

**NORME
INTERNATIONALE
INTERNATIONAL
STANDARD**

**CEI
IEC**

61508-6

Première édition
First edition
2000-04

**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**

**Functional safety of electrical/electronic/
programmable electronic safety-related systems –**

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



Numéro de référence
Reference number
CEI/IEC 61508-6:2000

Numéros des publications

Depuis le 1er janvier 1997, les publications de la CEI sont numérotées à partir de 60000.

Publications consolidées

Les versions consolidées de certaines publications de la CEI incorporant les amendements sont disponibles. Par exemple, les numéros d'édition 1.0, 1.1 et 1.2 indiquent respectivement la publication de base, la publication de base incorporant l'amendement 1, et la publication de base incorporant les amendements 1 et 2.

Validité de la présente publication

Le contenu technique des publications de la CEI est constamment revu par la CEI afin qu'il reflète l'état actuel de la technique.

Des renseignements relatifs à la date de reconfirmation de la publication sont disponibles dans le Catalogue de la CEI.

Les renseignements relatifs à des questions à l'étude et des travaux en cours entrepris par le comité technique qui a établi cette publication, ainsi que la liste des publications établies, se trouvent dans les documents ci-dessous:

- «Site web» de la CEI*
- **Catalogue des publications de la CEI**
Publié annuellement et mis à jour régulièrement
(Catalogue en ligne)*
- **Bulletin de la CEI**
Disponible à la fois au «site web» de la CEI* et comme périodique imprimé

Terminologie, symboles graphique et littéraux

En ce qui concerne la terminologie générale, le lecteur se reportera à la CEI 60050: *Vocabulaire Electrotechnique International (VEI)*.

Pour les symboles graphiques, les symboles littéraux et les signes d'usage général approuvés par la CEI, le lecteur consultera la CEI 60067: *Symboles littéraux à utiliser en électrotechnique*, la CEI 60417: *Symboles graphiques utilisés sur le matériel. Index, relevé et compilation des feuilles individuelles*, et la CEI 60617: *Symboles graphiques pour schémas*.

* Voir l'adresse «site web» sur la page de titre.

Numbering

As from 1 January 1997 all IEC publications are issued with a designation in the 60000 series.

Consolidated publications

Consolidated versions of some IEC publications including amendments are available. For example, edition numbers 1.0, 1.1 and 1.2 refer, respectively, to the base publication, the base publication incorporating amendment 1 and the base publication incorporating amendments 1 and 2.

Validity of this publication

The technical content of IEC publications is kept under constant review by the IEC, thus ensuring that the content reflects current technology.

Information relating to the date of the reconfirmation of the publication is available in the IEC catalogue.

Information on the subject under consideration and work in progress undertaken by the technical committee which has prepared this publication, as well as the list of publications issued, is to be found at the following IEC sources:

- **IEC web site***
- **Catalogue of IEC publications**
Published yearly with regular updates
(On-line catalogue)*
- **IEC Bulletin**
Available both at the IEC web site* and as a printed periodical

Terminology, graphical and letter symbols

For general terminology, readers are referred to IEC 60050: *International Electrotechnical Vocabulary (IEV)*.

For graphical symbols, and letter symbols and signs approved by the IEC for general use, readers are referred to publications IEC 60027: *Letter symbols to be used in electrical technology*, IEC 60417: *Graphical symbols for use on equipment. Index, survey and compilation of the single sheets* and IEC 60617: *Graphical symbols for diagrams*.

* See web site address on title page.

NORME
INTERNATIONALE
INTERNATIONAL
STANDARD

CEI
IEC

61508-6

Première édition
First edition
2000-04

**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**

**Functional safety of electrical/electronic/
programmable electronic safety-related systems –**

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

© IEC 2000 Droits de reproduction réservés — Copyright - all rights reserved

Aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie et les microfilms, sans l'accord écrit de l'éditeur.

No part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from the publisher.

