IEC 61508-2

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 2: Requirements for electrical/electronic/programmable electronic safety-related systems

Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 2: Exigences pour les systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité

INTERNATIONAL ELECTROTECHNICAL COMMISSION

COMMISSION ELECTROTECHNIQUE INTERNATIONALE

PRICE CODE XD
CODE PRIX

ICS 25.040.40

ISBN 978-2-88910-525-0

® 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
6 Management of functional safety 13
7 E/E/PE system safety lifecycle requirements 13
7.1 General 13
7.1.1 Objectives and requirements – general 13
7.1.2 Objectives 13
7.1.3 Requirements 13
7.2 E/E/PE system design requirements specification 17
7.2.1 Objective 17
7.2.2 General 17
7.2.3 E/E/PE system design requirements specification 18
7.3 E/E/PE system safety validation planning 19
7.3.1 Objective 19
7.3.2 Requirements 19
7.4 E/E/PE system design and development 19
7.4.1 Objective 20
7.4.2 General requirements 20
7.4.3 Synthesis of elements to achieve the required systematic capability 22
7.4.4 Hardware safety integrity architectural constraints 23
7.4.5 Requirements for quantifying the effect of random hardware failures 32
7.4.6 Requirements for the avoidance of systematic faults 34
7.4.7 Requirements for the control of systematic faults 35
7.4.8 Requirements for system behaviour on detection of a fault 35
7.4.9 Requirements for E/E/PE system implementation 36
7.4.10 Requirements for proven in use elements 38
7.4.11 Additional requirements for data communications 39
7.5 E/E/PE system integration 40
7.5.1 Objective 40
7.5.2 Requirements 40
7.6 E/E/PE system operation and maintenance procedures 41
7.6.1 Objective 41
7.6.2 Requirements 41
7.7 E/E/PE system safety validation 42
7.7.1 Objective 42
7.7.2 Requirements 42
7.8 E/E/PE system modification 43
7.8.1 Objective 43
7.8.2 Requirements 43
7.9 E/E/PE system verification 44
7.9.1 Objective 44

7.9.2 Requirements 44
8 Functional safety assessment 46
Annex A (normative) Techniques and measures for E/E/PE safety-related systems – control of failures during operation 47
Annex B (normative) Techniques and measures for E/E/PE safety-related systems – avoidance of systematic failures during the different phases of the lifecycle 62
Annex C (normative) Diagnostic coverage and safe failure fraction 71
Annex D (normative) Safety manual for compliant items 74
Annex E (normative) Special architecture requirements for integrated circuits (ICs) with on-chip redundancy 76
Annex F (informative) Techniques and measures for ASICs – avoidance of systematic failures 81
Bibliography 89

Figure 1 – Overall framework of the IEC 61508 series 11
Figure 2 – E/E/PE system safety lifecycle (in realisation phase) 14
Figure 3 – ASIC development lifecycle (the V-Model) 15
Figure 4 – Relationship between and scope of IEC 61508-2 and IEC 61508-3 15
Figure 5 – Determination of the maximum SIL for specified architecture (E/E/PE safety-related subsystem comprising a number of series elements, see 7.4.4.2.3) 28
Figure 6 – Determination of the maximum SIL for specified architecture (E/E/PE safety-related subsystem comprised of two subsystems X & Y, see 7.4.4.2.4) 30
Figure 7 – Architectures for data communication 40

Table 1 – Overview – realisation phase of the E/E/PE system safety lifecycle 16
Table 2 – Maximum allowable safety integrity level for a safety function carried out by a type A safety-related element or subsystem 26
Table 3 – Maximum allowable safety integrity level for a safety function carried out by a type B safety-related element or subsystem 27
Table A.1 – Faults or failures to be assumed when quantifying the effect of random hardware failures or to be taken into account in the derivation of safe failure fraction 49
Table A.2 – Electrical components 51
Table A.3 – Electronic components 51
Table A.4 – Processing units 52
Table A.5 – Invariable memory ranges 52
Table A.6 – Variable memory ranges 53
Table A.7 – I/O units and interface (external communication) 53
Table A.8 – Data paths (internal communication) 54
Table A.9 – Power supply 54
Table A.10 – Program sequence (watch-dog) 55
Table A.11 – Clock 55
Table A.12 – Communication and mass-storage 55
Table A.13 – Sensors 56
Table A.14 – Final elements (actuators) 56
Table A.15 – Techniques and measures to control systematic failures caused by hardware design 58

