IEC 61508-6

Edition 2.0 2010-04

INTERNATIONAL STANDARD

NORME INTERNATIONALE

Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3

Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 6: Lignes directrices pour l'application de la CEI 61508-2 et de la CEI 61508-3

INTERNATIONAL ELECTROTECHNICAL COMMISSION

COMMISSION ELECTROTECHNIQUE INTERNATIONALE

PRICE CODE
CODE PRIX XE

ICS 25.040.40

ISBN 978-2-88910-529-8

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

CONTENTS

FOREWORD 6
INTRODUCTION 8
1 Scope 10
2 Normative references 12
3 Definitions and abbreviations 12
Annex A (informative) Application of IEC 61508-2 and of IEC 61508-3 13
Annex B (informative) Example of technique for evaluating probabilities of hardware failure 21
Annex C (informative) Calculation of diagnostic coverage and safe failure fraction – worked example 76
Annex D (informative) A methodology for quantifying the effect of hardware-related common cause failures in E/E/PE systems 80
Annex E (informative) Example applications of software safety integrity tables of IEC 61508-3 95
Bibliography 110

Figure 1 – Overall framework of the IEC 61508 series 11
Figure A.1 – Application of IEC 61508-2 17
Figure A.2 – Application of IEC 61508-2 (Figure A.1 *continued*) 18
Figure A.3 – Application of IEC 61508-3 20
Figure B.1 – Reliability Block Diagram of a whole safety loop 22
Figure B.2 – Example configuration for two sensor channels 26
Figure B.3 – Subsystem structure 29
Figure B.4 – 1oo1 physical block diagram 30
Figure B.5 – 1oo1 reliability block diagram 31
Figure B.6 – 1oo2 physical block diagram 32
Figure B.7 – 1oo2 reliability block diagram 32
Figure B.8 – 2oo2 physical block diagram 33
Figure B.9 – 2oo2 reliability block diagram 33
Figure B.10 – 1oo2D physical block diagram 33
Figure B.11 – 1oo2D reliability block diagram 34
Figure B.12 – 2oo3 physical block diagram 34
Figure B.13 – 2oo3 reliability block diagram 35
Figure B.14 – Architecture of an example for low demand mode of operation 40
Figure B.15 – Architecture of an example for high demand or continuous mode of operation 49
Figure B.16 – Reliability block diagram of a simple whole loop with sensors organised into 2oo3 logic 51
Figure B.17 – Simple fault tree equivalent to the reliability block diagram presented on Figure B.1 52
Figure B.18 – Equivalence fault tree / reliability block diagram 52
Figure B.19 – Instantaneous unavailability *U(t)* of single periodically tested components 54
Figure B.20 – Principle of PFD_{avg} calculations when using fault trees 55

Figure B.21 – Effect of staggering the tests 56
Figure B.22 – Example of complex testing pattern 56
Figure B.23 – Markov graph modelling the behaviour of a two component system 58
Figure B.24 – Principle of the multiphase Markovian modelling 59
Figure B.25 – Saw-tooth curve obtained by multiphase Markovian approach 60
Figure B.26 – Approximated Markovian model 60
Figure B.27 – Impact of failures due to the demand itself 61
Figure B.28 – Modelling of the impact of test duration 61
Figure B.29 – Multiphase Markovian model with both DD and DU failures 62
Figure B.30 – Changing logic (2oo3 to 1oo2) instead of repairing first failure 63
Figure B.31 – "Reliability" Markov graphs with an absorbing state 63
Figure B.32 – "Availability" Markov graphs without absorbing states 65
Figure B.33 – Petri net for modelling a single periodically tested component 66
Figure B.34 – Petri net to model common cause failure and repair resources 69
Figure B.35 – Using reliability block diagrams to build Petri net and auxiliary Petri net for *PFD* and *PFH* calculations 70
Figure B.36 – Simple Petri net for a single component with revealed failures and repairs 71
Figure B.37 – Example of functional and dysfunctional modelling with a formal language 72
Figure B.38 – Uncertainty propagation principle 73
Figure D.1 – Relationship of common cause failures to the failures of individual channels 82
Figure D.2 – Implementing shock model with fault trees 93

