
**Sécurité fonctionnelle des systèmes électriques/
électroniques/électroniques programmables
relatifs à la sécurité –**

**Partie 7:
Présentation de techniques et mesures**

(<https://standards.iteh.ai>)
Document Preview

<https://standards.iteh.ai> IEC 61508-7:2000

<https://standards.iteh.ai/document/standards/iec/4d69740-ca18-40f7-8f62-52f6d6ef7719/iec-61508-7-2000>

*Cette version **française** découle de la publication d'origine **bilingue** dont les pages anglaises ont été supprimées.
Les numéros de page manquants sont ceux des pages supprimées.*

Numérotation des publications

Depuis le 1er janvier 1997, les publications de la CEI sont numérotées à partir de 60000. Ainsi, la CEI 34-1 devient la CEI 60034-1.

Editions 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

Informations supplémentaires sur les publications de la CEI

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 cette publication, y compris sa validité, sont disponibles dans le Catalogue des publications de la CEI (voir ci-dessous) en plus des nouvelles éditions, amendements et corrigenda. Des informations sur les sujets à l'étude et l'avancement des travaux entrepris par le comité d'études qui a élaboré cette publication, ainsi que la liste des publications parues, sont également disponibles par l'intermédiaire de:

- **Site web de la CEI (www.iec.ch)**

- **Catalogue des publications de la CEI**

Le catalogue en ligne sur le site web de la CEI (www.iec.ch/searchpub) vous permet de faire des recherches en utilisant de nombreux critères, comprenant des recherches textuelles, par comité d'études ou date de publication. Des informations en ligne sont également disponibles sur les nouvelles publications, les publications remplacées ou retirées, ainsi que sur les corrigenda.

- **IEC Just Published**

Ce résumé des dernières publications parues (www.iec.ch/online_news/justpub) est aussi disponible par courrier électronique. Veuillez prendre contact avec le Service client (voir ci-dessous) pour plus d'informations.

- **Service clients**

Si vous avez des questions au sujet de cette publication ou avez besoin de renseignements supplémentaires, prenez contact avec le Service clients:

Email: custserv@iec.ch
Tél: +41 22 919 02 11
Fax: +41 22 919 03 00

NORME INTERNATIONALE

CEI 61508-7

Première édition
2000-03

Sécurité fonctionnelle des systèmes électriques/ électroniques/électroniques programmables relatifs à la sécurité –

Partie 7: Présentation de techniques et mesures

(<https://standards.iteh.ai>)
Document Preview

IEC 61508-7:2000

<https://standards.iteh.ai/catalog/standards/iec/4d69740-ca18-40f7-8f62-52f6d6ef7719/iec-61508-7-2000>

© IEC 2000 Droits de reproduction réservés

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.

International Electrotechnical Commission, 3, rue de Varembe, PO Box 131, CH-1211 Geneva 20, Switzerland
Telephone: +41 22 919 02 11 Telefax: +41 22 919 03 00 E-mail: inmail@iec.ch Web: www.iec.ch



Commission Electrotechnique Internationale
International Electrotechnical Commission
Международная Электротехническая Комиссия