Table A.16 – Techniques and measures to control systematic failures caused by environmental stress or influences 59
Table A.17 – Techniques and measures to control systematic operational failures 60
Table A.18 – Effectiveness of techniques and measures to control systematic failures 61
Table B.1 – Techniques and measures to avoid mistakes during specification of E/E/PE system design requirements (see 7.2) 63
Table B.2 – Techniques and measures to avoid introducing faults during E/E/PE system design and development (see 7.4) 64
Table B.3 – Techniques and measures to avoid faults during E/E/PE system integration (see 7.5) 65
Table B.4 – Techniques and measures to avoid faults and failures during E/E/PE system operation and maintenance procedures (see 7.6) 66
Table B.5 – Techniques and measures to avoid faults during E/E/PE system safety validation (see 7.7) 67
Table B.6 – Effectiveness of techniques and measures to avoid systematic failures 68
Table E.1 – Techniques and measures that increase $\beta_{B\text{-}IC}$ 79
Table E.2 – Techniques and measures that decrease $\beta_{B\text{-}IC}$ 80
Table F.1 – Techniques and measures to avoid introducing faults during ASIC's design and development – full and semi-custom digital ASICs (see 7.4.6.7) 83
Table F.2 – Techniques and measures to avoid introducing faults during ASIC design and development: User programmable ICs (FPGA/PLD/CPLD) (see 7.4.6.7) 86

INTERNATIONAL ELECTROTECHNICAL COMMISSION

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

Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems

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 61508-2 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 2000. 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/549/FDIS	65A/573/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, though 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;
- 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 2: Requirements for electrical/electronic/programmable electronic safety-related systems

1 Scope

1.1 This part of the IEC 61508 series

a) is intended to be used only after a thorough understanding of IEC 61508-1, which provides the overall framework for the achievement of functional safety;

b) applies to any safety-related system, as defined by IEC 61508-1, that contains at least one electrical, electronic or programmable electronic element;

c) applies to all elements within an E/E/PE safety-related system (including sensors, actuators and the operator interface);

d) specifies how to refine the E/E/PE system safety requirements specification, developed in accordance with IEC 61508-1 (comprising the E/E/PE system safety functions requirements specification and the E/E/PE system safety integrity requirements specification), into the E/E/PE system design requirements specification;

e) specifies the requirements for activities that are to be applied during the design and manufacture of the E/E/PE safety-related systems (i.e. establishes the E/E/PE system safety lifecycle model) except software, which is dealt with in IEC 61508-3 (see Figures 2 to 4). These requirements include the application of techniques and measures that are graded against the safety integrity level, for the avoidance of, and control of, faults and failures;

f) specifies the information necessary for carrying out the installation, commissioning and final safety validation of the E/E/PE safety-related systems;

g) does not apply to the operation and maintenance phase of the E/E/PE safety-related systems – this is dealt with in IEC 61508-1 – however, IEC 61508-2 does provide requirements for the preparation of information and procedures needed by the user for the operation and maintenance of the E/E/PE safety-related systems;

h) specifies requirements to be met by the organisation carrying out any modification of the E/E/PE safety-related systems;

NOTE 1 This part of IEC 61508 is mainly directed at suppliers and/or in-company engineering departments, hence the inclusion of requirements for modification.

NOTE 2 The relationship between IEC 61508-2 and IEC 61508-3 is illustrated in Figure 4.

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

1.2 IEC 61508-1, IEC 61508-2, IEC 61508-3 and IEC 61508-4 are basic safety publications, although this status does not apply in the context of low complexity E/E/PE safety-related systems (see 3.4.3 of IEC 61508-4). As basic safety publications, they are intended for use by technical committees in the preparation of standards in accordance with the principles contained in IEC Guide 104 and ISO/IEC Guide 51. IEC 61508-1, IEC 61508-2, IEC 61508-3 and IEC 61508-4 are also intended for use as stand-alone standards. 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.

NOTE The functional safety of an E/E/PE safety-related system can only be achieved when all related requirements are met. Therefore, it is important that all related requirements are carefully considered and adequately referenced.

1.4 Figure 1 shows the overall framework of the IEC 61508 series and indicates the role that IEC 61508-2 plays in the achievement of functional safety for E/E/PE safety-related systems. Annex A of IEC 61508-6 describes the application of IEC 61508-2 and IEC 61508-3.