International Electrotechnical Commission
Telefax: +41 22 919 0300

e-mail: inmail@iec.ch

3, rue de Varembe Geneva, Switzerland
IEC web site <http://www.iec.ch>



Commission Electrotechnique Internationale
International Electrotechnical Commission
Международная Электротехническая Комиссия

CODE PRIX
PRICE CODE XB

*Pour prix, voir catalogue en vigueur
For price, see current catalogue*

SOMMAIRE

	Pages
AVANT-PROPOS	10
INTRODUCTION	14
Articles	
1 Domaine d'application	18
2 Références normatives.....	22
3 Définitions et abréviations	22
Annexe A (informative) Application de la CEI 61508-2 et de la CEI 61508-3	24
A.1 Généralités	24
A.2 Etapes fonctionnelles dans l'application de la CEI 61508-2	28
A.3 Etapes fonctionnelles pour l'application de la CEI 61508-3.....	36
Annexe B (informative) Exemple de technique permettant d'évaluer les probabilités de défaillance du matériel.....	40
B.1 Généralités	40
B.2 Probabilité moyenne de défaillance sur demande (pour un mode de fonctionnement faible demande)	48
B.3 Probabilité de défaillance par heure (pour un mode de fonctionnement demande élevée ou continu).....	74
B.4 Références	90
Annexe C (informative) Calcul de la couverture du diagnostic et de la proportion de défaillance en sécurité: exemple élaboré.....	92
Annexe D (informative) Méthodologie permettant de quantifier l'effet des défaillances de cause commune du matériel dans des systèmes E/E/PE	100
D.1 Généralités	100
D.2 Présentation concise.....	100
D.3 Domaine d'application de la méthodologie	108
D.4 Eléments à prendre en compte dans la méthodologie	108
D.5 Utilisation du facteur β pour le calcul de probabilité de défaillance due à des défaillances de cause commune dans un système E/E/PE relatif à la sécurité.....	110
D.6 Utilisation des tables pour l'estimation de β	112
D.7 Exemples de l'utilisation de la méthodologie	120
D.8 Références	122
Annexe E (informative) Exemples d'application des tableaux d'intégrité de sécurité logiciel contenus dans la CEI 61508-3.....	124
E.1 Généralités	124
E.2 Exemple pour le niveau 2 d'intégrité de sécurité	124
E.3 Exemple pour le niveau 3 d'intégrité de sécurité	134
Bibliographie	144

CONTENTS

	Page
FOREWORD	11
INTRODUCTION	15
Clause	
1 Scope	19
2 Normative references	23
3 Definitions and abbreviations	23
Annex A (informative) Application of IEC 61508-2 and of IEC 61508-3	25
A.1 General	25
A.2 Functional steps in the application of IEC 61508-2	29
A.3 Functional steps in the application of IEC 61508-3	37
Annex B (informative) Example technique for evaluating probabilities of hardware failure ...	41
B.1 General	41
B.2 Average probability of failure on demand (for low demand mode of operation)	49
B.3 Probability of failure per hour (for high demand or continuous mode of operation)	75
B.4 References	91
Annex C (informative) Calculation of diagnostic coverage and safe failure fraction: worked example	93
Annex D (informative) A methodology for quantifying the effect of hardware-related common cause failures in E/E/PE systems	101
D.1 General	101
D.2 Brief overview	101
D.3 Scope of the methodology	109
D.4 Points taken into account in the methodology	109
D.5 Using the β -factor to calculate the probability of failure in an E/E/PE safety-related system due to common cause failures	111
D.6 Using the tables to estimate β	113
D.7 Examples of the use of the methodology	121
D.8 References	123
Annex E (informative) Example applications of software safety integrity tables of IEC 61508-3	125
E.1 General	125
E.2 Example for safety integrity level 2	125
E.3 Example for safety integrity level 3	135
Bibliography	145