Table B.1 – Terms and their ranges used in this annex (applies to 1oo1, 1oo2, 2oo2, 1oo2D, 1oo3 and 2oo3) 27
Table B.2 – Average probability of failure on demand for a proof test interval of six months and a mean time to restoration of 8 h 36
Table B.3 – Average probability of failure on demand for a proof test interval of one year and mean time to restoration of 8 h 37
Table B.4 – Average probability of failure on demand for a proof test interval of two years and a mean time to restoration of 8 h 38
Table B.5 – Average probability of failure on demand for a proof test interval of ten years and a mean time to restoration of 8 h 39
Table B.6 – Average probability of failure on demand for the sensor subsystem in the example for low demand mode of operation (one year proof test interval and 8 h *MTTR*) 40
Table B.7 – Average probability of failure on demand for the logic subsystem in the example for low demand mode of operation (one year proof test interval and 8 h *MTTR*) 41
Table B.8 – Average probability of failure on demand for the final element subsystem in the example for low demand mode of operation (one year proof test interval and 8 h *MTTR*) 41
Table B.9 – Example for a non-perfect proof test 42
Table B.10 – Average frequency of a dangerous failure (in high demand or continuous mode of operation) for a proof test interval of one month and a mean time to restoration of 8 h 45

Table B.11 – Average frequency of a dangerous failure (in high demand or continuous mode of operation) for a proof test interval of three month and a mean time to restoration of 8 h 46

Table B.12 – Average frequency of a dangerous failure (in high demand or continuous mode of operation) for a proof test interval of six month and a mean time to restoration of 8 h ..... **Error! Bookmark not defined.**

Table B.13 – Average frequency of a dangerous failure (in high demand or continuous mode of operation) for a proof test interval of one year and a mean time to restoration of 8 h ..... **Error! Bookmark not defined.**

Table B.14 – Average frequency of a dangerous failure for the sensor subsystem in the example for high demand or continuous mode of operation (six month proof test interval and 8 h *MTTR*) 49

Table B.15 – Average frequency of a dangerous failure for the logic subsystem in the example for high demand or continuous mode of operation (six month proof test interval and 8 h *MTTR*) 50

Table B.16 – Average frequency of a dangerous failure for the final element subsystem in the example for high demand or continuous mode of operation (six month proof test interval and 8 h *MTTR*) 50

Table C.1 – Example calculations for diagnostic coverage and safe failure fraction 78

Table C.2 – Diagnostic coverage and effectiveness for different elements 79

Table D.1 – Scoring programmable electronics or sensors/final elements 88

Table D.2 – Value of *Z* – programmable electronics 89

Table D.3 – Value of *Z* – sensors or final elements 89

Table D.4 – Calculation of β_{int} or $\beta_{\text{D int}}$ 90

Table D.5 – Calculation of β for systems with levels of redundancy greater than 1oo2 91

Table D.6 – Example values for programmable electronics 92

Table E.1 – Software safety requirements specification 96

Table E.2 – Software design and development – software architecture design 97

Table E.3 – Software design and development – support tools and programming language 98

Table E.4 – Software design and development – detailed design 99

Table E.5 – Software design and development – software module testing and integration 100

Table E.6 – Programmable electronics integration (hardware and software) 100

Table E.7 – Software aspects of system safety validation 101

Table E.8 – Modification 101

Table E.9 – Software verification 102

Table E.10 – Functional safety assessment 102

Table E.11 – Software safety requirements specification 104

Table E.12 – Software design and development – software architecture design 104

Table E.13 – Software design and development – support tools and programming language 105

Table E.14 – Software design and development – detailed design 106

Table E.15 – Software design and development – software module testing and integration 106

Table E.16 – Programmable electronics integration (hardware and software) 107

Table E.17 – Software aspects of system safety validation 108

Table E.18 – Modification 108

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

INTERNATIONAL ELECTROTECHNICAL COMMISSION

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

Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3

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 61508-6 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.

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

FDIS	Report on voting
65A/553/FDIS	65A/577/RVD

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

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

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

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

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

INTRODUCTION

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

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

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;

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

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

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

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

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

Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3

1 Scope

1.1 This part of IEC 61508 contains information and guidelines on IEC 61508-2 and IEC 61508-3.

- Annex A gives a brief overview of the requirements of IEC 61508-2 and IEC 61508-3 and sets out the functional steps in their application.
- Annex B gives an example technique for calculating the probabilities of hardware failure and should be read in conjunction with 7.4.3 and Annex C of IEC 61508-2 and Annex D.
- Annex C gives a worked example of calculating diagnostic coverage and should be read in conjunction with Annex C of IEC 61508-2.
- Annex D gives a methodology for quantifying the effect of hardware-related common cause failures on the probability of failure.
- Annex E gives worked examples of the application of the software safety integrity tables specified in Annex A of IEC 61508-3 for safety integrity levels 2 and 3.

