NORME INTERNATIONALE

CEI 61508-3

Première édition
1998-12

PUBLICATION FONDAMENTALE DE SÉCURITÉ

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

Partie 3: Prescriptions concernant les logiciels

*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 61508-3:1998(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 61508-3

Première édition
1998-12

PUBLICATION FONDAMENTALE DE SÉCURITÉ

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

Partie 3: Prescriptions concernant les logiciels

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 X

Pour prix, voir catalogue en vigueur

SOMMAIRE

Tableaux Pages

Figures

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

Partie 3: Prescriptions concernant les logiciels

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 61508-3 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/269/FDIS	65A/277/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 et B font partie intégrante de cette norme.
L'annexe C est donnée uniquement à titre d'information.

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

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

INTRODUCTION

Les systèmes constitués de composants électriques et/ou 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 informatique (généralement désignés par l'appellation: «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 concernant les systèmes constitués de composants électriques et/ou électroniques et/ou électroniques programmables (E/E/PES) destinés à exécuter des fonctions de sécurité. Cette approche unifiée a été adoptée afin de développer une politique technique rationnelle et logique concernant tous les appareils électriques liés à la sécurité. L'un des principaux objectifs poursuivis consiste à faciliter l'élaboration de normes destinées à chaque 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 aussi qu'elle considère tous les systèmes de sécurité comme des éléments individuels d'un ensemble complexe. C'est pourquoi cette Norme internationale, bien que traitant essentiellement des E/E/PES, fournit néanmoins un cadre de sécurité susceptible de concerner les systèmes de 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 spécifiques à chaque secteur d'application.

La présente Norme internationale

– concerne toutes les phases appropriées du cycle de vie de sécurité des E/E/PES et de leurs logiciels (depuis la conceptualisation initiale jusqu'au déclassement, en passant par la création, l'installation, la mise en service et l'entretien) lorsque les E/E/PES exécutent des fonctions de sécurité;

– a été conçue 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 de sécurité E/E/PE;

– utilise des niveaux d'intégrité de sécurité afin de spécifier les niveaux objectifs d'intégrité de sécurité des fonctions de sécurité à réaliser par les systèmes de sécurité E/E/PE;

– adopte une approche basée sur le risque encouru pour déterminer les prescriptions de niveaux d'intégrité de sécurité;

– fixe des objectifs numériques 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 fonctionnement faible demande, la limite inférieure est fixée à une probabilité de défaillance de 10^{-5} par heure afin que les fonctions pour lesquelles le système a été conçu soient exécutées lorsqu'elles sont requises,

  • dans un mode de fonctionnement forte demande, ou continu, la limite inférieure est fixée à une probabilité de défaillance dangereuse de 10^{-9} par heure;

  NOTE – Un système E/E/PE de sécurité unique ne signifie pas nécessairement 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 non approprié 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 3: Prescriptions concernant les logiciels

1 Domaine d'application

1.1 La présente partie de la CEI 61508

a) est prévue pour n'être utilisée qu'après s'être assuré d'une compréhension parfaite de la CEI 61508-1 et de la CEI 61508-2;

b) s'applique à tout logiciel faisant partie d'un système relatif à la sécurité, ou utilisé pour développer un système relatif à la sécurité entrant dans le domaine de la CEI 61508-1 et de la CEI 61508-2. Ce type de logiciel est désigné par le terme «logiciel relatif à la sécurité»;

   – Les logiciels relatifs à la sécurité comprennent les systèmes d'exploitation, les logiciels système, les logiciels des réseaux de communication, les fonctions d'interface homme-machine, les outils supports et les micrologiciels («firmware»), ainsi que la programmation d'applications.

   – Les programmes d'applications comprennent les programmes de haut niveau, de bas niveau et les programmes spécifiques dans des langages de variabilité limitée (voir 3.2.7 de la CEI 61508-4).

c) nécessite que les fonctions de sécurité du logiciel et les niveaux d'intégrité de sécurité du logiciel soient précisés.

   NOTE 1 – Si cela a déjà été réalisé dans le cadre de la spécification des systèmes E/E/PE relatifs à la sécurité (voir 7.2 de la CEI 61508-2), il n'est pas nécessaire de le répéter dans la présente partie.

   NOTE 2 – Spécifier les fonctions de sécurité du logiciel et les niveaux d'intégrité de sécurité du logiciel est une procédure itérative; voir les figures 2 et 6.

