NORME INTERNATIONALE

CEI 61508-5

Première édition
1998-12

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

Partie 5: Exemples de méthodes de détermination des niveaux d'intégrité de sécurité

*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.

Numéro de référence
CEI 61508-5:1998(F)

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 61508-5

Première édition
1998-12

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

Partie 5: Exemples de méthodes de détermination des niveaux d'intégrité de sécurité

International Electrotechnical Commission, 3, rue de Varembé, 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 U

Pour prix, voir catalogue en vigueur

SOMMAIRE

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

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

Partie 5: Exemples de méthodes de détermination des niveaux d'intégrité de sécurité

AVANT-PROPOS

1) La CEI (Commission Electrotechnique 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, 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 61508-5 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/266/FDIS	65A/276/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.

Les annexes A, B, C, D, E et F 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 directives pour l'application de la CEI 61508-2 et de la CEI 61508-3
– Partie 7: Présentation de techniques et mesures

La partie 5 doit être lue conjointement avec la partie 1.

Elle a le statut d'une publication fondamentale de sécurité conformément au Guide CEI 104.

Le contenu du corrigendum d'avril 1999 a été pris en considération dans cet exemplaire.

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, 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, les actionneurs), mais elle doit aussi considérer 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 E/E/PES, fournit néanmoins un cadre de sécurité susceptible de concerner les systèmes relatifs à la sécurité basés sur des technologies différentes.

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 du cycle de vie de sécurité (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 fourni par cette Norme internationale 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, de la documentation, 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 requise des systèmes de sécurité E/E/PE;

– 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 de sécurité E/E/PE;

– 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 de sécurité E/E/PE 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 de sécurité E/E/PE unique. Dans le cas d'un système de sécurité E/E/PE 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 de sécurité E/E/PE 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 de sécurité E/E/PE, mais n'utilise pas le concept de «sécurité intrinsèque» qui a un sens particulier lorsque les modes de défaillances sont bien définis et que le niveau de complexité est relativement faible. Ce concept a été considéré comme inadéquat en raison de l'immense gamme de complexité des systèmes de sécurité E/E/PE qui entrent dans le domaine d'application de la présente norme.

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

Partie 5: Exemples de méthodes de détermination des niveaux d'intégrité de sécurité

1 Domaine d'application

1.1 La présente partie de la CEI 61508 fournit des informations sur

– les concepts sous-jacents à la notion de risque et les liens entre le risque et l'intégrité de sécurité (voir annexe A);

– des méthodes qui permettront d'assurer le niveau d'intégrité de sécurité des systèmes E/E/PE relatifs à la sécurité, des systèmes relatifs à la sécurité basés sur d'autres technologies et des dispositifs externes de réduction de risque (voir annexes B, C, D et E).

1.2 La méthode retenue dépendra du secteur d'application et des conditions spécifiques à prendre en considération. Les annexes B, C, D et E illustrent les approches quantitatives et qualitatives et ont été simplifiées dans le but d'illustrer les principes sous-jacents. Ces annexes ont été incluses pour illustrer les principes généraux d'un certain nombre de méthodes mais ne fournissent pas une explication définitive. Pour utiliser les méthodes indiquées dans ces annexes, il convient de consulter les sources indiquées.

NOTE – Pour plus d'informations concernant les approches illustrées par les annexes B, D et E, voir respectivement les références [4], [2] et [3] qui se trouvent en annexe F. Voir aussi la référence [5] de l'annexe F qui décrit une autre approche.

1.3 Les parties 1, 2, 3 et 4 de la présente norme sont des publications fondamentales de sécurité, bien qu'un tel statut ne soit pas applicable dans le contexte des systèmes E/E/PE de faible complexité relatifs à la sécurité (voir 3.4.4 de la partie 4). En tant que publications fondamentales de sécurité, ces normes sont prévues pour être utilisées par les comités techniques pour la préparation des normes selon les principes contenus dans le *Guide CEI 104* et le *Guide ISO/CEI 51*. Les parties 1, 2, 3 et 4 sont également destinées à être utilisées comme publications autonomes.

Une des responsabilités incombant à un comité technique est, dans la mesure du possible, d'utiliser les publications fonda-mentales de sécurité, pour la préparation de ses publications. Dans ce contexte les prescriptions, les méthodes d'essai ou 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 techniques.

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 S84.01-1996, voir référence [8] à l'annexe C) 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 œuvre de la CEI 61508 dans le domaine des processus soient publiées.

1.4 La figure 1 montre la structure générale des parties 1 à 7 de la CEI 61508 et indique le rôle de la CEI 61508-5 dans la réalisation de la sécurité fonctionnelle des systèmes E/E/PE relatifs à la sécurité.