1.2 IEC 61508-1, IEC 61508-2, IEC 61508-3 and IEC 61508-4 are basic safety publications, although this status does not apply in the context of low complexity E/E/PE safety-related systems (see 3.4.3 of IEC 61508-4). As basic safety publications, they are intended for use by technical committees in the preparation of standards in accordance with the principles contained in IEC Guide 104 and ISO/IEC Guide 51. IEC 61508-1, IEC 61508-2, IEC 61508-3 and IEC 61508-4 are also intended for use as stand-alone publications. The horizontal safety function of this international standard does not apply to medical equipment in compliance with the IEC 60601 series.

1.3 One of the responsibilities of a technical committee is, wherever applicable, to make use of basic safety publications in the preparation of its publications. In this context, the requirements, test methods or test conditions of this basic safety publication will not apply unless specifically referred to or included in the publications prepared by those technical committees.

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

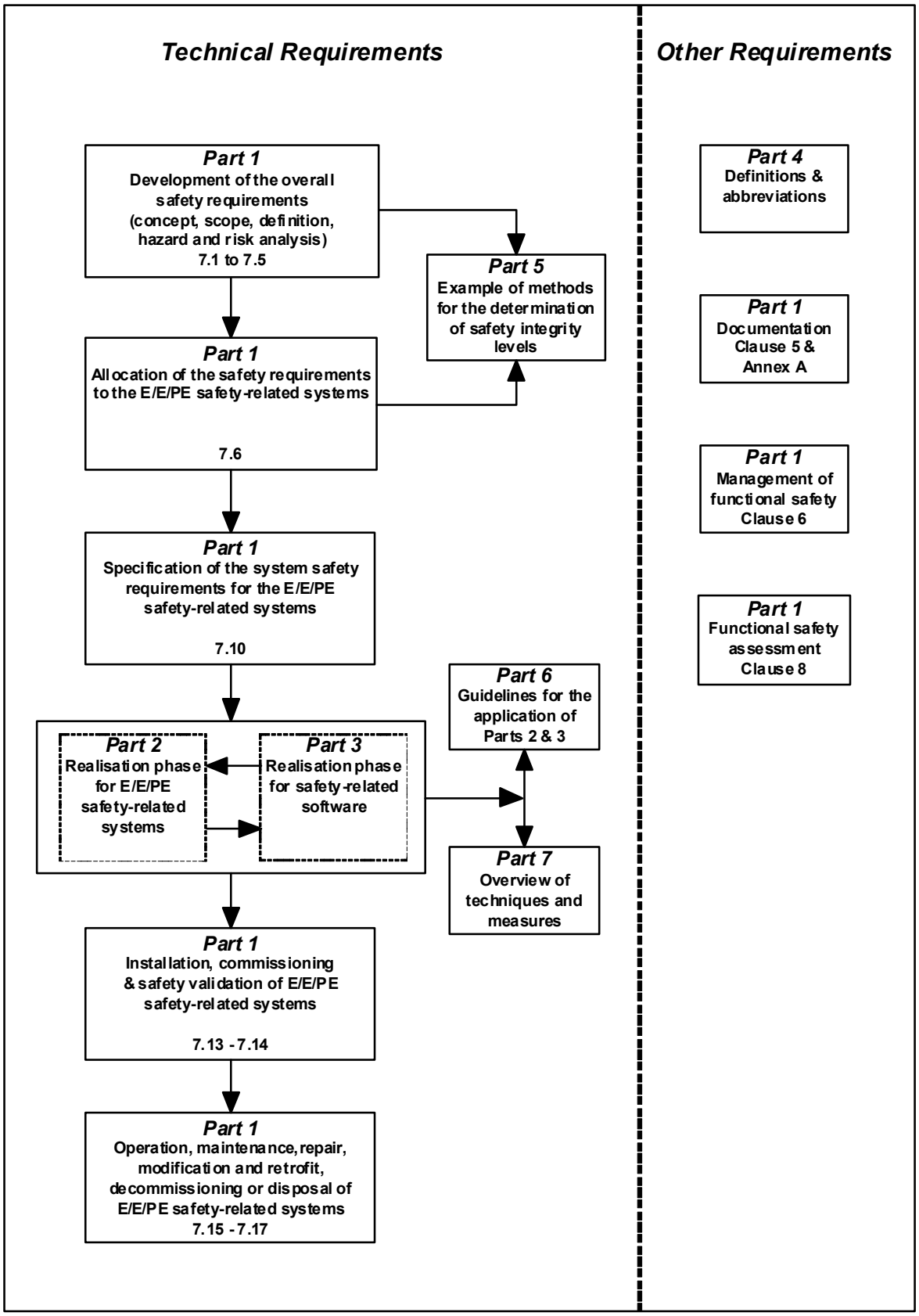


Figure 1 – Overall framework of the IEC 61508 series

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

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

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

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

SOMMAIRE

AVANT-PROPOS 116
INTRODUCTION 118
1 Domaine d'application 120
2 Références normatives 122
3 Définitions et abréviations 122
Annexe A (informative) Application de la CEI 61508-2 et de la CEI 61508-3 123
Annexe B (informative) Exemple de technique permettant d'évaluer les probabilités de défaillance du matériel 132
Annexe C (informative) Calcul de la couverture de diagnostic et de la proportion de défaillance en sécurité – exemple élaboré 193