	Pages
Figure 1 – Structure générale de la CEI 61508.....	20
Figure A.1 – Application de la CEI 61508-2.....	32
Figure A.2 – Application de la CEI 61508-2 (suite).....	34
Figure A.3 – Application de la CEI 61508-3.....	38
Figure B.1 – Exemple de configuration pour deux canaux de capteurs.....	44
Figure B.2 – Structure du sous-système.....	48
Figure B.3 – Diagramme du bloc physique 1oo1.....	50
Figure B.4 – Diagramme de fiabilité 1oo1.....	50
Figure B.5 – Diagramme du bloc physique 1oo2.....	52
Figure B.6 – Diagramme de fiabilité 1oo2.....	54
Figure B.7 – Diagramme du bloc physique 2oo2.....	54
Figure B.8 – Diagramme de fiabilité 2oo2.....	54
Figure B.9 – Diagramme du bloc physique 1oo2D.....	56
Figure B.10 – Diagramme de fiabilité 1oo2D.....	56
Figure B.11 – Diagramme du bloc physique 2oo3.....	58
Figure B.12 – Diagramme de fiabilité 2oo3.....	58
Figure B.13 – Architecture d'un exemple de fonctionnement en mode demande faible.....	68
Figure B.14 – Architecture d'un exemple pour un mode de fonctionnement en mode demande élevée ou continu.....	86
Figure D.1 – Relation entre défaillances de cause commune et défaillances de canaux individuels.....	104
Tableau B.1 – Termes et ordre de grandeur des paramètres correspondants utilisés dans cette annexe (s'applique à 1oo1, 1oo2, 2oo2, 1oo2D et 2oo3).....	46
Tableau B.2 – Probabilité moyenne de défaillance sur demande pour un intervalle entre tests périodiques de 6 mois et une durée moyenne de rétablissement de 8 h.....	60
Tableau B.3 – Probabilité moyenne de défaillance sur demande pour un intervalle entre tests périodiques de un an et une durée moyenne de rétablissement de 8 h.....	62
Tableau B.4 – Probabilité moyenne de défaillance sur demande pour un intervalle entre tests périodiques de deux ans et une durée moyenne de rétablissement de 8 h.....	64
Tableau B.5 – Probabilité moyenne de défaillance sur demande pour un intervalle entre tests périodiques de trois ans et une durée moyenne de rétablissement de 8 h.....	66
Tableau B.6 – Probabilité moyenne de défaillance sur demande pour le sous-système capteur dans l'exemple de fonctionnement en mode demande faible (intervalle entre tests périodiques d'un an et MTTR de 8 h).....	68
Tableau B.7 – Probabilité moyenne de défaillance sur demande pour le sous-système logique dans l'exemple de fonctionnement en mode demande faible (intervalle entre tests périodiques d'un an et MTTR de 8 h).....	70
Tableau B.8 – Probabilité moyenne de défaillance sur demande pour le sous-système élément final de l'exemple de fonctionnement en mode demande faible (intervalle entre tests périodiques d'un an et durée MTTR de 8 h).....	70

	Page
Figure 1 – Overall framework of IEC 61508	21
Figure A.1 – Application of IEC 61508-2	33
Figure A.2 – Application of IEC 61508-2 (continued)	35
Figure A.3 – Application of IEC 61508-3	39
Figure B.1 – Example configuration for two sensor channels	45
Figure B.2 – Subsystem structure	49
Figure B.3 – 1oo1 physical block diagram	51
Figure B.4 – 1oo1 reliability block diagram	51
Figure B.5 – 1oo2 physical block diagram	53
Figure B.6 – 1oo2 reliability block diagram	55
Figure B.7 – 2oo2 physical block diagram	55
Figure B.8 – 2oo2 reliability block diagram	55
Figure B.9 – 1oo2D physical block diagram	57
Figure B.10 – 1oo2D reliability block diagram	57
Figure B.11 – 2oo3 physical block diagram	59
Figure B.12 – 2oo3 reliability block diagram	59
Figure B.13 – Architecture of an example for low demand mode of operation	69
Figure B.14 – Architecture of an example for high demand or continuous mode of operation	87
Figure D.1 – Relationship of common cause failures to the failures of individual channels ..	105
Table B.1 – Terms and their ranges used in this annex (applies to 1oo1, 1oo2, 2oo2, 1oo2D and 2oo3)	47
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	61
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	63
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	65
Table B.5 – Average probability of failure on demand for a proof-test interval of 10 years and a mean time to restoration of 8 h	67
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)	69
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)	71
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)	71