   NOTE 3 – Voir l'article 5 et l'annexe A de la CEI 61508-1 pour la structure de la documentation. Cette structure peut tenir compte des procédures internes de la société et des procédés de travail des secteurs d'application spécifiques.

d) établit des prescriptions concernant les phases et activités du cycle de vie de sécurité qui doivent être appliquées durant la conception et développement du logiciel relatif à la sécurité (modèle de cycle de vie de sécurité du logiciel). Ces prescriptions comprennent l'application de mesures et de techniques qui suivent une gradation basée sur le niveau d'intégrité de sécurité, afin d'éviter et de maîtriser les défauts et défaillances du logiciel;

e) fournit les prescriptions pour les informations relatives à la validation de la sécurité du logiciel et devant être transmises à l'organisation en charge de l'intégration E/E/PES;

f) fournit les prescriptions pour la préparation des informations et procédures concernant le logiciel requis par l'utilisateur pour le fonctionnement et la maintenance d'un système relatif à la sécurité;

g) fournit les prescriptions devant être observées par l'organisation en charge des modifications du logiciel relatif à la sécurité;

h) fournit, en accord avec la CEI 61508-1 et CEI 61508-2, les prescriptions pour les outils supports tels que les outils de conception et développement, les traducteurs de langage, les outils de test et de mise au point et les outils de gestion de configuration.

   NOTE 4 – Les figures 4 et 6 montrent la relation entre la CEI 61508-2 et la CEI 61508-3.

1.2 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 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 œuvre de la CEI 61508 (soit la CEI 61511) dans le domaine des processus soient publiées.

1.3 La figure 1 montre la structure globale des parties 1 à 7 de la CEI 61508 et indique le rôle dévolu à la CEI 61508-3 pour assurer la sécurité fonctionnelle des systèmes E/E/PE relatifs à la sécurité. L'annexe A de la CEI 61508-6 décrit l'application de la CEI 61508-2 et de la CEI 61508-3.

