NORME INTERNATIONALE

INTERNATIONAL STANDARD

CEI
IEC
61508-1

Première édition
First edition
1998-12

PUBLICATION FONDAMENTALE DE SÉCURITÉ
BASIC SAFETY PUBLICATION

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

Partie 1: Prescriptions générales –

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

Part 1: General requirements

Numéro de référence
Reference number
CEI/IEC 61508-1:1998

Numéros des publications

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

Publications consolidées

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

Validité de la présente publication

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

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

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

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

Terminologie, symboles graphiques et littéraux

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

Pour les symboles graphiques, les symboles littéraux et les signes d'usage général approuvés par la CEI, le lecteur consultera la CEI 60027: *Symboles littéraux à utiliser en électrotechnique,* la CEI 60417: S*ymboles graphiques utilisables sur le matériel. Index, relevé et compilation des feuilles individuelles,* et la CEI 60617: *Symboles graphiques pour schémas.*

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

Numbering

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

Consolidated publications

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

Validity of this publication

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

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

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

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

Terminology, graphical and letter symbols

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

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

* See web site address on title page.

NORME INTERNATIONALE

INTERNATIONAL STANDARD

CEI
IEC
61508-1

Première édition
First edition
1998-12

PUBLICATION FONDAMENTALE DE SÉCURITÉ
BASIC SAFETY PUBLICATION

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

Partie 1: Prescriptions générales –

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

Part 1: General requirements

International Electrotechnical Commission 3, rue de Varembé Geneva, Switzerland
Telefax: +41 22 919 0300 e-mail: inmail@iec.ch IEC web site http://www.iec.ch

Commission Electrotechnique Internationale
International Electrotechnical Commission
Международная Электротехническая Комиссия

CODE PRIX
PRICE CODE XA

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

SOMMAIRE

Pages

CONTENTS

Annexes

Tableaux

Figures

Annexes

Tables

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.

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

FUNCTIONAL SAFETY OF ELECTRICAL/ELECTRONIC/PROGRAMMABLE ELECTRONIC SAFETY-RELATED SYSTEMS –

Part 1: General requirements

FOREWORD

1) The IEC (International Electrotechnical Commission) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of the IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, the IEC publishes International Standards. Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. The IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
2) The formal decisions or agreements of the IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested National Committees.
3) The documents produced have the form of recommendations for international use and are published in the form of standards, technical reports or guides and they are accepted by the National Committees in that sense.
4) In order to promote international unification, IEC National Committees undertake to apply IEC International Standards transparently to the maximum extent possible in their national and regional standards. Any divergence between the IEC Standard and the corresponding national or regional standard shall be clearly indicated in the latter.
5) The IEC provides no marking procedure to indicate its approval and cannot be rendered responsible for any equipment declared to be in conformity with one of its standards.
6) Attention is drawn to the possibility that some of the elements of this International Standard may be the subject of patent rights. The IEC shall not be held responsible for identifying any or all such patent rights.

International Standard IEC 61508-1 has been prepared by subcommittee 65A: System aspects, of IEC technical committee 65: Industrial-process measurement and control.

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

FDIS	Report on voting
65A/264/FDIS	65A/274/RVD

Full information on the voting for the approval of this standard can be found in the report on voting indicated in the above table.

Annexes A, B and C are for information only.

It has the status of a basic safety publication in accordance with IEC Guide 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.

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

– Part 1: General requirements
– Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems
– Part 3: Software requirements
– Part 4: Definitions and abbreviations
– Part 5: Examples of methods for the determination of safety integrity levels
– Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3
– Part 7: Overview of techniques and measures

The contents of the corrigendum of April 1999 have been included in this copy.

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;

INTRODUCTION

Systems comprised of electrical and/or electronic components have been used for many years to perform safety functions in most application sectors. Computer-based systems (generically referred to as programmable electronic systems (PESs)) are being used in all application sectors to perform non-safety functions and, increasingly, to perform safety functions. If computer system technology is to be effectively and safely exploited, it is essential that those responsible for making decisions have sufficient guidance on the safety aspects on which to make these decisions.

This International Standard sets out a generic approach for all safety lifecycle activities for systems comprised of electrical and/or electronic and/or programmable electronic components (electrical/electronic/programmable electronic systems (E/E/PESs)) that are used to perform safety functions. This unified approach has been adopted in order that a rational and consistent technical policy be developed for all electrically-based safety-related systems. A major objective is to facilitate the development of application sector standards.

In most situations, safety is achieved by a number of protective systems which rely on many technologies (for example mechanical, hydraulic, pneumatic, electrical, electronic, programmable electronic). Any safety strategy must therefore consider not only all the elements within an individual system (for example sensors, controlling devices and actuators) but also all the safety-related systems making up the total combination of safety-related systems. Therefore, while this International Standard is concerned with electrical/electronic/programmable electronic (E/E/PE) safety-related systems, it may also provide a framework within which safety-related systems based on other technologies may be considered.

It is recognized that there is a great variety of E/E/PES applications in a variety of application sectors and covering a wide range of complexity, hazard and risk potentials. In any particular application, the required safety measures will be dependent on many factors specific to the application. This International Standard, by being generic, will enable such measures to be formulated in future application sector international standards.