CODE PRIX

XE

Pour prix, voir catalogue en vigueur

SOMMAIRE

	Pages
AVANT-PROPOS.....	14
INTRODUCTION.....	18
Articles	
1 Domaine d'application.....	22
2 Références normatives.....	26
3 Définitions et abréviations.....	26
Annexe A (informative) Présentation de techniques et mesures pour les E/E/PES: maîtrise des défaillances aléatoires du matériel (voir la CEI 61508-2).....	28
A.1 Electriques.....	28
A.1.1 Détection des défaillances par surveillance en ligne.....	28
A.1.2 Surveillance des contacts de relais.....	28
A.1.3 Comparateur.....	28
A.1.4 Voteur majoritaire.....	30
A.1.5 Principe du courant au repos.....	30
A.2 Electroniques.....	30
A.2.1 Tests par du matériel redondant.....	30
A.2.2 Principes dynamiques.....	32
A.2.3 Port d'accès de test normalisé et architecture de test du type «scrutation aux frontières».....	32
A.2.4 Matériel à sécurité intégrée.....	32
A.2.5 Redondance surveillée.....	34
A.2.6 Composants électriques/électroniques avec contrôle automatique.....	34
A.2.7 Surveillance du signal analogique.....	34
A.2.8 Dévaluation.....	36
A.3 Unités de traitement.....	36
A.3.1 Autotest logiciel: nombre limité de configurations (un canal).....	36
A.3.2 Autotest logiciel: bit glissant (un canal).....	36
A.3.3 Autotest pris en charge par le matériel (un canal).....	36
A.3.4 Traitement codé (un canal).....	38
A.3.5 Comparaison réciproque par logiciel.....	38
A.4 Gamme de mémoire invariable.....	38
A.4.1 Redondance multi-bits à sauvegarde de mot (par exemple, surveillance de la ROM avec un code de Hamming modifié).....	38
A.4.2 Somme de contrôle modifiée.....	40
A.4.3 Signature d'un seul mot (8 bits).....	40
A.4.4 Signature d'un mot double (16 bits).....	40
A.4.5 Réplication du bloc (par exemple, double ROM avec comparaison par matériel ou logiciel).....	42
A.5 Gammes de mémoire variable.....	42
A.5.1 Test RAM «échiquier» ou «défilement».....	42
A.5.2 Test RAM «walkpath».....	44
A.5.3 Test RAM «galpat» ou «galpat transparent».....	44
A.5.4 Test RAM «Abraham».....	46
A.5.5 Redondance à un bit (par exemple, surveillance de la RAM avec un bit de parité) ..	46
A.5.6 Surveillance de la RAM avec un code de Hamming modifié, ou détection des défaillances concernant les données par des codes de détection d'erreurs (EDC) ..	46
A.5.7 Double RAM avec comparaison matérielle ou logicielle et test de lecture/écriture ...	48

Articles	Pages
A.6 Unités E/S et interfaces (communication externe).....	48
A.6.1 Trame de test.....	48
A.6.2 Protection par code.....	48
A.6.3 Sortie parallèle multi-canaux.....	50
A.6.4 Sorties surveillées.....	50
A.6.5 Comparaison/vote majoritaire sur les entrées.....	52
A.7 Chemins de données (communication interne).....	52
A.7.1 Redondance matérielle sur un bit.....	52
A.7.2 Redondance matérielle sur plusieurs bits.....	52
A.7.3 Redondance matérielle complète.....	52
A.7.4 Inspection utilisant des trames de test.....	54
A.7.5 Redondance de transmission.....	54
A.7.6 Redondance d'informations.....	54
A.8 Alimentation.....	54
A.8.1 Protection contre les surtensions avec arrêt de sécurité.....	54
A.8.2 Surveillance de la tension (secondaire).....	56
A.8.3 Mise hors tension avec arrêt de sécurité.....	56
A.9 Surveillance temporelle et logique de la séquence du programme.....	56
A.9.1 Chien de garde avec base de temps séparée sans fenêtre temporelle.....	56
A.9.2 Chien de garde avec base de temps séparée et fenêtre temporelle.....	58
A.9.3 Surveillance logique de la séquence du programme.....	58
A.9.4 Combinaison de surveillance temporelle et logique des séquences du programme.....	58
A.9.5 Surveillance temporelle avec contrôle en ligne.....	58
A.10 Aération et chauffage.....	60
A.10.1 Capteur de température.....	60
A.10.2 Surveillance des ventilateurs.....	60
A.10.3 Actionnement de l'arrêt de sécurité par l'intermédiaire d'un fusible thermique.....	60
A.10.4 Message échelonné des capteurs thermiques et de l'alarme conditionnelle.....	60
A.10.5 Connexion du refroidissement par air forcé et indication d'état.....	60
A.11 Communication et mémoire de masse.....	62
A.11.1 Séparation entre les lignes d'alimentation et les lignes d'informations.....	62
A.11.2 Séparation spatiale des lignes multiples.....	62
A.11.3 Augmentation de l'immunité aux interférences.....	62
A.11.4 Transmission de signaux complémentaires.....	64
A.12 Sondes.....	64
A.12.1 Capteur de référence.....	64
A.12.2 Commutateur à action directe.....	64
A.13 Organes finaux (actionneurs).....	64
A.13.1 Surveillance.....	64
A.13.2 Surveillance croisée de plusieurs actionneurs.....	66
A.14 Mesures contre l'environnement physique.....	66
Annexe B (informative) Présentation de techniques et mesures pour les E/E/PES: prévention des défaillances systématiques (voir la CEI 61508-2 et la CEI 61508-3).....	68
B.1 Mesures et techniques générales.....	68
B.1.1 Gestion de projet.....	68
B.1.2 Documentation.....	70
B.1.3 Séparation des systèmes relatifs à la sécurité et des systèmes non relatifs à la sécurité.....	72
B.1.4 Diversité du matériel.....	72