	Pages
Tableau B.9 – Exemple d'un test périodique imparfait	74
Tableau B.10 – Probabilité de défaillance par heure (en mode de fonctionnement demande élevée ou continu) pour un intervalle entre tests périodiques d'un mois et une durée moyenne de rétablissement de 8 h.....	78
Tableau B.11 – Probabilité de défaillance par heure (en mode de fonctionnement demande élevée ou continu) pour un intervalle entre tests périodiques de trois mois et une durée moyenne de rétablissement de 8 h.....	80
Tableau B.12 – Probabilité de défaillance par heure (en mode de fonctionnement demande élevée ou continu) pour un intervalle entre tests périodiques de six mois et une durée moyenne de rétablissement de 8 h.....	82
Tableau B.13 – Probabilité de défaillance par heure (en mode de fonctionnement demande élevée ou continu) pour un intervalle entre tests périodiques d'un an et une durée moyenne de rétablissement de 8 h.....	84
Tableau B.14 – Probabilité de défaillance par heure du sous-système capteur dans l'exemple de mode de fonctionnement demande élevée ou continu (intervalle entre tests périodiques de six mois et MTTR de 8 h)	86
Tableau B.15 – Probabilité de défaillance par heure du sous-système logique dans l'exemple de mode de fonctionnement demande élevée ou continu (intervalle entre tests périodiques de six mois et MTTR de 8 h)	88
Tableau B.16 – Probabilité de défaillance par heure du sous-système élément final dans l'exemple de mode de fonctionnement demande élevée ou continu (intervalle entre tests périodiques de six mois et MTTR de 8 h)	88
Tableau C.1 – Exemples de calcul de la couverture du diagnostic et de la proportion de défaillances en sécurité	96
Tableau C.2 – Couverture du diagnostic et efficacité pour différents sous-systèmes.....	98
Tableau D.1 – Calcul des résultats électroniques programmables ou des capteurs/éléments terminaux.....	114
Tableau D.2 – Valeur de Z: électronique programmable	118
Tableau D.3 – Valeur de Z: capteurs et éléments terminaux.....	118
Tableau D.4 – Calcul de β ou de ρ	120
Tableau D.5 – Exemples de valeurs pour l'électronique programmable.....	122
Tableau E.1 – Spécification et prescriptions de sécurité (voir 7.2 de la CEI 61508-3).....	126
Tableau E.2 – Conception et réalisation du logiciel: conception de l'architecture du logiciel (voir 7.4.3 de la CEI 61508-3).....	128
Tableau E.3 – Conception et réalisation du logiciel: outils supports et langages de programmation (voir 7.4.4 de la CEI 61508-3).....	128
Tableau E.4 – Conception et réalisation du logiciel: conception détaillée (voir 7.4.5 et 7.4.6 de la CEI 61508-3) (cela comprend la conception du système logiciel, la conception des modules logiciels et le codage).....	130
Tableau E.5 – Conception et réalisation du logiciel: test des modules logiciels et intégration (voir 7.4.7 et 7.4.8 de la CEI 61508-3)	130
Tableau E.6 – Intégration de l'électronique programmable (matériel et logiciel) (voir 7.5 de la CEI 61508-3)	130
Tableau E.7 – Validation de sécurité du logiciel (voir 7.7 de la CEI 61508-3)	132
Tableau E.8 – Modification du logiciel (voir 7.8 de la CEI 61508-3).....	132
Tableau E.9 – Vérification du logiciel (voir 7.9 de la CEI 61508-3).....	132
Tableau E.10 – Evaluation de la sécurité fonctionnelle (voir article 8 de la CEI 61508-3)	134

