although the overall safety lifecycle is primarily concerned with E/E/PE safety-related systems, it could also provide a technical framework for considering any safety-related system irrespective of the technology of that system (for example mechanical, hydraulic or pneumatic).

i) does not specify the safety integrity levels required for sector applications (which must be based on detailed information and knowledge of the sector application). The technical committees responsible for the specific application sectors shall specify, where appropriate, the safety integrity levels in the application sector standards;

j) provides general requirements for E/E/PE safety-related systems where no product or application sector international standards exist;

k) requires malevolent and unauthorised actions to be considered during hazard and risk analysis. The scope of the analysis includes all relevant safety lifecycle phases;

NOTE 5 Other IEC/ISO standards address this subject in depth; see ISO/IEC/TR 19791 and IEC 62443 series.

l) does not cover the precautions that may be necessary to prevent unauthorized persons damaging, and/or otherwise adversely affecting, the functional safety of E/E/PE safety-related systems (see k) above);

m) does not specify the requirements for the development, implementation, maintenance and/or operation of security policies or security services needed to meet a security policy that may be required by the E/E/PE safety-related system;

n) does not apply for medical equipment in compliance with the IEC 60601 series.

1.3 This part of the IEC 61508 series of standards includes general requirements that are applicable to all parts. Other parts of the IEC 61508 series concentrate on more specific topics:

– parts 2 and 3 provide additional and specific requirements for E/E/PE safety-related systems (for hardware and software);

– part 4 gives definitions and abbreviations that are used throughout this standard;

– part 5 provides guidelines on the application of part 1 in determining safety integrity levels, by showing example methods;

– part 6 provides guidelines on the application of parts 2 and 3;

– part 7 contains an overview of techniques and measures.

1.4 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.

NOTE 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.