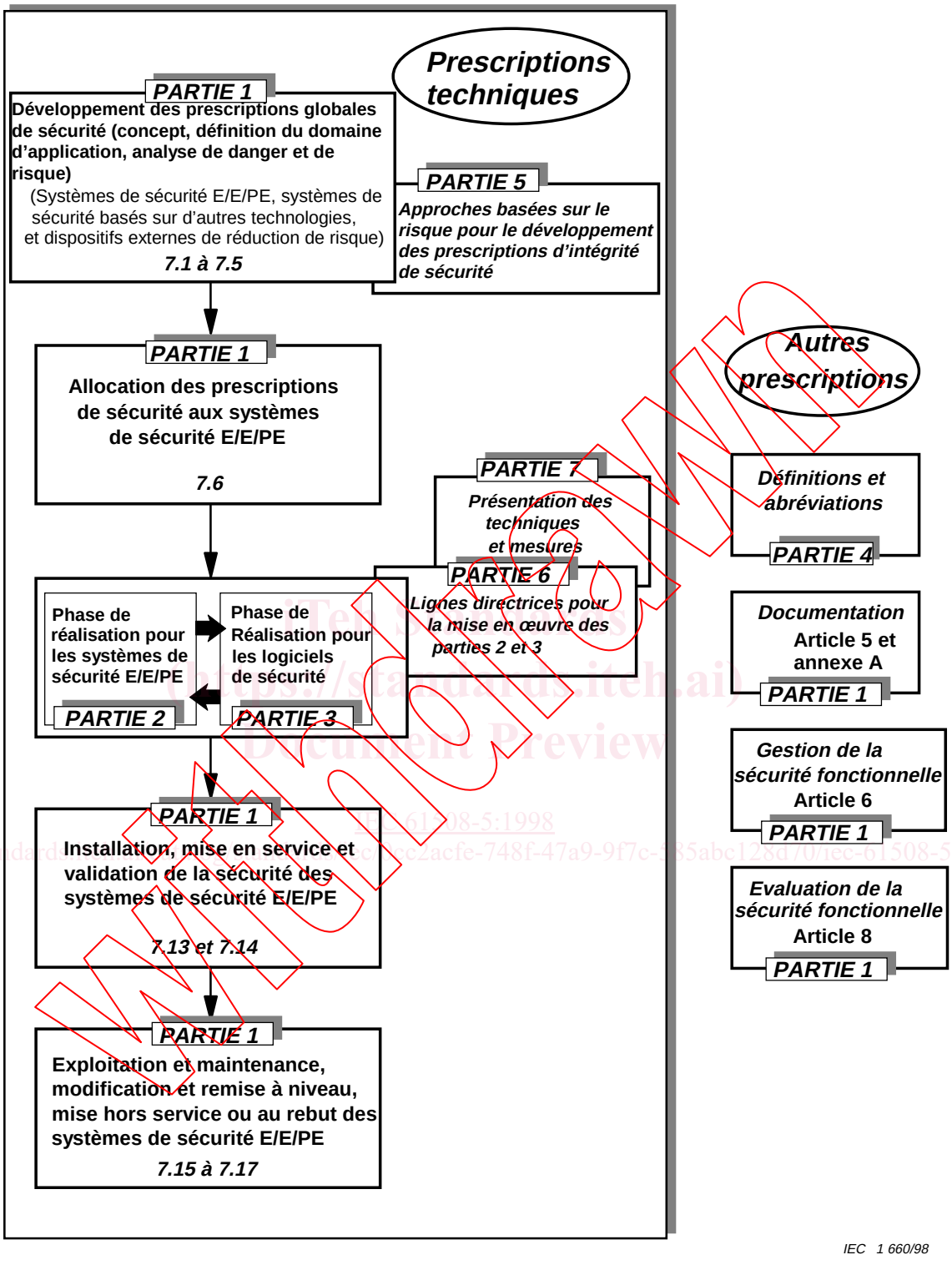

Figure 1 – Structure générale de la présente norme

2 Références normatives

Les documents normatifs suivants contiennent des dispositions qui, par suite de la référence qui y est faite, constituent des dispositions valables pour la présente Norme internationale. Au moment de sa publication, les éditions indiquées étaient en vigueur. Tout document normatif est sujet à révision et les parties prenantes aux accords fondés sur la présente Norme internationale sont invitées à rechercher la possibilité d'appliquer les éditions les plus récentes des documents normatifs indiqués ci-après. Les membres de la CEI et de l'ISO possèdent le registre des Normes internationales en vigueur.

CEI 61508-1:1998, *Sûreté fonctionelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 1: Prescriptions générales*

CEI 61508-2,— *Sûreté fonctionelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 2: Prescriptions pour les systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité* [1)]

CEI 61508-3:1998, *Sûreté fonctionelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 3: Prescriptions concernant les logiciels*

CEI 61508-4:1998, *Sûreté fonctionelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 4: Définitions et abréviations*

CEI 61508-6,— *Sûreté fonctionelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 6: Lignes directrices pour l'application des parties 2 et 3* [1)]

CEI 61508-7,— *Sûreté fonctionelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 7: Présentation de techniques et mesures* [1)]

Guide ISO/CEI 51:1990, *Principes directeurs pour inclure dans les normes les aspects liés à la sécurité*

Guide CEI 104:1997, *Guide pour la rédaction des normes de sécurité et rôle des comités chargés de fonctions pilotes de sécurité et de fonctions groupées de sécurité*

3 Définitions et abréviations

Pour les besoins de la présente norme, les définitions et les abréviations données à la partie 4 s'appliquent.

[1)] A publier.