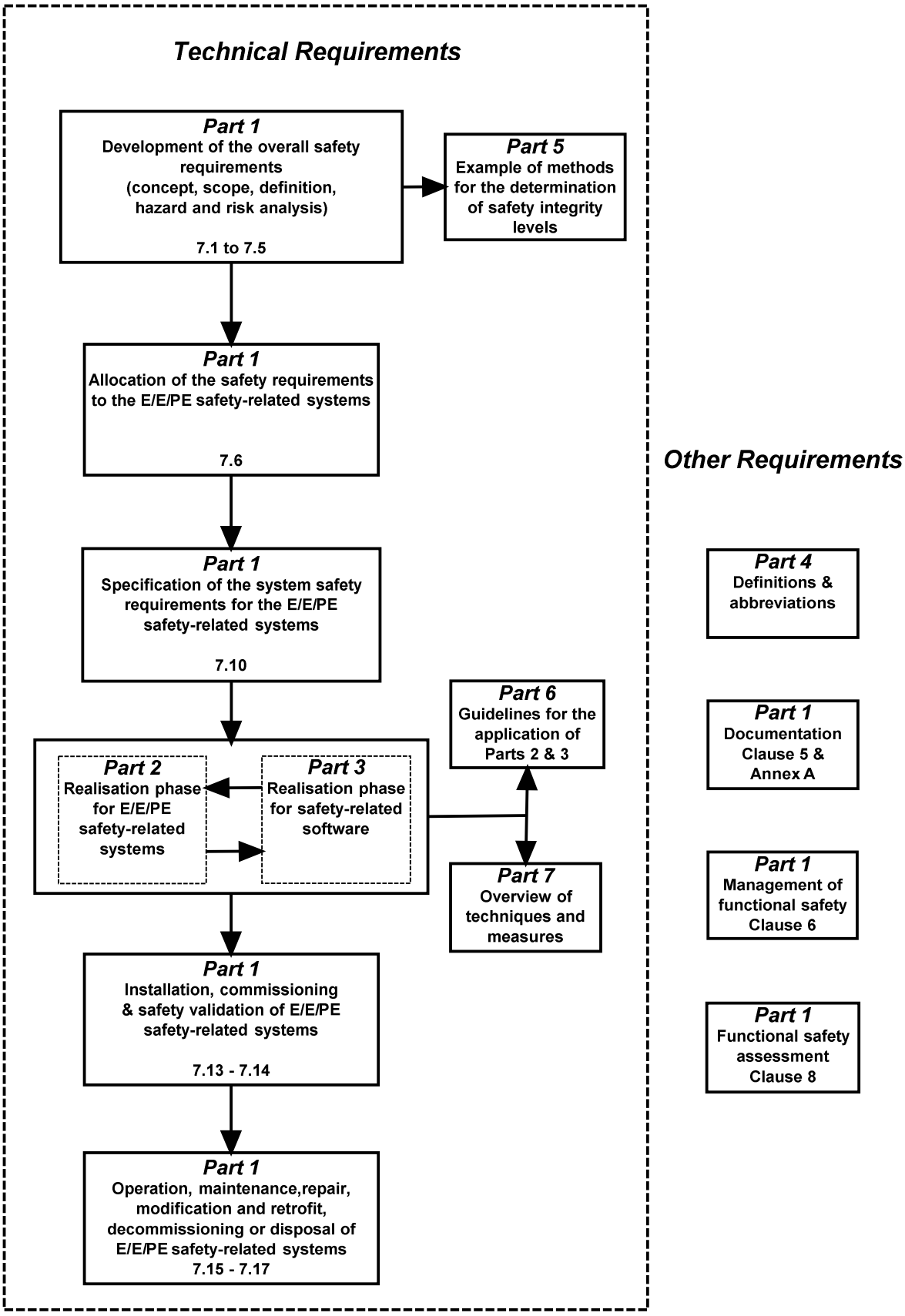


Figure 1 – Overall framework of the IEC 61508 series

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 60947-5-1, *Low-voltage switchgear and controlgear – Part 5-1: Control circuit devices and switching elements – Electromechanical control circuit devices*