Table B.9 – Example for a non-perfect proof test.....	75
Table B.10 – Probability of failure per hour (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.....	79
Table B.11 – Probability of failure per hour (in high demand or continuous mode of operation) for a proof test interval of three months and a mean time to restoration of 8 h.....	81
Table B.12 – Probability of failure per hour (in high demand or continuous mode of operation) for a proof test interval of six months and a mean time to restoration of 8 h.....	83
Table B.13 – Probability of failure per hour (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.....	85
Table B.14 – Probability of failure per hour for the sensor subsystem in the example for high demand or continuous mode of operation (six month proof-test interval and 8 h MTTR).....	87
Table B.15 – Probability of failure per hour for the logic subsystem in the example for high demand or continuous mode of operation (six month proof-test interval and 8 h MTTR).....	89
Table B.16 – Probability of failure per hour 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).....	89
Table C.1 – Example calculations for diagnostic coverage and safe failure fraction.....	97
Table C.2 – Diagnostic coverage and effectiveness for different subsystems.....	99
Table D.1 – Scoring programmable electronics or sensors/ final elements.....	115
Table D.2 – Value of Z: programmable electronics.....	119
Table D.3 – Value of Z: sensors or final elements.....	119
Table D.4 – Calculation of β or β_D	121
Table D.5 – Example values for programmable electronics.....	123
Table E.1 – Software safety requirements specification (see 7.2 of IEC 61508-3).....	127
Table E.2 – Software design and development: software architecture design (see 7.4.3 of IEC 61508-3).....	129
Table E.3 – Software design and development: support tools and programming language (see 7.4.4 of IEC 61508-3).....	129
Table E.4 – Software design and development: detailed design (see 7.4.5 and 7.4.6 of IEC 61508-3) (this includes software system design, software module design and coding).....	131
Table E.5 – Software design and development: software module testing and integration (see 7.4.7 and 7.4.8 of IEC 61508-3).....	131
Table E.6 – Programmable electronics integration (hardware and software) (see 7.5 of IEC 61508-3).....	131
Table E.7 – Software safety validation (see 7.7 of IEC 61508-3).....	133
Table E.8 – Software modification (see 7.8 of IEC 61508-3).....	133
Table E.9 – Software verification (see 7.9 of part 3).....	133
Table E.10 – Functional safety assessment (see clause 8 of IEC 61508-3).....	135

	Pages
Tableau E.11 – Spécification des prescriptions de sécurité du logiciel (voir 7.2 de la CEI 61508-3)	136
Tableau E.12 – Conception et réalisation du logiciel: conception de l'architecture du logiciel (voir 7.4.3 de la CEI 61508-3).....	136
Tableau E.13 – Conception et réalisation du logiciel: outils supports et langages de programmation (voir 7.4.4 de la CEI 61508-3)	138
Tableau E.14 – Conception et réalisation du logiciel: conception détaillée (voir 7.4.5 et 7.4.6 de la CEI 61508-3) (cela comprend la conception du système logiciel, la conception des modules logiciels et le codage)	138
Tableau E.15 – Conception et réalisation du logiciel: test des modules logiciels et intégration (voir 7.4.7 et 7.4.8 de la CEI 61508-3)	140
Tableau E.16 – Intégration de l'électronique programmable (matériel et logiciel) (voir 7.5 de la CEI 61508-3)	140
Tableau E.17 – Validation de sécurité du logiciel (voir 7.7 de la CEI 61508-3)	140
Tableau E.18 – Modification du logiciel (voir 7.8 de la CEI 61508-3)	142
Tableau E.19 – Vérification du logiciel (voir 7.9 de la CEI 61508-3)	142
Tableau E.20 – Evaluation de la sécurité fonctionnelle (voir article 8 de la CEI 61508-3)	142

currently in preview, click buy full vers.

	Page
Table E.11 – Software safety requirements specification (see 7.2 of IEC 61508-3).....	137
Table E.12 – Software design and development: software architecture design (see 7.4.3 of IEC 61508-3).....	137
Table E.13 – Software design and development: support tools and programming language (see 7.4.4 of IEC 61508-3)	139
Table E.14 – Software design and development: detailed design (see 7.4.5 and 7.4.6 of IEC 61508-3) (this includes software system design, software module design and coding)	139
Table E.15 – Software design and development: software module testing and integration (see 7.4.7 and 7.4.8 of IEC 61508-3).....	141
Table E.16 – Programmable electronics integration (hardware and software) (see 7.5 of IEC 61508-3).....	141
Table E.17 – Software safety validation (see 7.7 of IEC 61508-3).....	141
Table E.18 – Modification (see 7.8 of IEC 61508-3).....	143
Table E.19 – Software verification (see 7.9 of IEC 61508-3).....	143
Table E.20 – Functional safety assessment (see clause 8 of IEC 61508-3)	143