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

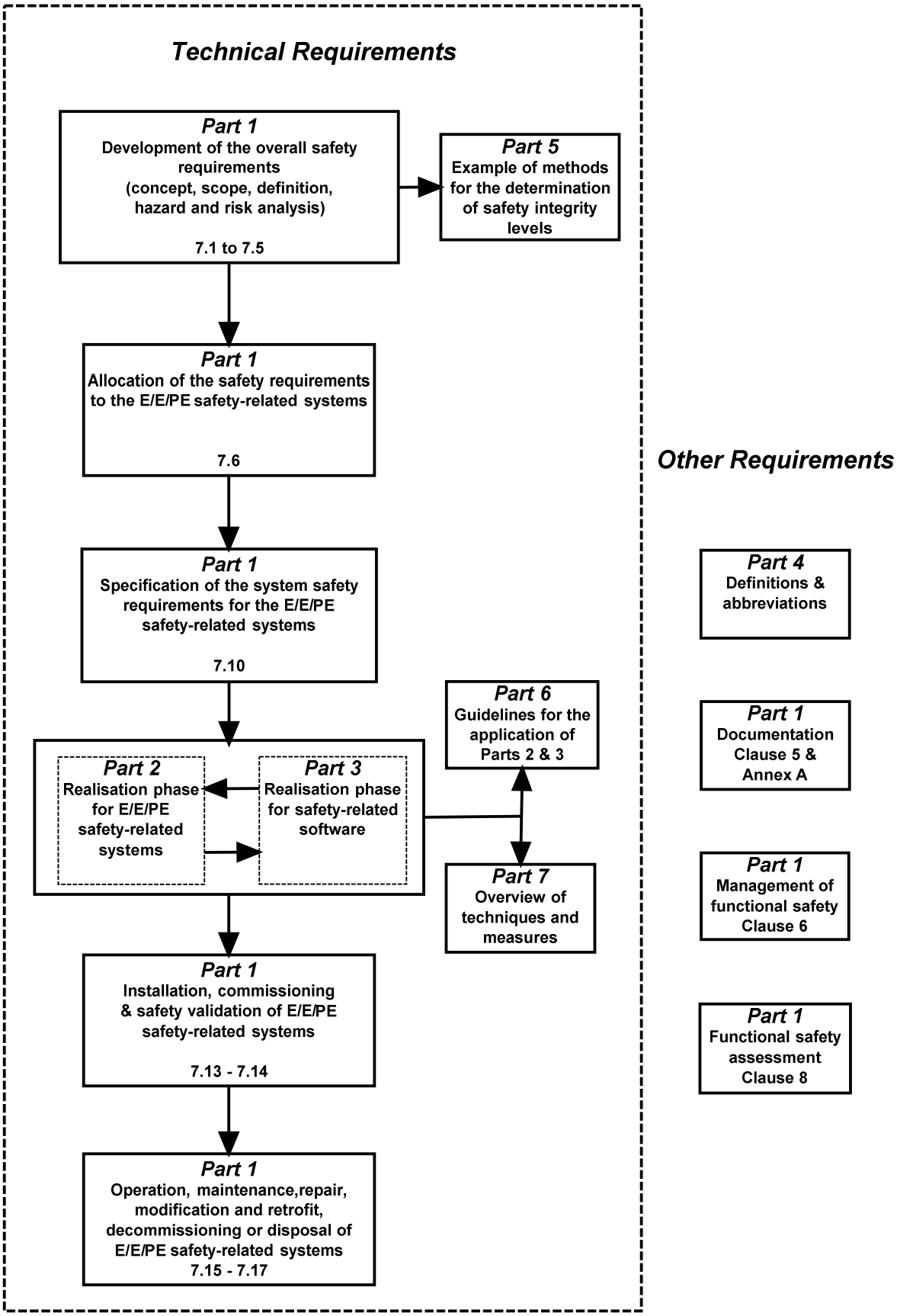


Figure 1 – Overall framework of the IEC 61508 series

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*

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*

SOMMAIRE

AVANT-PROPOS 65
INTRODUCTION 67
1 Domaine d'application 69
2 Références normatives 72
3 Définitions et abréviations 72
4 Conformité à la présente norme 72
5 Documentation 73
5.1 Objectifs 73
5.2 Exigences 73
6 Gestion de la sécurité fonctionnelle 74
6.1 Objectifs 74
6.2 Exigences 74
7 Exigences du cycle de vie de sécurité global 77
7.1 Généralités 77
7.1.1 Introduction 77
7.1.2 Objectifs et exigences – généralités 81
7.1.3 Objectifs 87
7.1.4 Exigences 87
7.2 Concept 88
7.2.1 Objectif 88
7.2.2 Exigences 88
7.3 Définition globale du domaine d'application 88
7.3.1 Objectifs 89
7.3.2 Exigences 89
7.4 Analyse des dangers et des risques 89
7.4.1 Objectifs 89
7.4.2 Exigences 90
7.5 Exigences globales de sécurité 91
7.5.1 Objectif 91
7.5.2 Exigences 92
7.6 Allocation des exigences globales de sécurité 93
7.6.1 Objectifs 93
7.6.2 Exigences 94
7.7 Planification globale de l'exploitation et de la maintenance 99
7.7.1 Objectif 99
7.7.2 Exigences 100
7.8 Planification globale de la validation de la sécurité 101
7.8.1 Objectif 101
7.8.2 Exigences 101
7.9 Planification globale de l'installation et de la mise en service 102
7.9.1 Objectifs 102
7.9.2 Exigences 102
7.10 Spécification des exigences de sécurité relatives aux systèmes E/E/PE 103
7.10.1 Objectif 103
7.10.2 Exigences 103
7.11 Systèmes E/E/PE relatifs à la sécurité – réalisation 105

7.11.1 Objectif 105
7.11.2 Exigences 105
7.12 Dispositifs externes de réduction de risque – spécification et réalisation 105
7.12.1 Objectif 106
7.12.2 Exigences 106
7.13 Installation et mise en service globales 106
7.13.1 Objectifs 106
7.13.2 Exigences 106
7.14 Validation globale de la sécurité 106
7.14.1 Objectif 107
7.14.2 Exigences 107
7.15 Exploitation, maintenance et réparation globales 107
7.15.1 Objectif 108
7.15.2 Exigences 108
7.16 Modification et remise à niveau globales 110
7.16.1 Objectif 111
7.16.2 Exigences 111
7.17 Mise hors service ou au rebut 113
7.17.1 Objectif 113
7.17.2 Exigences 113
7.18 Vérification 114
7.18.1 Objectif 114
7.18.2 Exigences 114
8 Evaluation de la sécurité fonctionnelle 115
8.1 Objectif 115
8.2 Exigences 115
Annexe A (informative) Exemple de structure de documentation 120
Bibliographie 126

