NORME INTERNATIONALE

CEI 61508-1

Première édition
1998-12

PUBLICATION FONDAMENTALE DE SÉCURITÉ

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

Partie 1: Prescriptions générales

*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 61508-1:1998(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 61508-1

Première édition
1998-12

PUBLICATION FONDAMENTALE DE SÉCURITÉ

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

Partie 1: Prescriptions générales

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 XA

Pour prix, voir catalogue en vigueur

SOMMAIRE

Pages

Annexes

Tableaux

Figures

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

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

Partie 1: Prescriptions générales

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 61508-1 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/264/FDIS	65A/274/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 et C sont données uniquement à titre d'information.

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

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 la CEI 61508-3
– Partie 7: Présentation de techniques et mesures

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, 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 et 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/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 fourni par la présente 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 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;

– 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'utilise pas 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.

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

Partie 1: Prescriptions générales

1 Domaine d'application

1.1 La présente Norme internationale traite des aspects à prendre en considération lors de l'utilisation de systèmes électriques/électroniques/électroniques programmables (E/E/PES) pour exécuter des fonctions de sécurité. L'un des objectifs majeurs de la présente Norme internationale est de permettre l'élaboration par les comités d'études responsables des secteurs concernés de Normes internationales spécifiques à chaque secteur d'application. Cela permettra de prendre en compte l'ensemble des facteurs pertinents pour chaque application, et donc de répondre aux besoins spécifiques de chacun de ces secteurs. Un autre des objectifs poursuivis par la présente Norme internationale est de permettre le développement de systèmes E/E/PE relatifs à la sécurité en l'absence éventuelle de Normes internationales pour ce secteur d'application.

1.2 En particulier, cette norme

a) s'applique aux systèmes relatifs à la sécurité lorsque l'un ou plus de ces systèmes comporte des dispositifs électriques/électroniques/électroniques programmables;

NOTE 1 – En ce qui concerne les systèmes E/E/PE relatifs à la sécurité de faible complexité, certaines prescriptions décrites dans la présente norme peuvent ne pas être nécessaires, et il est possible d'être exempté de la conformité avec de telles prescriptions (voir en 4.2, et la définition d'un système E/E/PE relatif à la sécurité de faible complexité en 3.4.4 de la CEI 61508-4.

NOTE 2 – Bien qu'une personne physique puisse faire partie d'un système relatif à la sécurité (voir 3.4.1 de la CEI 61508-4, les prescriptions sur le facteur humain dans la conception de systèmes E/E/PE relatifs à la sécurité ne sont pas détaillées dans cette norme.

b) est basée génériquement et est applicable à tout système E/E/PE relatif à la sécurité[1)] sans considération de son domaine d'application;

c) englobe les risques potentiels dus à des défaillances des fonctions de sécurité devant être réalisées par les systèmes E/E/PE relatifs à la sécurité, ces derniers étant bien distincts des risques découlant de l'équipement E/E/PE par lui-même (par exemple chocs électriques, etc.);

d) n'englobe pas les systèmes E/E/PE où

   – un système E/E/PE unique est capable de fournir la réduction de risque nécessaire et

   – l'intégrité de sécurité, du système E/E/PE, exigée est moindre que celle prescrite pour le niveau 1 d'intégrité de sécurité (niveau d'intégrité de sécurité le plus faible de la présente norme).

e) traite plus particulièrement des systèmes E/E/PE relatifs à la sécurité dont une défaillance pourrait avoir un impact sur la sécurité des personnes et/ou sur l'environnement; cependant, il est reconnu que les défaillances peuvent entraîner des conséquences économiques sérieuses, et dans de pareils cas, la présente norme pourrait également être utilisée pour prescrire tout système E/E/PE utilisé pour protéger l'équipement ou le produit;

NOTE – Voir 3.1.1 et 7.3.1.2 de la CEI 61508-4.

1) Par extension, les systèmes E/E/PE relatifs à la sécurité seront dénommés «systèmes de sécurité E/E/PE» dans les articles suivants.

f) considère les systèmes E/E/PE relatifs à la sécurité, les systèmes relatifs à la sécurité basés sur d'autres technologies et les dispositifs externes de réduction de risque afin que la définition des prescriptions de sécurité pour les systèmes E/E/PE relatifs à la sécurité puisse être déterminée de façon systématique en étant basée sur le risque;

g) utilise, en tant que cadre technique, un modèle de cycle de vie de sécurité global pour traiter, de façon systématique, des activités à réaliser pour assurer la sécurité fonctionnelle des systèmes E/E/PE relatifs à la sécurité;

NOTE 3 – Les premières phases du modèle de cycle de vie de sécurité global incluent, nécessairement, l'étude d'autres technologies (en plus des systèmes E/E/PE relatifs à la sécurité) et les dispositifs externes de réduction de risque, de façon à ce que les définitions des prescriptions de sécurité pour les systèmes E/E/PE relatifs à la sécurité puissent être déterminées de façon systématique en étant basées sur le risque.