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 CEI (Commission Electrotechnique Internationale) est une organisation internationale de normalisation composée de tous les comités électrotechniques nationaux (Comités nationaux de la CEI). La CEI a pour but de promouvoir la coopération internationale en matière de normalisation dans les domaines de l'électricité et de l'électronique. A cette fin et en plus d'autres activités, la CEI publie des Normes internationales. Leur préparation est confiée aux comités d'études; il est permis à tout Comité national intéressé par le sujet traité de participer à ces travaux préparatoires. Les organisations internationales, gouvernementales et non gouvernementales qui assurent la liaison avec la CEI participent également à cette préparation. La CEI travaille en collaboration étroite avec l'Organisation internationale de normalisation (ISO), conformément aux conditions de l'accord passé 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 intéressés sont représentés dans chaque comité d'études.
- 3) Les documents produits se présentent sous la forme de recommandations internationales. Ils sont publiés comme normes, spécifications techniques, rapports techniques ou guides et agréés comme tels par les Comités nationaux.
- 4) Dans le but d'encourager l'unification internationale, les Comités nationaux de la CEI s'engagent à appliquer de façon transparente, dans toute la mesure du possible, les Normes internationales de la CEI dans leurs normes nationales et régionales. Toute divergence entre la norme de la CEI et la norme nationale ou régionale correspondante doit être indiquée en termes clairs dans cette dernière.
- 5) La CEI n'a fixé aucune procédure concernant le marquage comme indication d'approbation et sa responsabilité n'est pas engagée quand un matériel est déclaré conforme à l'une de ses normes.
- 6) L'attention est attirée sur le fait que certains éléments de la présente Norme internationale 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 et commande dans les processus industriels.

Le texte de cette norme est issu des documents suivants:

FDIS	Rapport de vote
65A/295/FDIS	65A/304/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 3.

Les annexes A à E sont données uniquement à titre d'information.

La CEI 61508 est composée des parties suivantes, regroupées sous le titre général *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité*:

- Partie 1: Prescriptions générales
- Partie 2: Prescriptions pour les systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité

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 IEC (International Electrotechnical Commission) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of the 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, the IEC publishes International Standards. 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. The 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 the 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 National Committees.
- 3) The documents produced have the form of recommendations for international use and are published in the form of standards, technical specifications, technical reports or guides and they are accepted by the National Committees in that sense.
- 4) In order to promote international unification, IEC National Committees undertake to apply IEC International Standards transparently to the maximum extent possible in their national and regional standards. Any divergence between the IEC Standard and the corresponding national or regional standard shall be clearly indicated in the latter.
- 5) The IEC provides no marking procedure to indicate its approval and cannot be rendered responsible for any equipment declared to be in conformity with one of its standards.
- 6) Attention is drawn to the possibility that some of the elements of this International Standard may be the subject of patent rights. The IEC shall not be held responsible for identifying any or all such patent rights.

IEC 61508-6 has been prepared by subcommittee 65A: System aspects, of IEC technical committee 65: Industrial-process measurement and control.

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

FDIS	Report on voting
65A/295/FDIS	65A/304/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 3.

Annexes A to E are for information only.

IEC 61508 consists of the following parts, under the general title *Functional safety of electrical/electronic/programmable electronic safety-related systems*:

- Part 1: General requirements
- Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems

- Partie 3: Prescriptions concernant les logiciels
- Partie 4: Définitions et abréviations
- Partie 5: Exemples de méthodes pour la détermination des niveaux d'intégrité de sécurité
- Partie 6: Lignes directrices pour l'application de la CEI 61508-2 et la CEI 61508-3
- Partie 7: Présentation de techniques et mesures

Le comité a décidé que le contenu de cette publication ne sera pas modifié avant 2005. A cette date, la publication sera

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

- Part 3: Software requirements
- Part 4: Definitions and abbreviations
- Part 5: Examples of methods for the determination of safety integrity levels
- Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3
- Part 7: Overview of techniques and measures

The committee has decided that the contents of this publication will remain unchanged until 2005. At this date, the publication will be

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

INTRODUCTION

Les systèmes électriques/électroniques sont utilisés depuis des années pour exécuter des fonctions liées à la sécurité dans la plupart des secteurs d'application. Des systèmes à base d'informatique (que l'on nommera de façon générique «systèmes électroniques programmables (PES)» sont utilisés dans tous les secteurs d'application pour exécuter des fonctions non liées à la sécurité, mais aussi de plus en plus souvent liées 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 liés 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/électroniques/électroniques programmables (E/E/PES) 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 appareils électriques liés à la sécurité. L'un des principaux objectifs poursuivis consiste à faciliter l'élaboration de normes par secteur d'application.