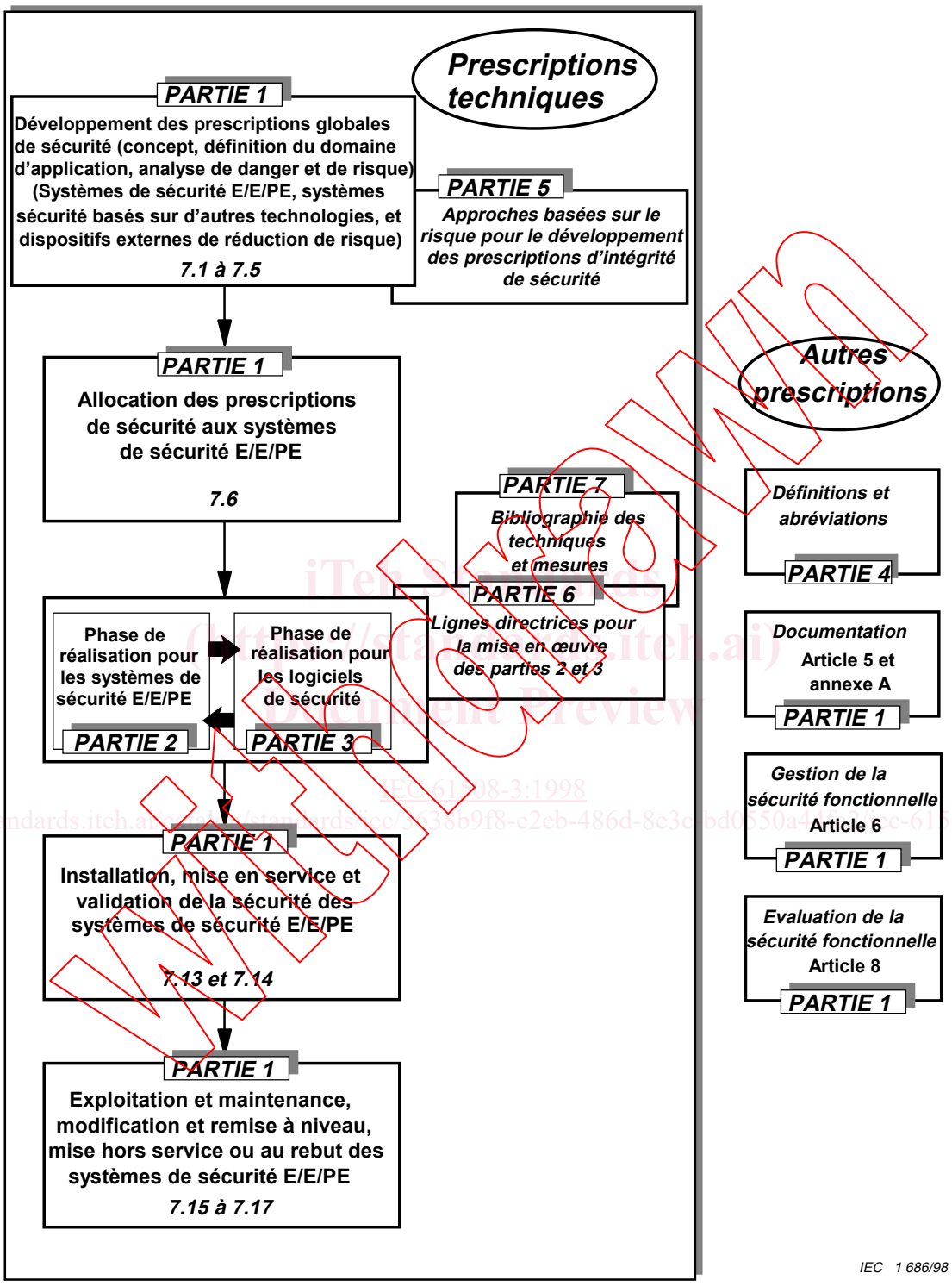

Figure 1 — Structure globale de la présente norme

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. 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 partie de la CEI 61508 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 fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 1: Prescriptions générales*

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 61508-4:1998, *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 pour la 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)]

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

Les définitions et abréviations utilisées dans la présente norme figurent dans la CEI 61508-4.

4 Conformité à la présente norme

Les prescriptions de conformité à la présente norme figurent à l'article 4 de la CEI 61508-1.

5 Documentation

Les objectifs et prescriptions concernant la documentation figurent à l'article 5 de la CEI 61508-1.

---

1) A publier.

6 Système de gestion de la qualité du logiciel

6.1 Objectifs

Les objectifs sont détaillés en 6.1 de la CEI 61508-1.

6.2 Prescriptions

6.2.1 Les prescriptions comprennent celles qui sont détaillées en 6.2 de la CEI 61508-1 ainsi que les prescriptions supplémentaires suivantes.

6.2.2 La planification de sécurité fonctionnelle doit définir la stratégie pour l'approvisionnement, le développement, l'intégration, la vérification, la validation et la modification du logiciel dans les limites requises par le niveau d'intégrité de sécurité du système E/E/PE relatif à la sécurité.

NOTE – La philosophie de cette approche est d'utiliser la planification de sécurité fonctionnelle comme une opportunité d'adapter la présente norme en vue de prendre en compte l'intégrité de sécurité variable requise pour les composants des systèmes E/E/PE relatifs à la sécurité. Il convient de prendre en compte 7.4.2.8 de la partie 3 lorsque des composants de niveau d'intégrité de sécurité différents doivent être utilisés ensemble dans un système E/E/PE relatif à la sécurité.

6.2.3 Il convient que la gestion de configuration du logiciel

a) maîtrise administrativement et techniquement, tout au long du cycle de vie de sécurité du logiciel, la gestion des modifications du logiciel, assurant ainsi la conformité permanente aux prescriptions de sécurité du logiciel spécifiées;

b) garantisse que toutes les opérations nécessaires ont été effectuées en vue de démontrer que le niveau d'intégrité requis de sécurité du logiciel a été atteint;

c) maintienne de manière précise et au moyen d'une identification unique tous les éléments de configuration qui sont nécessaires au maintien de l'intégrité du système E/E/PE relatif à la sécurité. La configuration comprend au moins les éléments suivants: prescriptions et analyse de sécurité, documents de conception et de spécification du logiciel, modules de code source du logiciel, plans de test et résultats, progiciels et composants logiciels préexistants à incorporer au système E/E/PE relatif à la sécurité et tous les outils et environnements de développement qui sont utilisés pour créer, tester ou effectuer une action sur le logiciel du système E/E/PE relatif à la sécurité;

d) applique des procédures de maîtrise des modifications afin d'empêcher toute modification non autorisée; de documenter les demandes de modification; d'analyser l'impact d'une modification proposée, et d'approuver ou rejeter la demande de modification; de documenter les détails et les autorisations pour toutes les modifications approuvées; d'établir le référentiel de la configuration à des points-clés appropriés lors du développement du logiciel, et de documenter le test d'intégration (partielle) qui justifie le référentiel (voir 7.8); de garantir la composition et la construction, de tous les référentiels logiciels (y compris la reconstruction de référentiels précédents);