IEC/TS 61000-1-2, *Electromagnetic compatibility (EMC) – Part 1-2: General – Methodology for the achievement of functional safety of electrical and electronic systems including equipment with regard to electromagnetic phenomena*

IEC 61326-3-1, *Electrical equipment for measurement, control and laboratory use – EMC requirements – Part 3-1: Immunity requirements for safety-related systems and for equipment intended to perform safety-related functions (functional safety) – General industrial applications*

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

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 61508-7: 2010, *Functional safety of electrical/electronic/programmable electronic safety related systems – Part 7: Overview of techniques and measures*

IEC 61784-3, *Industrial communication networks – Profiles – Part 3: Functional safety fieldbuses – General rules and profile definitions*

IEC 62280-1, *Railway applications – Communication, signalling and processing systems – Part 1: Safety-related communication in closed transmission systems*

IEC 62280-2, *Railway applications – Communication, signalling and processing systems – Part 2: Safety-related communication in open transmission systems*

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*

EN 50205, *Relays with forcibly guided (mechanically linked) contacts*

SOMMAIRE

AVANT-PROPOS 93
INTRODUCTION 95
1 Domaine d'application 97
2 Références normatives 100
3 Définitions et abréviations 101
4 Conformité à la présente norme 101
5 Documentation 101
6 Gestion de la sécurité fonctionnelle 101
7 Exigences concernant le cycle de vie de sécurité des systèmes E/E/PE 101
7.1 Généralités 101
7.1.1 Objectifs et exigences – généralités 101
7.1.2 Objectifs 101
7.1.3 Exigences 101
7.2 Spécification des exigences de conception des systèmes E/E/PE 107
7.2.1 Objectif 107
7.2.2 Généralités 108
7.2.3 Spécification des exigences de conception des systèmes E/E/PE 108
7.3 Planification de la validation de la sécurité des systèmes E/E/PE 109
7.3.1 Objectif 109
7.3.2 Exigences 110
7.4 Conception et développement des systèmes E/E/PE 110
7.4.1 Objectif 110
7.4.2 Exigences générales 110
7.4.3 Synthèse des éléments permettant d'obtenir la capabilité systématique requise 113
7.4.4 Contraintes architecturales portant sur l'intégrité de sécurité du matériel 114
7.4.5 Exigences relatives à la quantification de l'effet de défaillances aléatoires du matériel 123
7.4.6 Exigences pour l'évitement des anomalies systématiques 125
7.4.7 Exigences pour la maîtrise des anomalies systématiques 126
7.4.8 Exigences relatives au comportement du système, lors de la détection d'une anomalie 127
7.4.9 Exigences relatives à la mise en œuvre du système E/E/PE 128
7.4.10 Exigences relatives aux éléments éprouvés par une utilisation antérieure 130
7.4.11 Exigences supplémentaires relatives aux communications de données 131
7.5 Intégration des systèmes E/E/PE 132
7.5.1 Objectif 132
7.5.2 Exigences 132
7.6 Procédures d'exploitation et de maintenance des systèmes E/E/PE 133
7.6.1 Objectif 133
7.6.2 Exigences 133
7.7 Validation de la sécurité des systèmes E/E/PE 135
7.7.1 Objectif 135
7.7.2 Exigences 135

7.8 Modification des systèmes E/E/PE 136
7.8.1 Objectif 136
7.8.2 Exigences 136
7.9 Vérification des systèmes E/E/PE 136
7.9.1 Objectif 136
7.9.2 Exigences 137
8 Evaluation de la sécurité fonctionnelle 138
Annexe A (normative) Techniques et mesures applicables aux systèmes E/E/PE relatifs à la sécurité – maîtrise des défaillances en exploitation 139
Annexe B (normative) Techniques et mesures applicables aux systèmes E/E/PE relatifs à la sécurité – évitement des défaillances systématiques lors des différentes phases du cycle de vie 157
Annexe C (normative) Couverture de diagnostic et proportion de défaillances en sécurité 167
Annexe D (normative) Manuel de sécurité d'article conforme 170
Annexe E (normative) Exigences d'architecture particulières relatives aux circuits intégrés (CI) avec redondance sur la puce 172
Annexe F (informative) Techniques et mesures pour les ASIC – évitement des défaillances systématiques 178
Bibliographie 187