Figure 1 – Structure générale de la série CEI 61508 71
Figure 2 – Cycle de vie de sécurité global 79
Figure 3 – Cycle de vie de sécurité du système E/E/PE (en phase de réalisation) 80
Figure 4 – Cycle de vie de sécurité du logiciel (en phase de réalisation) 80
Figure 5 – Relation entre le cycle de vie de sécurité global du système E/E/PE et les cycles de vie de sécurité du logiciel 81
Figure 6 – Allocation des exigences de sécurité globale aux systèmes E/E/PE relatifs à la sécurité et dispositifs externes de réduction de risque 96
Figure 7 – Exemple de modèle d'activités d'exploitation et de maintenance 109
Figure 8 – Exemple de modèle de gestion d'exploitation et de maintenance 110
Figure 9 – Exemple de modèle de procédure de modification 113
Figure A.1 – Structuration de l'information en ensembles de documents pour les groupes d'utilisateurs 125

Tableau 1 – Cycle de vie de sécurité global – vue d'ensemble 82
Tableau 2 – Niveaux d'intégrité de sécurité – objectifs chiffrés de défaillance pour une fonction de sécurité en mode de fonctionnement à faible sollicitation 97

Tableau 3 – Niveaux d'intégrité de sécurité – objectifs chiffrés de défaillance pour une fonction de sécurité en mode de fonctionnement à sollicitation élevée ou en mode de fonctionnement continu 98

Tableau 4 – Degrés minimaux d'indépendance des responsables de l'évaluation de la sécurité fonctionnelle (phases 1 à 8 et 12 à 16 incluses du cycle de vie de sécurité global (voir Figure 2)) 118

Tableau 5 – Degrés minimaux d'indépendance des responsables de l'évaluation de la sécurité fonctionnelle (phases 9 et 10 du cycle de vie de sécurité global, incluant toutes les phases des cycles de vie de sécurité du système E/E/PE et du logiciel) (voir Figures 2, 3 et 4) 119

Tableau A.1 – Exemple de structure de documentation pour l'information relative au cycle de vie de sécurité global 122

Tableau A.2 – Exemple de structure de documentation pour l'information relative au cycle de vie de sécurité du système E/E/PE 123

Tableau A.3 – Exemple de structure de documentation pour l'information relative au cycle de vie de sécurité du logiciel 124

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

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

Partie 1: Exigences générales

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 61508-1 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 d'une publication fondamentale de sécurité conformément au Guide CEI 104.

Le texte de cette norme est issu des documents suivants:

FDIS	Rapport de vote
65A/548/FDIS	65A/572/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 maintenance 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 la conceptualisation initiale, 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 1: Exigences générales

1 Domaine d'application

1.1 La présente Norme internationale traite des aspects à prendre en considération lors de l'utilisation de systèmes électriques/électroniques/électroniques programmables (E/E/PE) pour exécuter des fonctions de sécurité. L'un des objectifs majeurs de la présente norme est de permettre l'élaboration par les comités d'études qui en sont responsables de normes internationales de produit et d'application sectorielle. Cela permet de prendre pleinement en compte l'ensemble des facteurs pertinents associés au produit ou à l'application, et donc de répondre aux besoins spécifiques des utilisateurs du produit et du secteur d'application concernés. Un second objectif de la présente norme est de permettre le développement de systèmes E/E/PE relatifs à la sécurité en l'absence de normes internationales de produit ou d'application sectorielle.

1.2 En particulier, la présente norme

a) s'applique aux systèmes relatifs à la sécurité lorsqu'un ou plusieurs de ces systèmes comporte(nt) des dispositifs électriques/électroniques/électroniques programmables,

NOTE 1 En ce qui concerne les systèmes E/E/PE relatifs à la sécurité de faible complexité, certaines exigences décrites dans la présente norme peuvent ne pas être nécessaires et une exemption de conformité à de telles exigences est possible (voir 4.2, et la définition d'un système E/E/PE relatif à la sécurité de faible complexité en 3.4.3 de la CEI 61508-4).