This International Standard

– considers all relevant overall, E/E/PES and software safety lifecycle phases (for example, from initial concept, through design, implementation, operation and maintenance to decommissioning) when E/E/PESs are used to perform safety functions;
– has been conceived with a rapidly developing technology in mind; the framework is sufficiently robust and comprehensive to cater for future developments;
– enables application sector international standards, dealing with safety-related E/E/PESs, to be developed; the development of application sector international standards, within the framework of this standard, should lead to a high level of consistency (for example, of underlying principles, terminology etc.) both within application sectors and across application sectors; this will have both safety and economic benefits;
– provides a method for the development of the safety requirements specification necessary to achieve the required functional safety for E/E/PE safety-related systems;

– 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.

– uses safety integrity levels for specifying the target level of safety integrity for the safety functions to be implemented by the E/E/PE safety-related systems;

– adopts a risk-based approach for the determination of the safety integrity level requirements;

– sets numerical target failure measures for E/E/PE safety-related systems which are linked to the safety integrity levels;

– sets a lower limit on the target failure measures, in a dangerous mode of failure, that can be claimed for a single E/E/PE safety-related system; for E/E/PE safety-related systems operating in

  – a low demand mode of operation, the lower limit is set at an average probability of failure of 10^{-5} to perform its design function on demand,

  – a high demand or continuous mode of operation, the lower limit is set at a probability of a dangerous failure of 10^{-9} per hour;

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

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

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

Partie 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.

FUNCTIONAL SAFETY OF ELECTRICAL/ELECTRONIC/PROGRAMMABLE ELECTRONIC SAFETY-RELATED SYSTEMS –

Part 1: General requirements

1 Scope

1.1 This International Standard covers those aspects to be considered when electrical/electronic/programmable electronic systems (E/E/PESs) are used to carry out safety functions. A major objective of this standard is to facilitate the development of application sector international standards by the technical committees responsible for the application sector. This will allow all the relevant factors, associated with the application, to be fully taken into account and thereby meet the specific needs of the application sector. A dual objective of this standard is to enable the development of electrical/electronic/programmable electronic (E/E/PE) safety-related systems where application sector international standards may not exist.

1.2 In particular, this standard

a) applies to safety-related systems when one or more of such systems incorporates electrical/electronic/programmable electronic devices;

NOTE 1 – In the context of low complexity E/E/PE safety-related systems, certain requirements specified in this standard may be unnecessary, and exemption from compliance with such requirements is possible (see 4.2, and the definition of a low complexity E/E/PE safety-related system in 3.4.4 of IEC 61508-4).

NOTE 2 – Although a person can form part of a safety-related system (see 3.4.1 of IEC 61508-4), human factor requirements related to the design of E/E/PE safety-related systems are not considered in detail in this standard.

b) is generically-based and applicable to all E/E/PE safety-related systems irrespective of the application;

c) covers possible hazards caused by failures of the safety functions to be performed by E/E/PE safety-related systems, as distinct from hazards arising from the E/E/PE equipment itself (for example electric shock etc);

d) does not cover E/E/PE systems where

   – a single E/E/PE system is capable of providing the necessary risk reduction, and

   – the required safety integrity of the E/E/PE system is less than that specified for safety integrity level 1 (the lowest safety integrity level in this standard).

e) is mainly concerned with the E/E/PE safety-related systems whose failure could have an impact on the safety of persons and/or the environment; however, it is recognized that the consequences of failure could also have serious economic implications and in such cases this standard could be used to specify any E/E/PE system used for the protection of equipment or product;

NOTE – See 3.1.1 and 7.3.1.2 of IEC 61508-4.

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.

f) considers E/E/PE safety-related systems, other technology safety-related systems and external risk reduction facilities in order that the safety requirements specification for the E/E/PE safety-related systems can be determined in a systematic, risk-based manner;

g) uses an overall safety lifecycle model as the technical framework for dealing systematically with the activities necessary for ensuring the functional safety of the E/E/PE safety-related systems;

NOTE 3 – The early phases of the overall safety lifecycle include, of necessity, consideration of other technology (as well as the E/E/PE safety-related systems) and external risk reduction facilities, in order that the safety requirements specification for the E/E/PE safety-related systems can be developed in a systematic, risk-based manner.

NOTE 4 – Although the overall safety lifecycle is primarily concerned with E/E/PE safety-related systems, it could also provide a technical framework for the consideration of any safety-related system irrespective of the technology of that system (for example mechanical, hydraulic or pneumatic).

h) does not specify the safety integrity levels required for sector applications (which must be based on detailed information and knowledge of the sector application). The technical committees responsible for the specific application sectors shall specify, where appropriate, the safety integrity levels in the application sector standards;

i) provides general requirements for E/E/PE safety-related systems where no application sector standards exist;

j) does not cover the precautions that may be necessary to prevent unauthorized persons damaging, and/or otherwise adversely affecting, the functional safety of E/E/PE safety-related systems.

1.3 This part of IEC 61508 specifies the general requirements that are applicable to all parts. Other parts of IEC 61508 concentrate on more specific topics:

– parts 2 and 3 provide additional and specific requirements for E/E/PE safety-related systems (for hardware and software);

– part 4 gives definitions and abbreviations that are used throughout this standard;

– part 5 provides guidelines on the application of part 1 in determining safety integrity levels, by showing example methods;

– part 6 provides guidelines on the application of parts 2 and 3;

– part 7 contains an overview of techniques and measures.

1.4 Parts 1, 2, 3 and 4 of this standard are basic safety publications, although this status does not apply in the context of low complexity E/E/PE safety-related systems (see 3.4.4 of part 4). As basic safety publications, they are intended for use by technical committees in the preparation of standards in accordance with the principles contained in *IEC Guide 104* and *ISO/IEC Guide 51*. Parts 1, 2, 3, and 4 are also intended for use as stand-alone publications.