Annexe D (informative) Méthodologie permettant de quantifier l'effet des défaillances de cause commune du matériel dans des systèmes E/E/PE 197
Annexe E (informative) Exemples d'application des tableaux d'intégrité de sécurité logicielle contenus dans la CEI 61508-3 214
Bibliographie 233

Figure 1 – Structure générale de la série CEI 61508 121
Figure A.1 – Application de la CEI 61508-2 128
Figure A.2 – Application de la CEI 61508-2 (Figure A.1 *suite*) 129
Figure A.3 – Application de la CEI 61508-3 131
Figure B.1 – Diagramme de fiabilité d'une boucle de sécurité complète 133
Figure B.2 – Exemple de configuration pour deux canaux de capteurs 138
Figure B.3 – Structure du sous-système 141
Figure B.4 – Diagramme du bloc physique 1oo1 142
Figure B.5 – Diagramme de fiabilité 1oo1 143
Figure B.6 – Diagramme du bloc physique 1oo2 144
Figure B.7 – Diagramme de fiabilité 1oo2 144
Figure B.8 – Diagramme du bloc physique 2oo2 145
Figure B.9 – Diagramme de fiabilité 2oo2 145
Figure B.10 – Diagramme du bloc physique 1oo2D 145
Figure B.11 – Diagramme de fiabilité 1oo2D 146
Figure B.12 – Diagramme du bloc physique 2oo3 146
Figure B.13 – Diagramme de fiabilité 2oo3 147
Figure B.14 – Architecture d'un exemple de fonctionnement en mode faible sollicitation 154
Figure B.15 – Architecture d'un exemple de fonctionnement en mode sollicitation élevée ou continu 164
Figure B.16 – Diagramme de fiabilité d'une boucle complète simple avec capteurs fonctionnant en logique majoritaire 2oo3 166
Figure B.17 – Arbre de panne simple équivalent au diagramme de fiabilité présenté à la Figure B.1 167
Figure B.18 – Équivalence arbre de panne / diagramme de fiabilité 168
Figure B.19 – Indisponibilité instantanée *U(t)* de composants individuels soumis à essais périodiques 170
Figure B.20 – Principe des calculs de PFD_{avg} utilisant les arbres de panne 171