NOTE 2 Bien qu'une personne physique puisse faire partie d'un système relatif à la sécurité (voir 3.4.1 de la CEI 61508-4), les exigences concernant le facteur humain dans la conception de systèmes E/E/PE relatifs à la sécurité ne sont pas détaillées dans la présente norme.

b) est génériquement basée sur et applicable à tous les systèmes E/E/PE relatifs à la sécurité, indépendamment de l'application,

c) couvre l'occurrence d'un risque tolérable engendré par l'application de systèmes E/E/PE relatifs à la sécurité, mais ne couvre pas les dangers qui découlent de l'équipement E/E/PE lui-même (par exemple, choc électrique),

d) s'applique à tous les types de systèmes E/E/PE relatifs à la sécurité, y compris les systèmes de protection et de commande,

e) ne couvre pas les systèmes E/E/PE lorsque

   – un système E/E/PE unique est capable par lui-même de pallier le risque tolérable, et

   – l'intégrité de sécurité requise des fonctions de sécurité du système E/E/PE unique est moindre que celle spécifiée pour le niveau 1 d'intégrité de sécurité (niveau d'intégrité de sécurité le plus faible décrit dans la présente norme),

f) traite principalement des systèmes E/E/PE relatifs à la sécurité dont la défaillance pourrait avoir un impact sur la sécurité des personnes et/ou sur l'environnement; cependant, les défaillances peuvent avoir des conséquences économiques sévères, et dans de pareils cas, la présente norme peut être utilisée pour prescrire tout système E/E/PE utilisé pour protéger l'équipement ou le produit,

NOTE 3 Voir 3.1.1 de la CEI 61508-4.

g) considère les systèmes E/E/PE relatifs à la sécurité et les dispositifs externes de réduction de risque de façon à ce que la spécification des exigences de sécurité pour les systèmes E/E/PE relatifs à la sécurité puisse être déterminée en étant basée systématiquement sur le risque,

h) utilise, en tant que cadre technique, un modèle de cycle de vie de sécurité global pour traiter, de façon systématique, des activités nécessaires pour assurer la sécurité fonctionnelle des systèmes E/E/PE relatifs à la sécurité,

NOTE 4 Bien que le cycle de vie de sécurité global concerne avant tout les systèmes E/E/PE relatifs à la sécurité, il peut aussi fournir un cadre technique pour l'étude de tout système relatif à la sécurité, indépendamment de la technologie employée par ce système (par exemple, mécanique, hydraulique ou pneumatique).

i) ne spécifie pas les niveaux d'intégrité de sécurité requis pour les applications sectorielles (ces niveaux doivent être basés sur des informations détaillées et une bonne connaissance de l'application sectorielle). Les comités d'études responsables des secteurs d'application spécifiques doivent spécifier, si nécessaire, les niveaux d'intégrité de sécurité dans les normes sectorielles,

j) spécifie des exigences générales pour les systèmes E/E/PE relatifs à la sécurité en l'absence de normes internationales de produit ou d'application sectorielle,

k) nécessite de prendre en considération au cours de l'analyse des dangers et des risques, les actions malveillantes et non autorisées. L'étendue de l'analyse comprend toutes les phases pertinentes du cycle de vie de sécurité,

NOTE 5 D'autres normes CEI/ISO traitent de ce sujet en profondeur; voir ISO/CEI/TR 19791 et la série CEI 62443.

l) ne traite pas des mesures préventives qu'il peut être nécessaire de prendre afin d'éviter que des personnes non autorisées altèrent, et/ou exercent, d'une manière quelconque, une activité dommageable pour la sécurité fonctionnelle des systèmes E/E/PE relatifs à la sécurité (voir k) ci-dessus),

m) ne spécifie pas les exigences relatives au développement, à la mise en oeuvre, à la maintenance et/ou à l'application de politiques ou de services de sécurité nécessaires pour satisfaire à une politique de sécurité donnée, susceptible d'être requise par le système E/E/PE relatif à la sécurité,

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

1.3 La présente partie de la série de normes CEI 61508 définit les exigences générales qui sont applicables à toutes les parties. Les autres parties de la série CEI 61508 traitent de sujets plus spécifiques:

– les parties 2 et 3 fournissent des exigences supplémentaires et spécifiques pour les systèmes E/E/PE relatifs à la sécurité (pour le matériel et le logiciel),

– la partie 4 donne les définitions et les abréviations qui sont utilisées tout au long de la présente norme,

– la partie 5 fournit des lignes directrices concernant l'application de la partie 1 pour la détermination des niveaux d'intégrité de sécurité, en présentant des exemples de méthodes,

– la partie 6 fournit des lignes directrices concernant l'application des parties 2 et 3,

– la partie 7 contient une présentation des techniques et des mesures.