One of the responsibilities of a technical committee is, wherever applicable, to make use of basic safety publications in the preparation of its publications. In this context, the requirements, test methods or test conditions of this basic safety publication will not apply unless specifically referred to or included in the publications prepared by those technical committees.

NOTE – In the USA and Canada, until the proposed process sector implementation of IEC 61508 is published as an international standard in the USA and Canada, existing national process safety standards based on IEC 61508 (i.e. ANSI/ISA S84.01-1996) (see reference [8] in annex C) can be applied to the process sector instead of IEC 61508.

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

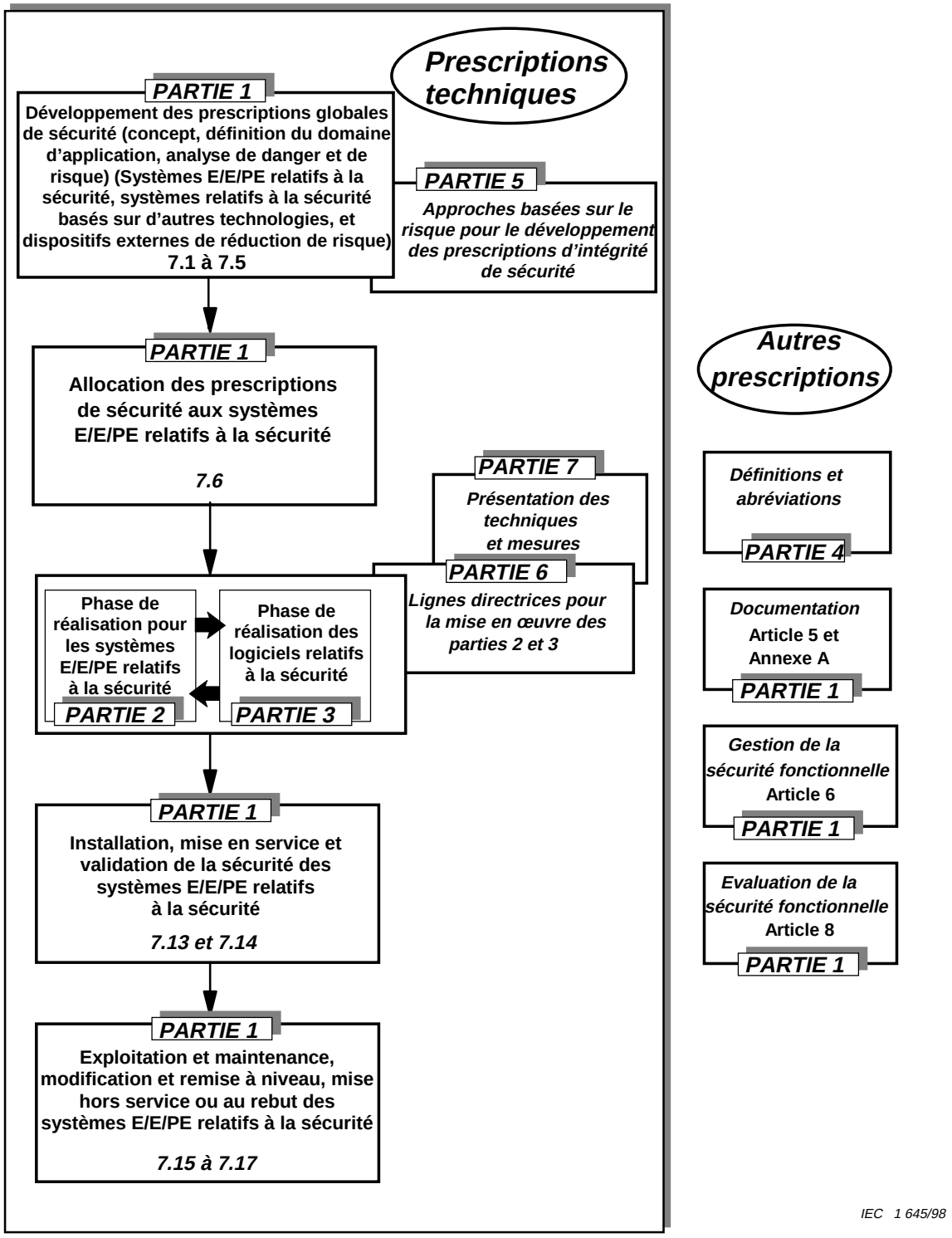


Figure 1 – Structure générale de la présente norme

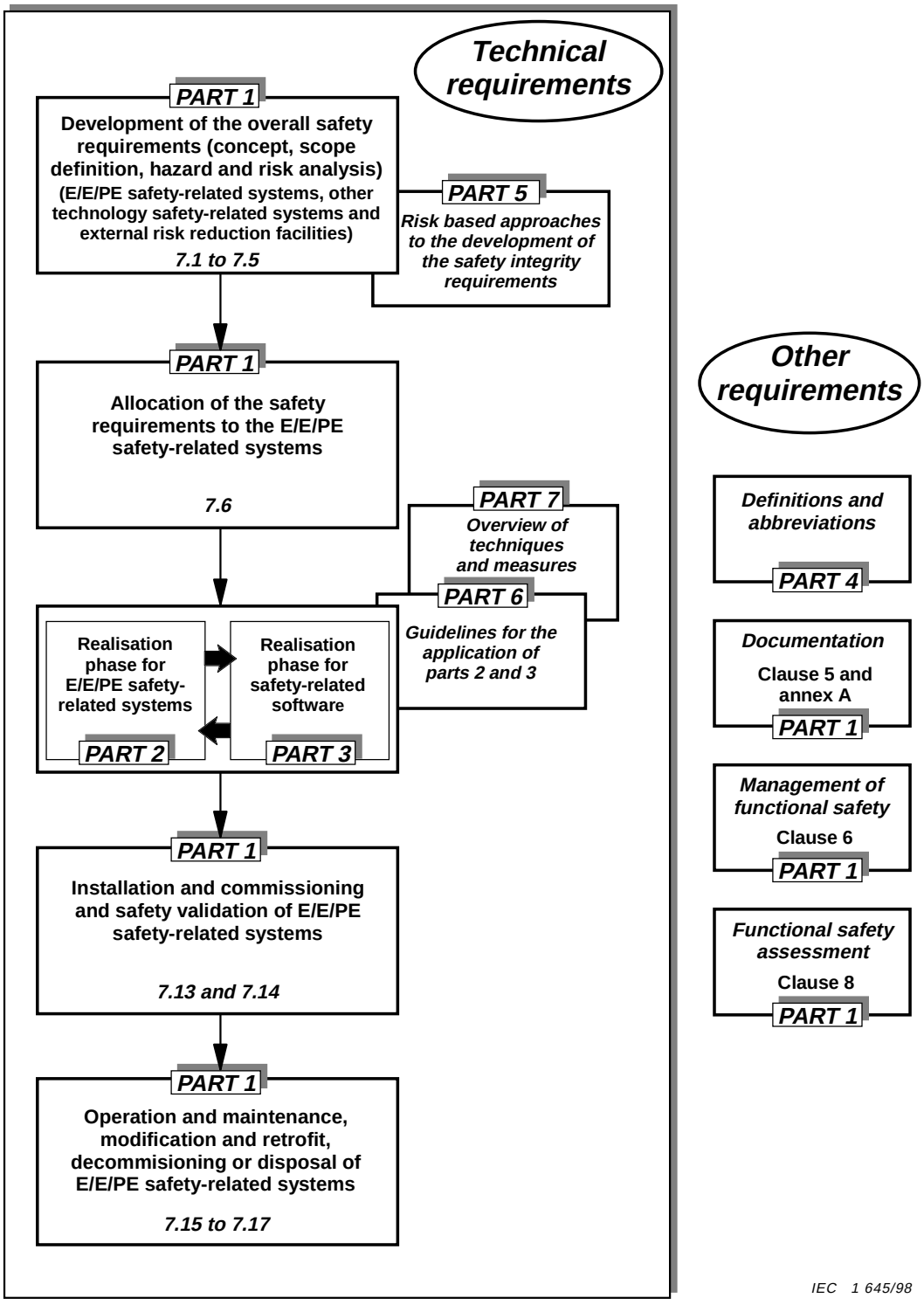


Figure 1 – Overall framework of this standard

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.

2 Normative references

The following normative documents contain provisions which, through reference in this text, constitute provisions of this part of IEC 61508. For dated references, subsequent amendments to, or revisions of, any of these publications do not apply. However, parties to agreements based on this part of IEC 61508 are encouraged to investigate the possibility of applying the most recent editions of the normative documents indicated below. For undated references, the latest edition of the normative document referred to applies. Members of IEC and ISO maintain registers of currently valid international standards.

ISO/IEC Guide 51:1990, *Guidelines for the inclusion of safety aspects in standards*

IEC Guide 104:1997, *Guide to the drafting of safety standards, and the role of Committees with safety pilot functions and safety group functions*