Figure B.21 – Effet du décalage des essais 172
Figure B.22 – Exemple de modèle d'essai complexe 172
Figure B.23 – Diagramme de Markov modélisant le comportement d'un système à deux composants 174
Figure B.24 – Principe de la modélisation de Markov multiphase 175
Figure B.25 – Courbe en dents de scie obtenue par l'approche de Markov multiphase 176
Figure B.26 – Approximation du modèle markovien 177
Figure B.27 – Effet des défaillances dues à la sollicitation même 177
Figure B.28 – Modélisation de l'effet de la durée d'essai 178
Figure B.29 – Modèle markovien multiphase avec des défaillances DD et DU 178
Figure B.30 – Changement de logique (2oo3 à 1oo2) au lieu de réparer une première défaillance 179
Figure B.31 – Diagrammes de Markov de « fiabilité » avec un état absorbant 180
Figure B.32 – Diagrammes de Markov de « disponibilité » sans état absorbant 181
Figure B.33 – Réseau de Pétri pour modélisation d'un composant simple soumis à essai périodique 183
Figure B.34 – Réseau de Pétri pour modélisation de défaillance de cause commune et des ressources de réparation 186
Figure B.35 – Utilisation des diagrammes de fiabilité pour construire le réseau de Pétri et le réseau de Pétri auxiliaire pour les calculs de *PFD* et de *PFH* 187
Figure B.36 – Réseau de Pétri simple pour un composant simple avec défaillances détectées et réparations 188
Figure B.37 – Exemple de modélisation fonctionnelle et dysfonctionnelle avec un langage formel 189
Figure B.38 – Principe de la propagation de l'incertitude 190
Figure D.1 – Relation entre défaillances de cause commune et défaillances propres à un canal 200
Figure D.2 – Mise en œuvre d'un modèle des chocs avec des arbres de panne 212

Tableau B.1 – Termes et ordre de grandeur des paramètres correspondants utilisés dans cette annexe (s'applique à 1oo1, 1oo2, 2oo2, 1oo2D, 1oo3 et 2oo3) 138
Tableau B.2 – Probabilité moyenne de non fonctionnement en cas de sollicitation pour un intervalle entre essais périodiques de six mois et une durée moyenne de rétablissement de 8 h 148
Tableau B.3 – Probabilité moyenne de non fonctionnement en cas de sollicitation pour un intervalle entre essais périodiques de un an et une durée moyenne de rétablissement de 8 h 150
Tableau B.4 – Probabilité moyenne de non fonctionnement en cas de sollicitation pour un intervalle entre essais périodiques de deux ans et une durée moyenne de rétablissement de 8 h 151
Tableau B.5 – Probabilité moyenne de non fonctionnement en cas de sollicitation pour un intervalle entre essais périodiques de dix ans et une durée moyenne de rétablissement de 8 h 153
Tableau B.6 – Probabilité moyenne de non fonctionnement en cas de sollicitation pour le sous-système capteur dans l'exemple de fonctionnement en mode faible sollicitation (intervalle entre essais périodiques d'un an et *MTTR* de 8 h) 155
Tableau B.7 – Probabilité moyenne de non fonctionnement en cas de sollicitation pour le sous-système logique de l'exemple de fonctionnement en mode faible sollicitation (intervalle entre essais périodiques d'un an et *MTTR* de 8 h) 155

Tableau B.8 – Probabilité moyenne de non fonctionnement en cas de sollicitation pour le sous-système élément final de l'exemple de fonctionnement en mode faible sollicitation (intervalle entre essais périodiques d'un an et durée *MTTR* de 8 h)..... 155

Tableau B.9 – Exemple d'un essai périodique imparfait 157

Tableau B.10 – Fréquence moyenne d'une défaillance dangereuse (en mode de fonctionnement sollicitation élevée ou continu) pour un intervalle entre essais périodiques d'un mois et une durée moyenne de rétablissement de 8 h..... 160

Tableau B.11 – Fréquence moyenne d'une défaillance dangereuse (en mode de fonctionnement sollicitation élevée ou continu) pour un intervalle entre essais périodiques de trois mois et une durée moyenne de rétablissement de 8 h..... 161

Tableau B.12 – Fréquence moyenne d'une défaillance dangereuse (en mode de fonctionnement sollicitation élevée ou continu) pour un intervalle entre essais périodiques de six mois et une durée moyenne de rétablissement de 8 h 162

Tableau B.13 – Fréquence moyenne d'une défaillance dangereuse (en mode de fonctionnement sollicitation élevée ou continu) pour un intervalle entre essais périodiques d'un an et une durée moyenne de rétablissement de 8 h 163

Tableau B.14 – Fréquence moyenne d'une défaillance dangereuse du sous-système capteur dans l'exemple de mode de fonctionnement sollicitation élevée ou continu (intervalle entre essais périodiques de six mois et *MTTR* de 8 h) 164