Figure 1 – Structure générale de la série CEI 61508 99
Figure 2 – Cycle de vie de sécurité du système E/E/PE (en phase de réalisation) 103
Figure 3 – Cycle de vie de développement d'un ASIC (modèle en V) 104
Figure 4 – Relation et domaine d'application pour la CEI 61508-2 et la CEI 61508-3 105
Figure 5 – Détermination du SIL maximal pour l'architecture spécifiée (sous-système E/E/PE relatif à la sécurité comprenant un grand nombre d'éléments en série, voir 7.4.4.2.3) 119
Figure 6 – Détermination du SIL maximal pour l'architecture spécifiée (sous-système E/E/PE relatif à la sécurité comprenant deux sous-systèmes X & Y, voir 7.4.4.2.4) 121
Figure 7 – Architectures pour la communication des données 132

Tableau 1 – Présentation – Phase de réalisation du cycle de vie de sécurité du système E/E/PE 106
Tableau 2 – Niveau d'intégrité de sécurité maximal admissible pour une fonction de sécurité exécutée par un élément ou sous-système relatif à la sécurité de type A 117
Tableau 3 – Niveau d'intégrité de sécurité maximal admissible pour une fonction de sécurité exécutée par un élément ou sous-système relatif à la sécurité de type B 118
Tableau A.1 – Anomalies ou défaillances à supposer lors de la quantification de l'effet des défaillances aléatoires du matériel ou à prendre en compte pour déduire la proportion de défaillances en sécurité 141
Tableau A.2 – Composants électriques 143
Tableau A.3 – Composants électroniques 143
Tableau A.4 – Unités de traitement 144
Tableau A.5 – Plages de mémoire invariable 145
Tableau A.6 – Plages de mémoire variable 146
Tableau A.7 – Unités E/S et interface (communication externe) 147
Tableau A.8 – Chemins de données (communication interne) 147

Tableau A.9 – Alimentation 148
Tableau A.10 – Séquence du programme (chien de garde) 148
Tableau A.11 – Horloge 149
Tableau A.12 – Communication et mémoire de masse 149
Tableau A.13 – Capteurs 150
Tableau A.14 – Eléments finaux (actionneurs) 150
Tableau A.15 – Techniques et mesures pour maîtriser les défaillances systématiques dues à la conception du matériel 152
Tableau A.16 – Techniques et mesures pour maîtriser les défaillances systématiques dues aux contraintes ou influences environnementales 153
Tableau A.17 – Techniques et mesures pour maîtriser les défaillances systématiques en exploitation 154
Tableau A.18 – Efficacité des techniques et mesures pour la maîtrise des défaillances systématiques 155
Tableau B.1 – Techniques et mesures pour éviter les erreurs lors de la spécification des exigences de conception des systèmes E/E/PE (voir 7.2) 159
Tableau B.2 – Techniques et mesures pour éviter l'introduction d'anomalies lors de la conception et du développement des systèmes E/E/PE (voir 7.4) 160
Tableau B.3 – Techniques et mesures pour éviter les anomalies lors de l'intégration des systèmes E/E/PE (voir 7.5) 161
Tableau B.4 – Techniques et mesures pour éviter les anomalies et les défaillances pendant les procédures d'exploitation et de maintenance des systèmes E/E/PE (voir 7.6) 162
Tableau B.5 – Techniques et mesures pour éviter les anomalies lors de la validation de sécurité des systèmes E/E/PE (voir 7.7) 163
Tableau B.6 – Efficacité des techniques et mesures d'évitement des défaillances systématiques 164
Tableau E.1 – Techniques et mesures d'accroissement du facteur $\beta_{B\text{-}IC}$ 176
Tableau E.2 – Techniques et mesures de diminution du facteur $\beta_{B\text{-}IC}$ 177
Tableau F.1 – Techniques et mesures pour éviter l'introduction d'anomalies lors de la conception et du développement des ASIC – circuits intégrés numériques spécifiques et semi-personnalisés (voir 7.4.6.7) 180
Tableau F.2 – Techniques et mesures pour éviter l'introduction d'anomalies lors de la conception et du développement des ASIC: Circuits intégrés programmables par l'utilisateur (FPGA/PLD/CPLD) (voir 7.4.6.7) 184

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

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

Partie 2: Exigences pour les systèmes électriques/électroniques/ électroniques programmables relatifs à la sécurité

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 61508-2 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 2000 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/549/FDIS	65A/573/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 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,