IEC 61508-2, — *Functional safety of electrical/electronical/programmable electronic safety-related systems – Part 2: Requirements for electrical/electronical/programmable electronic safety-related systems* [1)]

IEC 61508-3:1998, *Functional safety of electrical/electronical/programmable electronic safety-related systems – Part 3: Software requirements*

IEC 61508-4:1998, *Functional safety of electrical/electronical/programmable electronic safety-related systems – Part 4: Definitions and abbreviations*

IEC 61508-5:1998, *Functional safety of electrical/electronical/programmable electronic safety-related systems – Part 5: Examples of methods for the determination of safety integrity levels*

IEC 61508-6, — *Functional safety of electrical/electronical/programmable electronic safety-related systems – Part 6: Guidelines on the application of parts 2 and 3* [1)]

IEC 61508-7, — *Functional safety of electrical/electronical/programmable electronic safety-related systems – Part 7: Overview of techniques and measures* [2)]

3 Definitions and abbreviations

For the purposes of this standard, the definitions and abbreviations given in part 4 apply.

_____

2) To be published.

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.

4 Conformance to this standard

4.1 To conform to this standard it shall be demonstrated that the requirements have been satisfied to the required criteria specified (for example safety integrity level) and therefore, for each clause or subclause, all the objectives have been met.

NOTE – It is not generally possible to single out any one factor that determines the degree to which a requirement is to be satisfied (degree of rigour). It will be dependent upon a number of factors which, themselves, may depend upon the specific overall, E/E/PES or software safety lifecycle phase and activity. The factors will include:

– nature of the hazards;

– consequence and risk reduction;

– safety integrity level;

– type of implementation technology;

– size of systems;

– number of teams involved;

– physical distribution;

– novelty of design.