Dans la plupart des cas, la sécurité est obtenue par un certain nombre de systèmes de protection fondés sur diverses technologies (par exemple mécanique, hydraulique, pneumatique, électrique, électronique, électronique programmable). En conséquence, il est nécessaire que toute stratégie de sécurité prenne non seulement en compte tous les éléments d'un système individuel (par exemple les capteurs, les appareils de commande, les actionneurs), mais aussi qu'elle considère tous les systèmes relatifs à la sécurité comme des éléments individuels d'un ensemble complexe. C'est pourquoi la présente Norme internationale, bien que traitant essentiellement des systèmes E/E/PE relatifs à la sécurité, fournit néanmoins un cadre de sécurité susceptible de concerner les systèmes relatifs à la sécurité basés sur d'autres technologies.

Personne n'ignore la grande variété des applications E/E/PES. Celles-ci recouvrent, à des degrés de complexité très divers, un fort potentiel de danger et de risques dans tous les secteurs d'application. Pour chaque application, la nature exacte des mesures de sécurité envisagées dépend de plusieurs facteurs propres à l'application. La présente Norme internationale, de par son caractère général, rend désormais possible la prescription de ces mesures dans des normes internationales par secteur d'application.

La présente Norme internationale

- concerne toutes les phases appropriées du cycle de vie de sécurité global des E/E/PES et du logiciel (depuis la conceptualisation initiale, en passant par la conception, l'installation, l'exploitation et la maintenance, jusqu'à la mise hors service) lorsque les E/E/PES exécutent des fonctions de sécurité;
- a été élaborée dans le souci de l'évolution rapide des technologies – le cadre est suffisamment solide et étendu pour pourvoir aux évolutions futures;
- permet l'élaboration de normes internationales par secteur d'application concernant les E/E/PES relatifs à la sécurité. L'élaboration de normes internationales par secteur d'application à partir de la présente Norme internationale devrait permettre 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 est une amélioration en termes de sécurité et de bénéfices économiques;
- fournit une méthode de développement des prescriptions de sécurité nécessaires pour réaliser la sécurité fonctionnelle des systèmes E/E/PE relatifs à la sécurité;
- utilise des niveaux d'intégrité de sécurité afin de spécifier les niveaux cibles d'intégrité de sécurité des fonctions de sécurité devant être réalisées par les systèmes E/E/PE relatifs à la sécurité;

INTRODUCTION

Systems comprised of electrical and/or electronic components have been used for many years to perform safety functions in most application sectors. Computer-based systems (generically referred to as programmable electronic systems (PESs)) 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 those 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 components (electrical/ electronic/programmable electronic systems (E/E/PESs)) 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 application sector standards.

In most situations, safety is achieved by a number of protective 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 electrical/ electronic/programmable electronic (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 E/E/PES applications in a variety of application sectors and covering a wide range of complexity, hazard and risk potentials. In any particular application, the exact prescription of safety measures is dependent on many factors specific to the application. This International Standard, by being generic, will enable such a prescription to be formulated in future application sector international standards.

This International Standard

- considers all relevant overall, E/E/PES and software safety lifecycle phases (for example, from initial concept, through design, implementation, operation and maintenance to decommissioning) when E/E/PESs 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 application sector international standards, dealing with safety-related E/E/PESs, to be developed; the development of application sector international standards, within the framework of this International 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;
- uses 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;

- adopte une approche basée sur le risque encouru pour déterminer les niveaux d'intégrité de sécurité prescrits;
- fixe des objectifs quantitatifs pour les mesures de défaillances des 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 mesures de défaillances, dans le cas d'un mode de défaillance dangereux, cette limite pouvant être exigée pour un système E/E/PE relatif à la sécurité unique; dans le cas d'un système E/E/PE relatif à la sécurité fonctionnant
 - dans un mode de faible sollicitation, la limite inférieure est fixée à une probabilité moyenne de défaillance de 10^{-5} afin que les fonctions pour lesquelles le système a été conçu soient exécutées lorsqu'elles sont requises;
 - dans un mode de fonctionnement continu ou de forte sollicitation, la limite inférieure est fixée à une probabilité de défaillance dangereuse de 10^{-9} par heure;

NOTE Un système E/E/PE relatif à la sécurité unique n'implique pas nécessairement une architecture à une seule voie.