– 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 2: Exigences pour les systèmes électriques/électroniques/ électroniques programmables relatifs à la sécurité

1 Domaine d'application

1.1 La présente partie de la série CEI 61508

a) est destinée à être utilisée uniquement après avoir assimilé sans ambiguïté la CEI 61508-1 qui fournit le cadre global permettant d'obtenir la sécurité fonctionnelle;

b) s'applique à tout système relatif à la sécurité tel que défini dans la CEI 61508-1, qui contient au moins un composant à base électrique, électronique ou électronique programmable;

c) s'applique à tous les éléments d'un système E/E/PE relatif à la sécurité (y compris les capteurs, les actionneurs et l'interface opérateur);

d) spécifie la manière d'affiner la spécification des exigences de sécurité des systèmes E/E/PE, développée conformément à la CEI 61508-1 (comprenant la spécification des exigences relatives aux fonctions de sécurité des systèmes E/E/PE et la spécification des exigences d'intégrité de sécurité de ces systèmes), dans le cadre de la spécification des exigences de conception des systèmes E/E/PE;

e) spécifie les exigences pour des activités qui doivent être appliquées pendant la conception et la fabrication des systèmes E/E/PE relatifs à la sécurité (ce qui signifie qu'elle établit le modèle du cycle de vie de sécurité des systèmes E/E/PE), à l'exception du logiciel qui est traité dans la CEI 61508-3 (voir Figures 2 à 4). Ces exigences comprennent l'application de techniques et de mesures qui sont classées en fonction du niveau d'intégrité de sécurité pour éviter et maîtriser les anomalies et défaillances;

f) spécifie les informations nécessaires à l'installation, à la mise en service et à la validation finale de la sécurité des systèmes E/E/PE relatifs à la sécurité;

g) ne s'applique pas à la phase d'exploitation et de maintenance des systèmes E/E/PE relatifs à la sécurité - celle-ci étant traitée dans la CEI 61508-1 - cependant, la CEI 61508-2 fournit des exigences relatives à la préparation des informations et procédures nécessaires à l'utilisateur pour l'exploitation et la maintenance des systèmes E/E/PE relatifs à la sécurité;

h) spécifie les exigences auxquelles doit satisfaire l'entité qui effectue une modification des systèmes E/E/PE relatifs à la sécurité;

NOTE 1 Cette partie de la CEI 61508 est principalement destinée aux fournisseurs et/ou aux services techniques internes des entreprises. Ceci est la raison pour laquelle elle comprend des exigences applicables en matière de modification.

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

i) 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.

NOTE La sécurité fonctionnelle d'un système E/E/PE relatif à la sécurité ne peut être réalisée que lorsque toutes les exigences pertinentes sont satisfaites. En conséquence, il est important d'accorder une attention toute particulière aux exigences associées et de les référencer de façon appropriée.

1.4 La Figure 1 illustre la structure générale de la série CEI 61508 et montre le rôle que la CEI 61508-4 joue dans la réalisation de la sécurité fonctionnelle pour les systèmes E/E/PE relatifs à la sécurité. L'Annexe A de la CEI 61508-6 décrit l'application des CEI 61508-2 et 61508-3.