NOTE 4 – Bien que le cycle de vie de sécurité global concerne avant tout les systèmes E/E/PE relatifs à la sécurité, il peut aussi servir de cadre technique pour l'étude de tout système relatif à la sécurité, indépendamment de la technologie employée par ce système (par exemple mécanique, hydraulique ou pneumatique).

h) ne prescrit pas les niveaux d'intégrité de sécurité exigés par secteur d'application (ces niveaux doivent être basés sur des informations détaillées et une bonne connaissance de l'application sectorielle). Les comités d'études responsables des secteurs d'application spécifiques doivent prescrire, si nécessaire, les niveaux d'intégrité de sécurité dans leurs normes sectorielles;

i) fournit des prescriptions générales pour les systèmes E/E/PE relatifs à la sécurité qui ne sont pas couverts par une norme sectorielle;

j) ne traite pas des précautions qu'il peut être nécessaire de prendre afin d'éviter que des personnes non autorisées abîment, et/ou aient, d'une manière quelconque, une activité dommageable sur la sécurité fonctionnelle des systèmes E/E/PE relatifs à la sécurité.

1.3 La présente partie de la CEI 61508 définit les prescriptions générales qui sont applicables à toutes les autres parties. Les autres parties de la norme CEI 61508 traitent de sujets plus spécifiques:

– les parties 2 et 3 fournissent des prescriptions spécifiques et supplémentaires pour les systèmes E/E/PE relatifs à la sécurité (pour le matériel et le logiciel);

– la partie 4 donne les définitions et les abréviations qui sont utilisées tout au long de la présente norme;

– la partie 5 fournit des lignes directrices pour la mise en œuvre de la détermination des niveaux d'intégrité de sécurité, définis dans la partie 1, en présentant des exemples de méthodes;

– la partie 6 fournit des lignes directrices pour la mise en œuvre des parties 2 et 3;

– la partie 7 contient une présentation des techniques et des mesures.

1.4 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 fondamentales 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 oeuvre de la CEI 61508 dans le domaine des processus soient publiées.