4.2 This standard specifies the requirements for E/E/PE safety-related systems and has been developed to meet the full range of complexity associated with such systems. However, for low complexity E/E/PE safety-related systems (see 3.4.4 of IEC 61508-4), where dependable field experience exists which provides the necessary confidence that the required safety integrity can be achieved, the following options are available:

– in application sector standards implementing the requirements of IEC 61508-1 to IEC 61508-7, certain requirements may be unnecessary and exemption from compliance with such requirements is acceptable;

– if this standard is used directly for those situations where no application sector international standard exists, certain of the requirements specified in this standard may be unnecessary and exemption from compliance with such requirements is acceptable providing this is justified.

4.3 Application sector international standards for E/E/PE safety-related systems developed within the framework of this standard shall take into account the requirements of ISO/IEC Guide 51 and IEC Guide 104.

5 Documentation

5.1 Objectives

5.1.1 The first objective of the requirements of this clause is to specify the necessary information to be documented in order that all phases of the overall, E/E/PES and software safety lifecycles can be effectively performed.

5.1.2 Le second objectif des prescriptions de cet article est de spécifier l'information qu'il sera nécessaire de documenter afin que les activités de gestion de la sécurité fonctionnelle (voir article 6), de vérification (voir 7.18) et d'évaluation de la sécurité fonctionnelle (voir article 8) puissent s'accomplir efficacement.

NOTE 1– Les prescriptions de documentation de la présente norme se rapportent, essentiellement, à l'information en tant que telle plutôt qu'aux documents physiques. L'information peut ne faire partie d'aucun document, sauf si c'est explicitement indiqué dans le paragraphe s'y rapportant.

NOTE 2 – La documentation peut être disponible sous différentes formes (par exemple sur papier, film, ou tout support de donnée devant être affiché sur écran).

NOTE 3 – Voir l'annexe A pour des exemples de structure de documentation.

NOTE 4 – Voir aussi la référence [4] à l'annexe C.

5.2 Prescriptions

5.2.1 Pour chaque phase réalisée du cycle de vie de sécurité global du système E/E/PE et du logiciel, la documentation doit contenir l'information nécessaire et suffisante à la réalisation efficace des phases suivantes et des activités de vérification.

NOTE – Ce que l'on entend par «information suffisante» dépend d'un certain nombre de facteurs, dont la complexité et la taille du système de sécurité E/E/PE et les prescriptions dépendant des spécificités de l'application.

5.2.2 La documentation doit contenir l'information nécessaire et suffisante pour la gestion de la sécurité fonctionnelle (article 6).

NOTE – Voir notes en 5.1.2.

5.2.3 La documentation doit contenir l'information nécessaire et suffisante à la mise en œuvre et à l'évaluation de la sécurité fonctionnelle, ainsi que l'information et les résultats provenant de toute évaluation de la sécurité fonctionnelle.

NOTE – Voir notes en 5.1.2.

5.2.4 Sauf justification contraire donnée dans la planification de la sécurité fonctionnelle ou sauf spécification contraire dans la norme d'application sectorielle, l'information à documenter doit être telle que mentionnée dans les divers articles de la présente norme.

5.2.5 La disponibilité de la documentation doit être suffisante pour permettre l'accomplissement des activités dans le respect des articles de la présente norme.

NOTE – La personne (physique ou morale) appropriée n'a besoin de détenir que l'information strictement nécessaire à la réalisation d'une activité déterminée, prescrite par la présente norme.

5.2.6 La documentation doit

– être concise et précise;
– être facile à comprendre par les personnes qui devront l'utiliser;
– correspondre à son objectif;
– être accessible et actualisable.

5.2.7 La documentation ou les ensembles d'informations doivent comporter des titres ou des noms indiquant le domaine d'application de leurs contenus, et posséder un système d'index permettant un accès rapide aux informations prescrites dans la présente norme.

5.2.8 La structure de la documentation peut tenir compte des procédures de l'entreprise et des habitudes de travail de secteurs d'application spécifiques.

5.2.9 Les documents ou ensembles d'informations doivent comporter un index de révision (numéros de version) permettant d'identifier les différentes versions d'un même document.

5.1.2 The second objective of the requirements of this clause is to specify the necessary information to be documented in order that the management of functional safety (see clause 6), verification (see 7.18) and the functional safety assessment (see clause 8) activities can be effectively performed.

NOTE 1 – The documentation requirements in this standard are concerned, essentially, with information rather than physical documents. The information need not be contained in physical documents unless this is explicitly declared in the relevant subclause.

NOTE 2 – Documentation may be available in different forms (for example on paper, film, or any data medium to be presented on screens or displays).

NOTE 3 – See annex A concerning possible documentation structures.

NOTE 4 – See reference [4] in annex C.

5.2 Requirements

5.2.1 The documentation shall contain sufficient information, for each phase of the overall, E/E/PES and software safety lifecycles completed, necessary for effective performance of subsequent phases and verification activities.

NOTE – What constitutes sufficient information will be dependent upon a number of factors, including the complexity and size of the E/E/PE safety-related systems and the requirements relating to the specific application.

5.2.2 The documentation shall contain sufficient information required for the management of functional safety (clause 6).

NOTE – See notes to 5.1.2.

5.2.3 The documentation shall contain sufficient information required for the implementation of a functional safety assessment, together with the information and results derived from any functional safety assessment.

NOTE – See notes to 5.1.2.

5.2.4 Unless justified in the functional safety planning or specified in the application sector standard, the information to be documented shall be as stated in the various clauses of this standard.