NOTE 1 – Une autorité de gestion et de décision est nécessaire pour guider et assurer la maîtrise administrative et technique.

e) documente les informations suivantes afin de permettre un audit ultérieur: état de la configuration, état des versions, justification et approbation de toutes les modifications, et détails des modifications;

f) documente de manière formelle la version du logiciel relatif à la sécurité. Il convient de conserver les copies originales du logiciel et toute la documentation associée afin de permettre la maintenance de la modification au cours de l'exploitation de la version du logiciel.

NOTE 2 – Pour tout renseignement complémentaire concernant les processus de gestion de la configuration, voir ISO/CEI 12207.

7 Prescriptions concernant le cycle de vie de sécurité du logiciel

7.1 Généralités

7.1.1 Objectif

L'objectif des prescriptions de ce paragraphe est de structurer le développement du logiciel sous forme de phases et d'activités définies (voir tableau 1 et figures 2 à 5).

7.1.2 Prescriptions

7.1.2.1 Un cycle de vie de sécurité pour le développement du logiciel doit être sélectionné et spécifié pendant la planification de sécurité conformément à l'article 6 de la CEI 61508-1.

NOTE – Un modèle de cycle de vie de sécurité conforme aux prescriptions de l'article 7 de la CEI 61508-1 peut être adapté de manière adéquate aux besoins particuliers du projet ou de l'organisation.

7.1.2.2 Les procédures d'assurance qualité et sécurité doivent être intégrées dans les activités du cycle de vie de sécurité.

7.1.2.3 Chaque phase du cycle de vie de sécurité du logiciel doit être divisée en activités élémentaires avec le domaine d'application, les entrées et sorties spécifiées pour chaque phase.

NOTE 1 – Pour tout renseignement complémentaire concernant les phases du cycle de vie, voir ISO/CEI 12207.

NOTE 2 – L'article 5 de la CEI 61508-1 prend en compte les sorties des phases du cycle de vie de sécurité. Durant le développement de certains systèmes E/E/PE relatifs à la sécurité, la sortie de certaines phases du cycle de vie de sécurité peut être couverte par un document distinct tandis que les sorties documentées de plusieurs phases peuvent être fusionnées. La prescription principale est que la sortie de la phase du cycle de vie de sécurité soit adaptée au but prévu. Pour les développements simples, certaines phases du cycle de vie de sécurité peuvent être également fusionnées (voir 7.4.5).

7.1.2.4 A condition que le cycle de vie de sécurité du logiciel satisfasse aux prescriptions de la figure 3 et du tableau 1, il est acceptable d'adapter la profondeur, le nombre et la quantité de travail des phases du modèle en V (voir figure 5), afin de tenir compte de l'intégrité de sécurité et de la complexité du projet.

NOTE – La liste complète des phases du cycle de vie fournie dans le tableau 1 convient pour de grands systèmes nouvellement développés. Pour les petits systèmes, il peut être approprié, par exemple, de fusionner les phases de conception du système logiciel et de conception d'architecture.

7.1.2.5 Il est acceptable d'ordonner le projet logiciel différemment de l'organisation préconisée dans cette norme (c'est-à-dire d'utiliser un autre modèle de cycle de vie de sécurité) à condition que tous les objectifs et prescriptions du présent article soient remplis.

7.1.2.6 Pour chaque phase du cycle de vie, des techniques et mesures appropriées doivent être utilisées. Les annexes A et B (guide pour la sélection de techniques et mesures) donnent des recommandations. Sélectionner des techniques dans les annexes A et B ne garantit pas, de ce fait, que l'intégrité de sécurité requise sera atteinte.

7.1.2.7 Les résultats des activités menées dans le cadre du cycle de vie de sécurité du logiciel doivent être documentés (voir article 5).

7.1.2.8 Si, à un stade quelconque du cycle de vie de sécurité du logiciel, il est nécessaire d'effectuer une modification portant sur une phase précédente du cycle de vie, cette phase précédente du cycle de vie de sécurité doit alors être répétée ainsi que les phases suivantes.