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

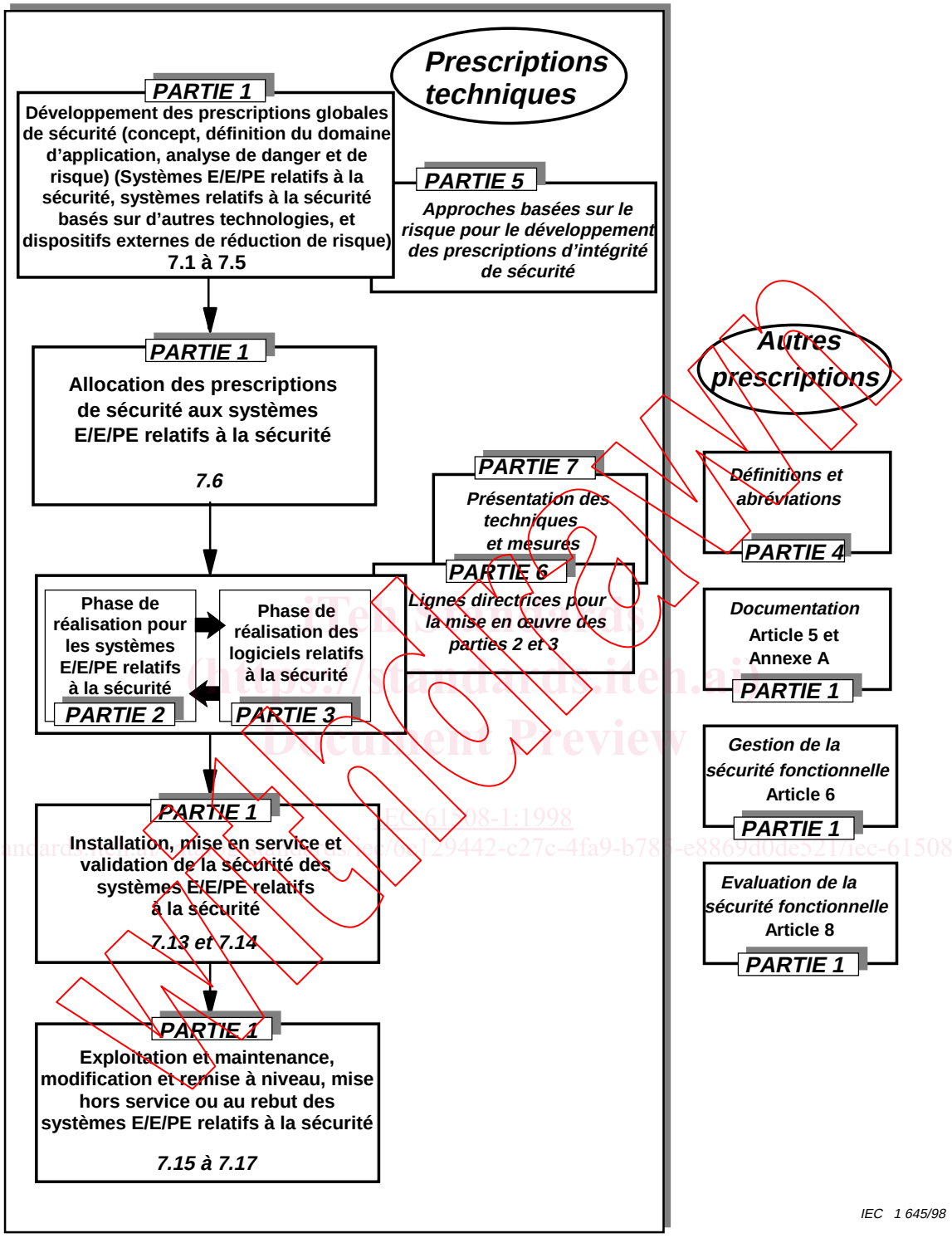

Figure 1 – Structure générale de la présente norme

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 partie de la CEI 61508. Pour les références datées, les amendements ultérieurs ou les révisions de ces publications ne s'appliquent pas. Toutefois, les parties prenantes aux accords fondés sur la présente partie de la CEI 61508 sont invitées à rechercher la possibilité d'appliquer les éditions les plus récentes des documents normatifs indiqués ci-après. Pour les références non datées, la dernière édition du document normatif en référence s'applique. Les membres de la CEI et de l'ISO possèdent le registre des Normes internationales en vigueur.

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

CEI Guide 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*

CEI 61508-2, — *Sûreté fonctionnelle 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 fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 3: Prescriptions concernant les logiciels*

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

CEI 61508-5:1998, *Sûreté fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 5: Exemples de méthodes de détermination des niveaux d'intégrité de sécurité*

CEI 61508-6, — *Sûreté fonctionnelle 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 fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 7: Présentation de techniques et mesures* [1)]

3 Définitions et abréviations

Pour les besoins de la présente Norme internationale, les définitions et abréviations données dans la partie 4 s'appliquent.

1) A publier.

4 Conformité à la présente Norme internationale

4.1 Afin de se conformer à la présente Norme internationale, il doit être démontré que les prescriptions ont été remplies pour le critère prescrit spécifié (par exemple, le niveau d'intégrité de sécurité), et que, par conséquent, pour chaque article ou paragraphe, tous les objectifs ont été atteints.

NOTE – Il n'est généralement pas possible de choisir chaque facteur qui détermine le niveau auquel une prescription devra être respectée (niveau de rigueur). Ce choix dépendra d'un certain nombre de facteurs, qui peuvent dépendre eux-mêmes de l'ensemble des phases et activités spécifiques du cycle de vie de sécurité du logiciel ou des systèmes E/E/PE. Ces facteurs comprennent:

– la nature des dangers;
– la réduction des risques et des conséquences;
– le niveau d'intégrité de sécurité;
– le type de technologie de mise en œuvre;
– la taille des systèmes;
– le nombre d'équipes impliquées;
– la répartition physique;
– l'originalité de la conception.

4.2 La présente norme spécifie les prescriptions pour les systèmes de sécurité E/E/PE et a été développée pour couvrir tous les niveaux de complexité possible de ces systèmes. Cependant, pour les systèmes de sécurité E/E/PE de faible complexité (voir en 3.4.4 de la CEI 61508-4) où une solide expérience de terrain apporte la confiance nécessaire pour assurer que l'intégrité de sécurité prescrite puisse être réalisée, les options suivantes sont envisageables:

– dans les normes de secteurs d'application mettant en œuvre les prescriptions de la CEI 61508-1 à la CEI 61508-7, certaines prescriptions de la présente norme peuvent ne pas être nécessaires, et il est acceptable d'être exempté de conformité avec de telles prescriptions;
– si la présente norme est directement utilisée dans les cas où il n'existe pas de Norme internationale pour ce secteur d'application, certaines prescriptions spécifiées dans la présente norme peuvent ne pas être nécessaires et l'exemption de conformité avec de telles prescriptions est acceptable à condition d'être dûment justifiée.

4.3 Les Normes internationales par secteur d'application pour les systèmes de sécurité E/E/PE développées dans le cadre de la présente norme doivent prendre en compte les prescriptions du Guide ISO/CEI 51 et du Guide CEI 104.

5 Documentation

5.1 Objectifs

5.1.1 Le premier objectif des prescriptions de cet article est de spécifier l'information qu'il sera nécessaire de documenter afin que toutes les phases du cycle de vie global du système E/E/PE et du logiciel puissent s'accomplir efficacement.