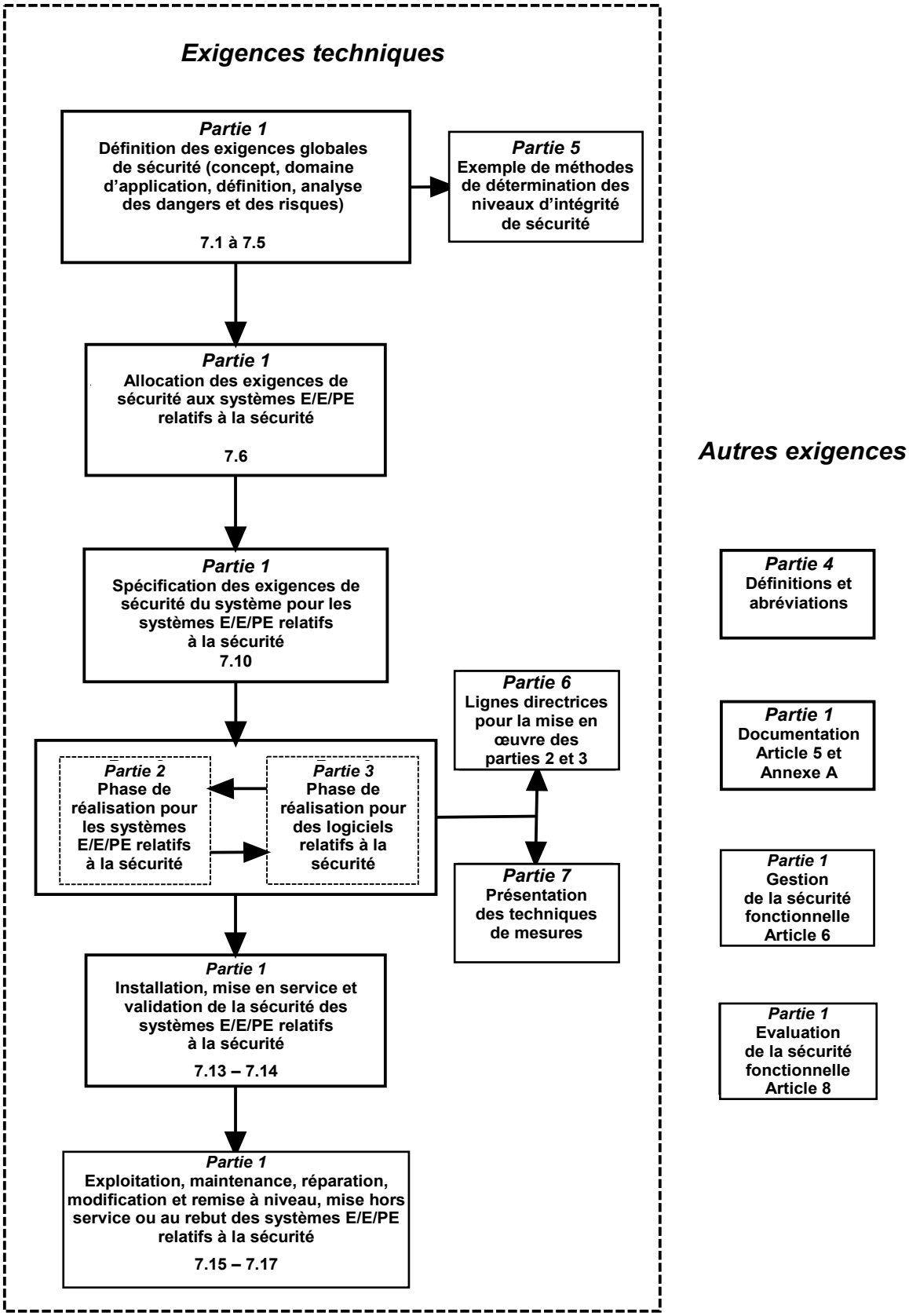


Figure 1 – Structure générale de la série CEI 61508

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 60947-5-1, *Appareillage à basse tension – Partie 5-1: Appareils et éléments de commutation pour circuits de commande – Appareils électromécaniques pour circuits de commande*

CEI/TS 61000-1-2, *Electromagnetic compatibility (EMC) – Part 1-2: General – Methodology for the achievement of functional safety of electrical and electronic systems including equipment with regard to electromagnetic phenomena* (disponible en anglais seulement)

CEI 61326-3-1, *Matériel électrique de mesure, de commande et de laboratoire – Exigences relatives à la CEM – Partie 3-1: Exigences d'immunité pour les systèmes relatifs à la sécurité et pour les matériels destinés à réaliser des fonctions relatives à la sécurité (sécurité fonctionnelle) – Applications industrielles générales*

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

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*

CEI 61508-7 : 2010, *Sécurité fonctionnelle des systèmes électriques / électroniques / électroniques programmables relatifs à la sécurité – Partie 7: Présentation de techniques et mesures*

CEI 61784-3, *Industrial communication networks – Profiles – Part 3: Functional safety fieldbuses – General rules and profile definitions* (disponible en anglais seulement)

CEI 62280-1, *Applications ferroviaires – Systèmes de signalisation, de télécommunication et de traitement – Partie 1: Communication de sécurité sur des systèmes de transmission fermés*

CEI 62280-2, *Applications ferroviaires – Systèmes de signalisation, de télécommunication et de traitement – Partie 2: Communication de sécurité sur des systèmes de transmission ouverts*

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*

EN 50205, *Relais de tout ou rien à contacts guidés (liés)*