Articles	Pages
B.2	Spécification des exigences relatives aux E/E/PES..... 74
B.2.1	Spécification structurée..... 74
B.2.2	Méthodes formelles..... 74
B.2.3	Méthodes semi-formelles..... 76
B.2.3.1	Généralités..... 76
B.2.3.2	Automates finis/diagrammes de changement d'états..... 76
B.2.3.3	Réseaux de Pétri temporels..... 78
B.2.4	Outils de spécification assistée par ordinateur..... 78
B.2.4.1	Généralités..... 78
B.2.4.2	Outils orientés vers aucune méthode spécifique..... 80
B.2.4.3	Procédure orientée vers le modèle avec une analyse hiérarchique..... 80
B.2.4.4	Modèles d'entité..... 80
B.2.4.5	Interrogation et réponse..... 82
B.2.5	Listes de contrôle..... 82
B.2.6	Inspection de la spécification..... 84
B.3	Conception et développement des E/E/PES..... 84
B.3.1	Respect des lignes directrices et des normes..... 84
B.3.2	Conception structurée..... 86
B.3.3	Utilisation de composants ayant fait leurs preuves..... 88
B.3.4	Modularisation..... 88
B.3.5	Outils de conception assistée par ordinateur..... 90
B.3.6	Simulation..... 90
B.3.7	Inspection (revues et analyses)..... 90
B.3.8	Sondage..... 92
B.4	Procédures d'exploitation et de maintenance des E/E/PES..... 92
B.4.1	Instructions d'exploitation et de maintenance..... 92
B.4.2	Convivialité en termes d'utilisation..... 94
B.4.3	Convivialité en termes de maintenance..... 94
B.4.4	Possibilités d'exploitation limitées..... 94
B.4.5	Exploitation uniquement par des opérateurs qualifiés..... 96
B.4.6	Protection contre les erreurs humaines..... 96
B.4.7	(Non utilisé)..... 96
B.4.8	Protection contre les modifications..... 96
B.4.9	Accusé de réception des entrées..... 96
B.5	Intégration des E/E/PES..... 98
B.5.1	Test fonctionnel..... 98
B.5.2	Test «boîte noire»..... 98
B.5.3	Test statistique..... 100
B.5.4	Retour d'expérience..... 100
B.6	Validation de la sécurité des E/E/PES..... 102
B.6.1	Tests fonctionnels dans des conditions environnementales..... 102
B.6.2	Essai d'immunité aux interférences et aux ondes de choc..... 104
B.6.3	(Non utilisé)..... 104
B.6.4	Analyse statique..... 104
B.6.5	Analyse dynamique..... 106