5.2.5 The availability of documentation shall be sufficient for the duties to be performed in respect of the clauses of this standard.

NOTE – Only the information necessary to undertake a particular activity, required by this standard, need be held by each relevant party.

5.2.6 The documentation shall

– be accurate and concise;
– be easy to understand by those persons having to make use of it;
– suit the purpose for which it is intended;
– be accessible and maintainable.

5.2.7 The documentation or set of information shall have titles or names indicating the scope of the contents, and some form of index arrangement so as to allow ready access to the information required in this standard.

5.2.8 The documentation structure may take account of company procedures and the working practices of specific application sectors.

5.2.9 The documents or set of information shall have a revision index (version numbers) to make it possible to identify different versions of the document.

5.2.10 Les documents ou ensembles d'informations doivent être structurés de façon à permettre la recherche d'information pertinente. Il doit être possible d'identifier la dernière révision (version) d'un document ou d'un ensemble d'informations.

NOTE – L'organisation pratique de la documentation sera fonction d'un certain nombre de facteurs, comme la dimension du système, sa complexité ou encore les prescriptions en matière d'organisation.

5.2.11 Tous les documents pertinents doivent faire l'objet de révisions, d'amendements, de revues et d'approbations, cela dans le cadre d'un plan approprié de contrôle des documents.

NOTE – Lorsque des outils de production automatique ou semi-automatique de la documentation sont utilisés, des procédures spéciales peuvent être nécessaires pour s'assurer que des mesures efficaces pour la gestion des versions ou d'autres aspects du contrôle des documents sont en place.

6 Gestion de la sécurité fonctionnelle

6.1 Objectifs

6.1.1 Le premier objectif des prescriptions de cet article est de spécifier les activités techniques et de gestion qu'il sera nécessaire de réaliser pendant les phases du cycle de vie global des logiciels et systèmes E/E/PE pour garantir la sécurité fonctionnelle prescrite des systèmes de sécurité E/E/PE.

6.1.2 Le second objectif des prescriptions de cet article est de spécifier les responsabilités des personnes, services et organisations responsables pour chaque phase du cycle de vie global des logiciels et systèmes E/E/PE ou pour les activités comprises dans chaque phase.

NOTE – Les mesures d'organisation dont traite cet article permettent la mise en œuvre efficace des prescriptions techniques et ont pour unique but la réalisation et le maintien de la sécurité fonctionnelle des systèmes de sécurité E/E/PE. Les prescriptions techniques nécessaires pour maintenir la sécurité fonctionnelle doivent normalement être spécifiées dans une partie de la documentation donnée par le fournisseur du système de sécurité E/E/PE.

6.2 Prescriptions

6.2.1 Les organismes ou les individus qui ont une responsabilité globale pour l'une ou plusieurs des phases du cycle de vie de sécurité global des logiciels ou systèmes E/E/PE, doivent, à l'égard des phases pour lesquelles ils ont une responsabilité globale, spécifier toutes les activités techniques et de gestion qui sont nécessaires pour s'assurer que les systèmes de sécurité E/E/PE réalisent et maintiennent la sécurité fonctionnelle prescrite. En particulier, il convient que les éléments suivants soient pris en considération:

a) la politique et la stratégie pour réaliser la sécurité fonctionnelle, y compris les moyens pour évaluer sa réalisation, et les moyens de communication au sein des organisations permettant d'obtenir une culture de sécurité du travail;

b) l'identification des personnes, services et autres organisations qui sont responsables de l'exécution et de la revue des phases appropriées du cycle de vie global de sécurité des logiciels et systèmes E/E/PE (y compris, lorsque c'est utile, les administrations d'autorisation ou les organismes de réglementation de la sécurité);

c) les phases du cycle de vie de sécurité global des logiciels ou systèmes E/E/PE devant être appliquées;

d) la façon dont l'information doit être structurée et l'étendue de l'information devant être documentée (voir article 5);

e) les mesures choisies et les techniques utilisées pour satisfaire aux prescriptions d'un article ou d'un paragraphe déterminé (voir CEI 61508-2, CEI 61508-3 et 61508-6);

f) les activités d'évaluation de la sécurité fonctionnelle (voir article 8);

5.2.10 The documents or set of information shall be so structured as to make it possible to search for relevant information. It shall be possible to identify the latest revision (version) of a document or set of information.

NOTE – The physical structure of the documentation will vary depending upon a number of factors such as the size of the system, its complexity and organizational requirements.

5.2.11 All relevant documents shall be revised, amended, reviewed, approved and be under the control of an appropriate document control scheme.

NOTE – Where automatic or semi-automatic tools are used for the production of documentation, specific procedures may be necessary to ensure effective measures are in place for the management of versions or other control aspects of the documents.

6 Management of functional safety

6.1 Objectives

6.1.1 The first objective of the requirements of this clause is to specify the management and technical activities during the overall, E/E/PES and software safety lifecycle phases which are necessary for the achievement of the required functional safety of the E/E/PE safety-related systems.

6.1.2 The second objective of the requirements of this clause is to specify the responsibilities of the persons, departments and organizations responsible for each overall, E/E/PES and software safety lifecycle phase or for activities within each phase.

NOTE – The organizational measures dealt with in this clause provide for the effective implementation of the technical requirements and are solely aimed at the achievement and maintenance of functional safety of the E/E/PE safety-related systems. The technical requirements necessary for maintaining functional safety will normally be specified as part of the information provided by the supplier of the E/E/PE safety-related system.