Tableau B.15 – Fréquence moyenne d'une défaillance dangereuse du sous-système logique dans l'exemple de mode de fonctionnement sollicitation élevée ou continu (intervalle entre essais périodiques de six mois et *MTTR* de 8 h) 165

Tableau B.16 – Fréquence moyenne d'une défaillance dangereuse du sous-système élément final dans l'exemple de mode de fonctionnement sollicitation élevée ou continu (intervalle entre essais périodiques de six mois et *MTTR* de 8 h) 165

Tableau C.1 – Exemples de calcul de la couverture de diagnostic et de la proportion de défaillances en sécurité..... 195

Tableau C.2 – Couverture de diagnostic et efficacité pour différents éléments 196

Tableau D.1 – Calcul des résultats électroniques programmables ou des capteurs/éléments finaux 206

Tableau D.2 – Valeur de *Z* – électronique programmable..... 208

Tableau D.3 – Valeur de *Z* – capteurs ou éléments finaux..... 208

Tableau D.4 – Calcul de β_{int} ou de $\beta_{\text{D int}}$..... 209

Tableau D.5 – Calcul de β pour des systèmes à niveaux de redondance supérieurs à 1oo2 209

Tableau D.6 – Exemples de valeurs pour l'électronique programmable 210

Tableau E.1 – Spécification des exigences pour la sécurité du logiciel..... 215

Tableau E.2 – Conception et développement du logiciel – conception de l'architecture du logiciel 216

Tableau E.3 – Conception et développement du logiciel – outils de support et langages de programmation..... 217

Tableau E.4 – Conception et développement du logiciel – conception détaillée 218

Tableau E.5 – Conception et développement du logiciel – essai et intégration des modules logiciels..... 219

Tableau E.6 – Intégration de l'électronique programmable (matériel et logiciel)..... 220

Tableau E.7 – Validation de sécurité du logiciel 220

Tableau E.8 – Modification du logiciel..... 221

Tableau E.9 – Vérification du logiciel..... 222

Tableau E.10 – Evaluation de la sécurité fonctionnelle..... 223

Tableau E.11 – Spécification des exigences pour la sécurité du logiciel 224

Tableau E.12 – Conception et développement du logiciel – conception de l'architecture du logiciel 225
Tableau E.13 – Conception et développement du logiciel – outils de support et langage de programmation 226
Tableau E.14 – Conception et développement du logiciel – conception détaillée 227
Tableau E.15 – Conception et développement du logiciel – essai et intégration des modules logiciels 228
Tableau E.16 – Intégration de l'électronique programmable (matériel et logiciel) 229
Tableau E.17 – Validation de sécurité du logiciel 229
Tableau E.18 – Modification du logiciel 230
Tableau E.19 – Vérification du logiciel 231
Tableau E.20 – Evaluation de la sécurité fonctionnelle 232

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

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

Partie 6: Lignes directrices pour l'application de la CEI 61508-2 et de la CEI 61508-3

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 61508-6 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

Le texte de cette norme est issu des documents suivants:

FDIS	Rapport de vote
65A/553/FDIS	65A/577/RVD

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

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

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

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

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

INTRODUCTION

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

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

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

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

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

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 6: Lignes directrices pour l'application de la CEI 61508-2 et de la CEI 61508-3

1 Domaine d'application

1.1 La présente partie de la CEI 61508 contient des informations et lignes directrices sur la CEI 61508-2 et la CEI 61508-3.

– L'Annexe A présente un bref aperçu des exigences de la CEI 61508-2 et de la CEI 61508-3 et établit les étapes fonctionnelles de leur application.

– L'Annexe B donne une technique servant d'exemple pour le calcul des probabilités de défaillance du matériel; il convient de la lire conjointement au 7.4.3 et à l'Annexe C de la CEI 61508-2, et à l'Annexe D.

– L'Annexe C donne un exemple élaboré de calcul de la couverture de diagnostic; il convient de la lire conjointement avec l'Annexe C de la CEI 61508-2.

– L'Annexe D donne une méthodologie de quantification de l'effet des défaillances de cause commune relatives au matériel sur la probabilité de défaillance.

– L'Annexe E donne des exemples d'application des tableaux d'intégrité de sécurité du logiciel spécifiés dans l'Annexe A de la CEI 61508-3 pour les niveaux 2 et 3 d'intégrité de sécurité.