- 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 ne dépend pas du concept de sécurité intrinsèque qui peut être intéressant lorsque les modes de défaillances sont bien définis et que le niveau de complexité est relativement faible. Le concept de sécurité intrinsèque a été considéré comme inadéquat en raison de l'immense gamme de complexité des systèmes E/E/PE relatifs à la sécurité qui entrent dans le domaine d'application de la présente norme.

- adopts a risk-based approach for the determination of the safety integrity level requirements;
- sets numerical target failure measures for E/E/PE safety-related systems which are linked to the safety integrity levels;
- sets a lower limit on the target failure measures, in a dangerous mode of failure, that can be claimed for 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 failure of 10^{-5} to perform its design function on demand,
 - a high demand or continuous mode of operation, the lower limit is set at a probability of a dangerous failure of 10^{-9} per hour;

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

- adopts a broad range of principles, techniques and measures to achieve functional safety for E/E/PE safety-related systems, but does not rely on the concept of fail-safe, which may be of value when the failure modes are well-defined and the level of complexity is relatively low – the concept of fail-safe was considered inappropriate because of the full range of complexity of E/E/PE safety-related systems that are within the scope of the standard.

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 prescriptions de la CEI 61508-2 et 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 avec le paragraphe 7.4.3 et l'annexe C de la CEI 61508-2, et l'annexe D.
- L'annexe C donne un exemple élaboré de calcul de la couverture du 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 La CEI 61508-1, la CEI 61508-2, la CEI 61508-3 et la CEI 61508-4 sont des publications fondamentales de sécurité, bien que ce statut ne s'applique pas dans le cas de systèmes E/E/PE de sécurité de faible complexité (voir 3.4.4 de la CEI 61508-4). En tant que publications fondamentales de sécurité, elles sont destinées à être utilisées par tous les comités d'études pour la mise au point de leurs normes, conformément aux principes décrits dans le Guide 104 de la CEI et dans le Guide 51 ISO/CEI. La CEI 61508 est également prévue pour une utilisation en tant que norme autonome.

1.3 L'une des responsabilités d'un comité d'études est, chaque fois que cela peut s'appliquer, d'utiliser les publications fondamentales de sécurité pour préparer ses publications. Dans ce contexte, les prescriptions, les méthodes d'essais ou les conditions d'essais de la présente publication fondamentale de sécurité ne sont pas applicables, sauf s'il y est spécifiquement fait référence, ou si elles sont incorporées dans les publications préparées par ces comités d'études.

NOTE Aux Etats-Unis d'Amérique et au Canada, les normes nationales de sécurité des processus existantes, basées sur la CEI 61508 (par exemple l'ANSI/ISA S48.01-1996) peuvent être appliquées dans le domaine des processus, à la place de la CEI 61508, et cela jusqu'à ce que les normes internationales concernant la mise en oeuvre de la CEI 61508 (soit la CEI 61511) dans le domaine des processus soient publiées.

1.4 La figure 1 montre la structure générale des parties 1 à 7 et indique le rôle que la présente CEI 61508-6 joue dans la réalisation de la sécurité fonctionnelle pour les systèmes E/E/PE relatifs à la sécurité.

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 3.4.4 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 IEC/ISO Guide 51. IEC 61508 is also intended for use as a stand-alone standard.

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 do not apply unless specifically referred to or included in the publications prepared by those technical committees.

NOTE In the USA and Canada, until the proposed process sector implementation of IEC 61508 (i.e. IEC 61511) is published as an international standard, existing national process safety standards based on IEC 61508 (i.e. ANSI/ISA S84.01-1996) can be applied to the process sector instead of IEC 61508.

1.4 Figure 1 shows the overall framework for parts 1 to 7 of this standard and indicates the role that IEC 61508-6 plays in the achievement of functional safety for E/E/PE safety-related systems.