1.4 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.

NOTE 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.

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

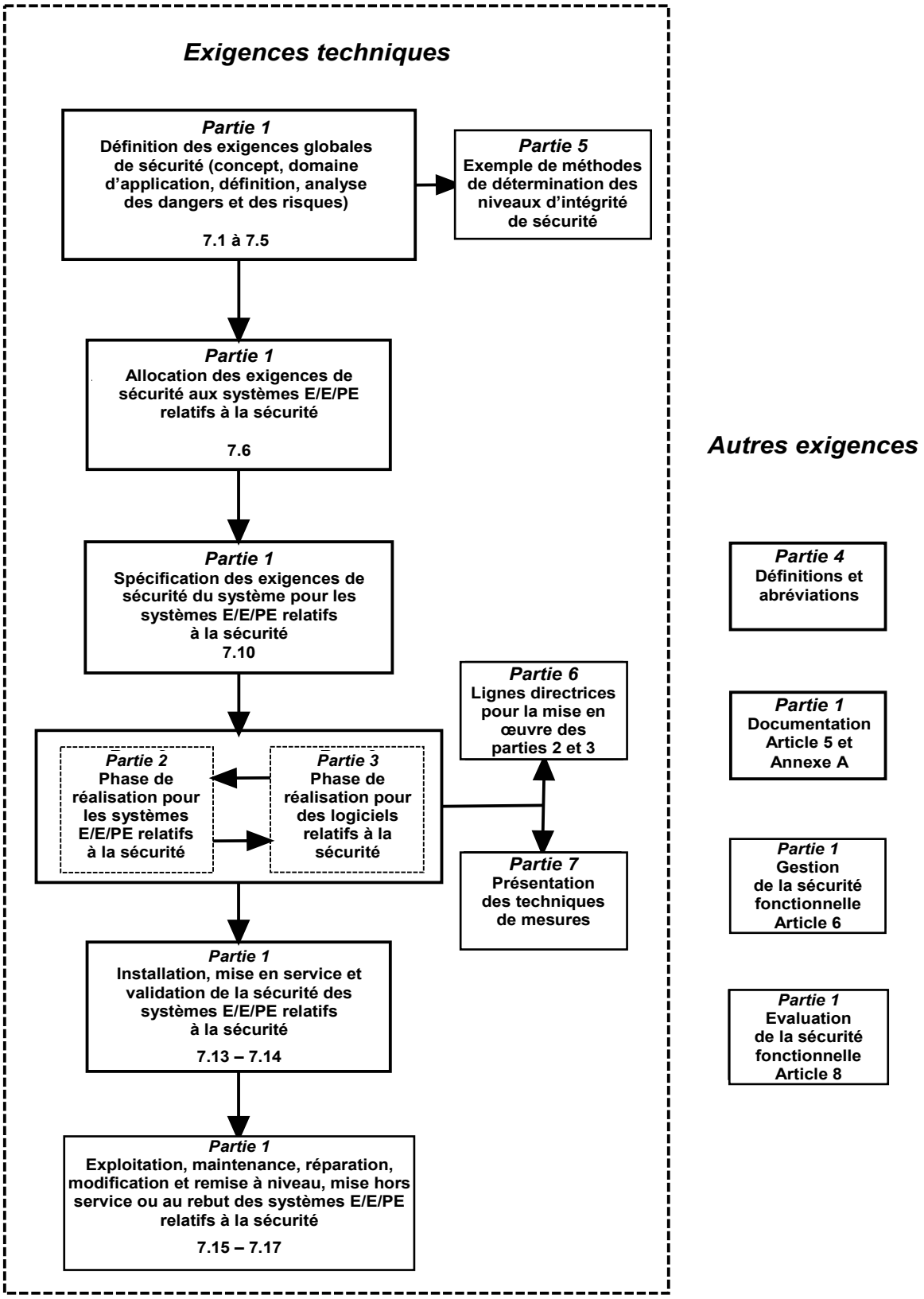


Figure 1 – Structure générale de la série CEI 61508

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 61508-2:2010, *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 61508-3:2010, *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 3: Exigences concernant les logiciels*

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*