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. La CEI 61508-2 est également destinée à être utilisée comme publication autonome. La fonction de sécurité horizontale de la présente norme internationale ne s'applique pas aux appareils médicaux conformes à la série CEI 60601.

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

1.4 La Figure 1 illustre la structure générale de la série CEI 61508 et montre le rôle que la CEI 61508-6 joue dans la réalisation de la sécurité fonctionnelle pour les systèmes E/E/PE relatifs à la sécurité.

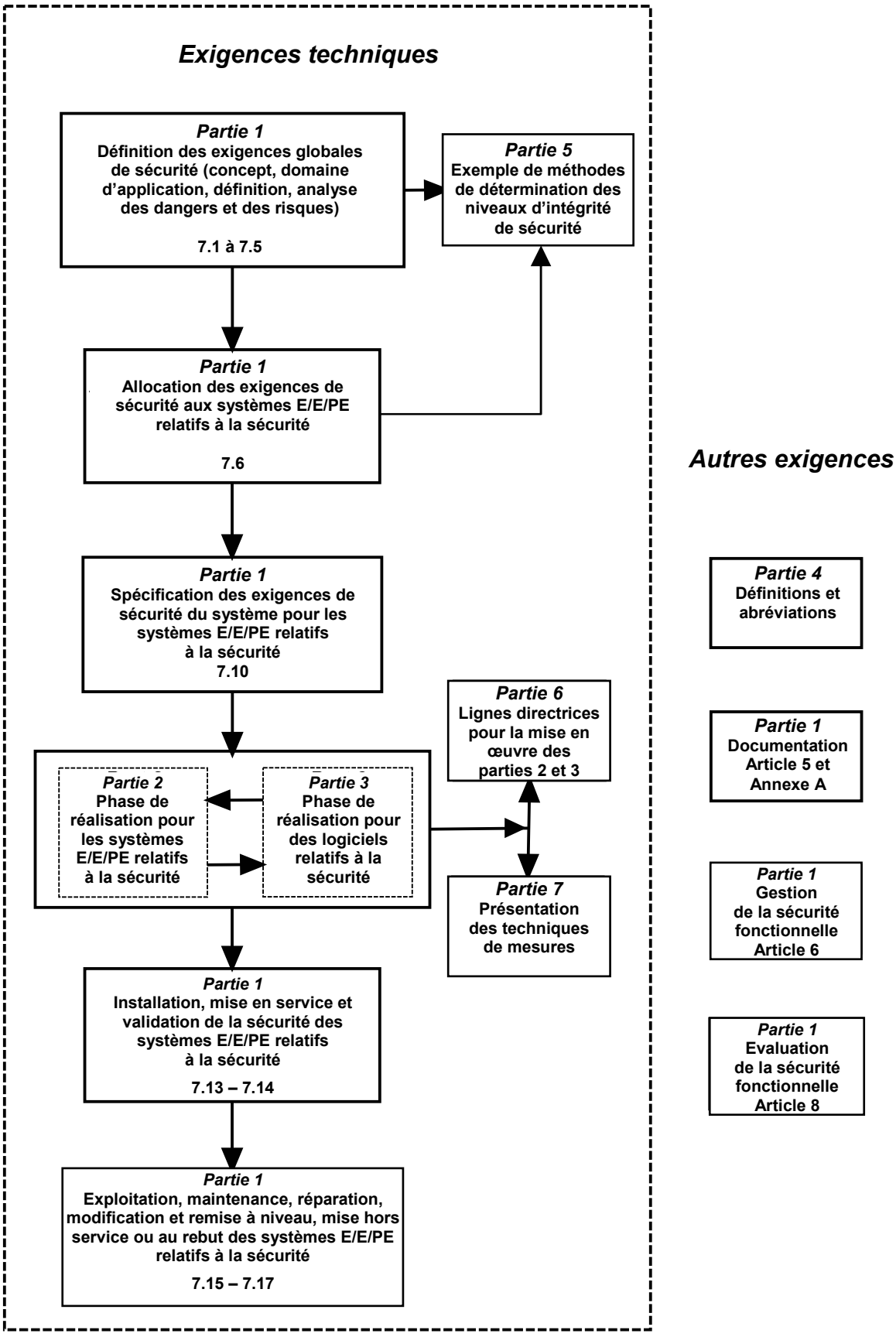


Figure 1 – Structure générale de la série CEI 61508

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*