6.2 Requirements

6.2.1 Those organizations or individuals that have overall responsibility for one or more phases of the overall, E/E/PES or software safety lifecycles shall, in respect of those phases for which they have overall responsibility, specify all management and technical activities that are necessary to ensure that the E/E/PE safety-related systems achieve and maintain the required functional safety. In particular, the following should be considered:

a) the policy and strategy for achieving functional safety, together with the means for evaluating its achievement, and the means by which this is communicated within the organization to ensure a culture of safe working;

b) identification of the persons, departments and organizations which are responsible for carrying out and reviewing the applicable overall, E/E/PES or software safety lifecycle phases (including, where relevant, licensing authorities or safety regulatory bodies);

c) the overall, E/E/PES or software safety lifecycle phases to be applied;

d) the way in which information is to be structured and the extent of the information to be documented (see clause 5);

e) the selected measures and techniques used to meet the requirements of a specified clause or subclause (see IEC 61508-2, IEC 61508-3 and 61508-6);

f) the functional safety assessment activities (see clause 8);

g) les procédures permettant d'assurer rapidement un suivi et une prise en compte satisfaisante des recommandations ayant trait aux systèmes de sécurité E/E/PE, et provenant de

   – l'analyse de danger et de risque (voir 7.4);

   – l'évaluation de la sécurité fonctionnelle (voir article 8);

   – les activités de vérification (voir 7.18);

   – les activités de validation (voir 7.8 et 7.14);

   – la gestion de configuration (voir 6.2.1 o), 7.16 et la CEI 61508-2 ainsi que la CEI 61508-3;

h) les procédures permettant de s'assurer que les personnes appropriées, impliquées dans l'une quelconque des activités du cycle de vie de sécurité global des logiciels ou systèmes E/E/PE, sont compétentes pour réaliser les activités dont elles sont responsables; en particulier, il convient de spécifier ce qui suit:

   – la formation du personnel pour le diagnostic et la réparation des défauts et pour le test du système;

   – la formation du personnel d'exploitation;

   – la formation continue du personnel à intervalles réguliers;

NOTE 1 – L'annexe B fournit des lignes directrices sur les prescriptions de compétence des gens impliqués dans l'une quelconque des activités du cycle de vie de sécurité global des logiciels ou systèmes E/E/PE.

i) les procédures pour que les incidents dangereux (ou les incidents pouvant potentiellement créer un danger) soient analysés, et que des recommandations soient faites pour minimiser la probabilité de réapparition;

j) les procédures d'analyse des performances en exploitation et en maintenance. En particulier les procédures pour

   – reconnaître les défauts systématiques qui pourraient compromettre la sécurité fonctionnelle, y compris les procédures utilisées pendant la maintenance systématique qui permettent de détecter les défauts cycliques;

   – évaluer si les taux de sollicitations et les taux de pannes pendant l'exploitation et la maintenance sont conformes aux hypothèses faites pendant la conception du système;

k) les prescriptions pour des audits périodiques de la sécurité fonctionnelle, conformément à ce paragraphe, incluant

   – la fréquence des audits de sécurité fonctionnelle;

   – la considération du niveau d'indépendance nécessaire pour les responsables des audits;

   – les activités de documentation et de suivi;

l) les procédures pour initier des modifications aux systèmes de sécurité (voir 7.16.2.2);

m) la procédure d'approbation et d'autorisation prescrite pour les modifications;

n) les procédures pour maintenir une information précise sur les dangers potentiels et les systèmes de sécurité;

o) les procédures pour la gestion de configuration des systèmes de sécurité E/E/PE pendant les phases du cycle de vie de sécurité global des logiciels et systèmes E/E/PE; en particulier, il convient de spécifier ce qui suit:

   – l'étape où un contrôle formel de configuration doit être mis en œuvre;

   – les procédures devant être utilisées pour identifier de façon unique chaque partie constitutive d'un élément (matériel ou logiciel);

   – les procédures pour éviter que des éléments non autorisés n'entrent en service;

NOTE 2 – Pour de plus amples détails sur la gestion de configuration, voir les références [6] et [7] à l'annexe C.

p) lorsque cela est pertinent, les dispositions de formation et d'information pour les services d'intervention d'urgence.

g) the procedures for ensuring prompt follow-up and satisfactory resolution of recommendations relating to E/E/PE safety-related systems arising from
   - hazard and risk analysis (see 7.4);
   - functional safety assessment (see clause 8);
   - verification activities (see 7.18);
   - validation activities (see 7.8 and 7.14);
   - configuration management (see 6.2.1 o), 7.16 and IEC 61508-2 and IEC 61508-3);

h) the procedures for ensuring that applicable parties involved in any of the overall, E/E/PES or software safety lifecycle activities are competent to carry out the activities for which they are accountable; in particular, the following should be specified:
   - the training of staff in diagnosing and repairing faults and in system testing;
   - the training of operations staff;
   - the retraining of staff at periodic intervals;

NOTE 1 – Annex B provides guidelines on the competence requirements of those involved in any overall, E/E/PES or software safety lifecycle activity.