Articles	Pages
B.6.6	Analyse des défaillances..... 106
B.6.6.1	Analyse des modes de défaillance et de leurs effets..... 106
B.6.6.2	Diagramme cause-conséquence..... 108
B.6.6.3	Analyse par arbre d'événement..... 108
B.6.6.4	Analyse des modes de défaillance, de leurs effets et de leur criticité... 108
B.6.6.5	Analyse par arbre de panne 110
B.6.7	Analyse des cas les plus défavorables..... 110
B.6.8	Test fonctionnel étendu..... 110
B.6.9	Test du cas le plus défavorable 112
B.6.10	Test d'insertion d'anomalie 112
Annexe C (informative) Présentation de techniques et mesures pour l'obtention de l'intégrité de sécurité logicielle (voir la CEI 61508-3) 114	
C.1	Généralités..... 114
C.2	Prescriptions et conception détaillée 114
C.2.1	Méthodes structurées..... 114
C.2.1.1	Généralités..... 114
C.2.1.2	CORE – Controlled Requirements Expression..... 116
C.2.1.3	JSD – Jackson System Development..... 116
C.2.1.4	MASCOT – Modular Approach to Software Construction, Operation and Test..... 118
C.2.1.5	Yourdon temps réel..... 118
C.2.1.6	SADT – Structured Analysis and Design Technique..... 120
C.2.2	Diagrammes de flux de données..... 122
C.2.3	Diagrammes de structures..... 124
C.2.4	Méthodes formelles..... 124
C.2.4.1	Généralités..... 124
C.2.4.2	CCS – Calculus of Communicating Systems..... 126
C.2.4.3	CSP – Communicating Sequential Processes..... 126
C.2.4.4	HOL – Higher Order Logic..... 128
C.2.4.5	LOTOS..... 128
C.2.4.6	OBJ..... 128
C.2.4.7	Logique temporelle..... 130
C.2.4.8	VDM, VDM++ – Vienna Development Method..... 132
C.2.4.9	Z..... 134
C.2.5	Programmation défensive 136
C.2.6	Règles de conception et de codage 138
C.2.6.1	Généralités..... 138
C.2.6.2	Règles de codage 138
C.2.6.3	Pas de variables dynamiques ni d'objets dynamiques..... 140
C.2.6.4	Contrôle en ligne pendant la création de variables dynamiques ou d'objets dynamiques..... 140
C.2.6.5	Utilisation limitée des interruptions..... 140
C.2.6.6	Utilisation limitée des pointeurs..... 142
C.2.6.7	Utilisation limitée de la récursion..... 142
C.2.7	Programmation structurée..... 142
C.2.8	Masquage/encapsulation des informations 144
C.2.9	Approche modulaire 146
C.2.10	Utilisation de modules logiciels et composants éprouvés/vérifiés 146

Articles	Pages
C.3	Conception d'architecture..... 148
C.3.1	Détection d'anomalie et diagnostic..... 148
C.3.2	Codes de détection et correction d'erreurs..... 150
C.3.3	Programmation par assertion des défaillances 150
C.3.4	Dispositif externe de sécurité 152
C.3.5	Diversité logicielle (programmation diversifiée) 152
C.3.6	Bloc de récupération 154
C.3.7	Récupération arrière 156
C.3.8	Récupération avant..... 156
C.3.9	Mécanismes de récupération d'anomalie par relance 156
C.3.10	Mémorisation de cas d'exécution 158
C.3.11	Dégradation «élégante» 158
C.3.12	Correction d'anomalie en utilisant les techniques d'intelligence artificielle 160
C.3.13	Reconfiguration dynamique..... 160
C.4	Outils de développement et langages de programmation..... 162
C.4.1	Langages de programmation fortement types..... 162
C.4.2	Sous-ensembles de langages 162
C.4.3	Outils certifiés et traducteurs certifiés 164
C.4.4	Outils et traducteurs: confiance accrue résultant de l'utilisation 164
C.4.4.1	Comparaison du programme source et du code exécutable 166
C.4.5	Bibliothèque des modules logiciels et composants éprouvés/vérifiés..... 166
C.4.6	Langages de programmation adéquats..... 168
C.5	Vérification et modification 174
C.5.1	Test probabiliste..... 174
C.5.2	Enregistrement et analyse de données 176
C.5.3	Test d'interface 176
C.5.4	Analyse des valeurs aux limites 176
C.5.5	Estimation des erreurs 178
C.5.6	Implantation d'erreurs 178
C.5.7	Classes d'équivalence et test des partitions d'entrée 180
C.5.8	Tests basés sur la structure 180
C.5.9	Analyse du flux de commandes 182
C.5.10	Analyse du flux de données 184
C.5.11	Analyse de circuit parasite 184
C.5.12	Exécution symbolique 186
C.5.13	Preuve formelle..... 186
C.5.14	Métriques de complexité 188
C.5.15	Inspection selon Fagan 188
C.5.16	Lectures croisées/revues de conception 190
C.5.17	Prototypage/animation 190
C.5.18	Simulation du procédé 192
C.5.19	Prescriptions relatives au fonctionnement..... 192
C.5.20	Modélisation du fonctionnement..... 194
C.5.21	Tests d'avalanche/de stress..... 194
C.5.22	Temps de réponse et contraintes mémoire..... 196
C.5.23	Analyse d'impact..... 196
C.5.24	Gestion de configuration logicielle..... 198

Articles	Pages
C.6 Evaluation de la sécurité fonctionnelle	198
C.6.1 Tables de décision (tables de vérité).....	198
C.6.2 Etude de danger et d'opérabilité (HAZOP)	198
C.6.3 Analyse des défaillances de cause commune.....	202
C.6.4 Modèles de Markov.....	202
C.6.5 Diagrammes de blocs de fiabilité	204
C.6.6 Simulation de Monte-Carlo.....	206
Annexe D (informative) Une approche probabiliste pour déterminer l'intégrité de sécurité logicielle pour un logiciel prédéveloppé	208
D.1 Généralités.....	208
D.2 Formules de tests statistiques et exemples d'utilisation	210
D.2.1 Test statistique simple en mode de fonctionnement faible demande.....	210
D.2.1.1 Conditions préalables	210
D.2.1.2 Résultats	210
D.2.1.3 Exemple	210
D.2.2 Test d'un espace (domaine) d'entrée pour un mode de fonctionnement faible demande	210
D.2.2.1 Conditions préalables	210
D.2.2.2 Résultats	210
D.2.2.3 Exemple	212
D.2.3 Test statistique simple en mode de fonctionnement continu ou forte demande ..	212
D.2.3.1 Conditions préalables	212
D.2.3.2 Résultats	212
D.2.3.3 Exemple	214
D.2.4 Test complet	214
D.2.4.1 Conditions préalables	214
D.2.4.2 Résultats	214
D.2.4.3 Exemple	216
D.3 Références.....	216
Bibliographie	218
Index	222
Tableau C.1 – Recommandations applicables aux langages de programmation spécifiques ...	172
Tableau D.1 – Historique nécessaire pour s'assurer des niveaux d'intégrité de sécurité.....	208
Tableau D.2 – Probabilités de défaillance en mode de fonctionnement faible demande	210
Tableau D.3 – Distances moyennes de deux points de test	212
Tableau D.4 – Probabilité de défaillance en mode de fonctionnement forte demande ou continu	214
Tableau D.5 – Probabilité de test de toutes les propriétés du programme.....	216

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

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

Partie 7: Présentation de techniques et mesures

AVANT-PROPOS

- 1) La CEI (Commission Électrotechnique Internationale) 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. 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 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 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 des 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 61508-7 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/293/FDIS	65A/299/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, B, C et D 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

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 de 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 2006. A cette date, la publication sera

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

iTech Standards
(<https://standards.iteh.ai>)
Document Preview

IEC 61508-7:2000

<https://standards.iteh.ai/catalog/standards/iec/4d69740-ca18-40f7-8f62-52f6d6ef7719/iec-61508-7-2000>

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 comprenant des composants électriques et/ou électroniques et/ou électroniques programmables (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 faut 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 qu'elle considère aussi 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/PES 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 dépendra de plusieurs facteurs propres à l'application. La présente Norme internationale, de par son caractère général, rendra 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 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 à réaliser par les systèmes E/E/PE relatifs à la sécurité;
- 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 n'est pas fondée sur le 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.

(<https://standards.iteh.ai>)
Document Preview

IEC 61508-7:2000

<https://standards.iteh.ai/doc/standards/iec/4469740-ca18-40f7-8f62-52f6d6ef7719/iec-61508-7-2000>

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

Partie 7: Présentation de techniques et mesures

1 Domaine d'application

1.1 La présente partie de la CEI 61508 contient une présentation de différentes techniques et mesures de sécurité pertinentes pour la CEI 61508-2 et la CEI 61508-3.

NOTE Il convient que les références citées soient considérées comme des références fondamentales des méthodes et outils, ou comme des exemples; elles peuvent ne pas représenter l'état de l'art.

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.

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 propres 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 1 La sécurité fonctionnelle d'un système E/E/PE relatif à la sécurité ne peut être réalisée que lorsque toutes les prescriptions pertinentes sont remplies. En conséquence, il est important que toutes les prescriptions pertinentes soient prises en considération avec soin et référencées de façon appropriée.

NOTE 2 Aux Etats-Unis et au Canada, dans l'attente de la publication de la future CEI 61511 (la version de CEI 61508 pour le processus) les normes nationales existantes pour la sécurité des processus industriels basés sur la CEI 61508 (c'est-à-dire ANSI/ISA 584.01-1996) peuvent être appliquées au domaine des processus industriels à la place de la CEI 61508.

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