i) the procedures which ensure that hazardous incidents (or incidents with potential to create hazards) are analysed, and that recommendations made to minimise the probability of a repeat occurrence;

j) the procedures for analysing operations and maintenance performance. In particular procedures for
   - recognising systematic faults which could jeopardise functional safety, including procedures used during routine maintenance which detect recurring faults;
   - assessing whether the demand rates and failure rates during operation and maintenance are in accordance with assumptions made during the design of the system;

k) requirements for periodic functional safety audits in accordance with this subclause including
   - the frequency of the functional safety audits;
   - consideration as to the level of independence required for those responsible for the audits;
   - the documentation and follow-up activities;

l) the procedures for initiating modifications to the safety-related systems (see 7.16.2.2);

m) the required approval procedure and authority for modifications;

n) the procedures for maintaining accurate information on potential hazards and safety-related systems;

o) the procedures for configuration management of the E/E/PE safety-related systems during the overall, E/E/PES and software safety lifecycle phases; in particular the following should be specified:
   - the stage at which formal configuration control is to be implemented;
   - the procedures to be used for uniquely identifying all constituent parts of an item (hardware and software);
   - the procedures for preventing unauthorized items from entering service;

NOTE 2 – For more details on configuration management see references [6] and [7] in annex C.

p) where appropriate, the provision of training and information for the emergency services.

6.2.2 Les activités spécifiées suite à 6.2.1 doivent être mises en œuvre et leur avancement doit être surveillé.

6.2.3 Les prescriptions développées suite à 6.2.1 doivent être revues de manière formelle par les organismes concernés et doivent faire l'objet d'un accord.

6.2.4 Toute personne spécifiée comme étant responsable pour la gestion des activités de sécurité fonctionnelle doit être informée des responsabilités qui lui sont assignées.

6.2.5 Les fournisseurs offrant des produits ou services à une organisation ayant une responsabilité globale pour l'une ou plusieurs des phases du cycle de vie de sécurité global des logiciels ou systèmes E/E/PE (voir 6.2.1) doivent délivrer leurs produits ou services comme cela est prescrit par cette organisation et doivent posséder un système de gestion de la qualité approprié.

7 Prescriptions relatives au cycle de vie de sécurité global

7.1 Généralités

7.1.1 Introduction

7.1.1.1 Afin de traiter de façon systématique de toutes les activités nécessaires pour assurer le niveau d'intégrité de sécurité prescrit pour les systèmes E/E/PE relatifs à la sécurité, la présente norme a choisi un cycle de vie de sécurité global (voir figure 2) comme cadre technique.

NOTE – Pour la déclaration de conformité à la présente norme, il convient d'utiliser comme base le cycle de vie de sécurité global, mais un cycle de vie de sécurité global différent de celui décrit dans la figure 2 peut être utilisé, dans la mesure où les prescriptions de chaque article de la présente norme sont remplies.

7.1.1.2 Le cycle de vie de sécurité global englobe les mesures suivantes de réduction des risques:

– systèmes de sécurité E/E/PE;

– systèmes de sécurité basés sur d'autres technologies;

– dispositifs externes de réduction de risque.

7.1.1.3 La portion du cycle de vie de sécurité global qui concerne les systèmes de sécurité E/E/PE est présentée de façon détaillée à la figure 3. Elle sera appelée «cycle de vie de sécurité du système E/E/PE» et forme le cadre technique pour la CEI 61508-2. Le cycle de vie de sécurité du logiciel est présenté à la figure 4 et forme le cadre technique pour la CEI 61508-3. La relation entre le cycle de vie de sécurité global et les cycles de vie de sécurité du logiciel et des systèmes E/E/PE, pour les systèmes relatifs à la sécurité, est présentée à la figure 5.

7.1.1.4 Les figures du cycle de vie de sécurité global du logiciel et des E/E/PES (figures 2 à 4) sont des vues simplifiées de la réalité et ne représentent donc pas toutes les itérations correspondant à des phases particulières ou entre certaines phases. Cependant, l'itération est une partie essentielle et vitale d'un développement qui utilise les cycles de vie de sécurité globaux des E/E/PES et du logiciel.

7.1.1.5 Les activités relatives à la gestion de la sécurité fonctionnelle (article 6), à la vérification (7.18) et à l'évaluation de la sécurité fonctionnelle (article 8) ne sont pas représentées sur les cycles de vie de sécurité globaux des E/E/PES ou du logiciel. Ce choix a été fait pour réduire la complexité des figures du cycle de vie de sécurité global du logiciel et des E/E/PES. Lorsqu'elles sont prescrites, ces activités nécessiteront d'être appliquées à toutes les phases appropriées des cycles de vie de sécurité globaux des E/E/PES et du logiciel.

6.2.2 The activities specified as a result of 6.2.1 shall be implemented and progress monitored.

6.2.3 The requirements developed as a result of 6.2.1 shall be formally reviewed by the organizations concerned, and agreement reached.

6.2.4 All those specified as responsible for management of functional safety activities shall be informed of the responsibilities assigned to them.

6.2.5 Suppliers providing products or services to an organization having overall responsibility for one or more phases of the overall, E/E/PES or software safety lifecycles (see 6.2.1), shall deliver products or services as specified by that organization and shall have an appropriate quality management system.

7 Overall safety lifecycle requirements

7.1 General

7.1.1 Introduction

7.1.1.1 In order to deal in a systematic manner with all the activities necessary to achieve the required safety integrity level for the E/E/PE safety-related systems, this standard adopts an overall safety lifecycle (see figure 2) as the technical framework.

NOTE – The overall safety lifecyle should be used as a basis for claiming conformance to this standard, but a different overall safety lifecycle can be used to that given in figure 2, providing the objectives and requirements of each clause of this standard are met.

7.1.1.2 The overall safety lifecycle encompasses the following risk reduction measures:

– E/E/PE safety-related systems;

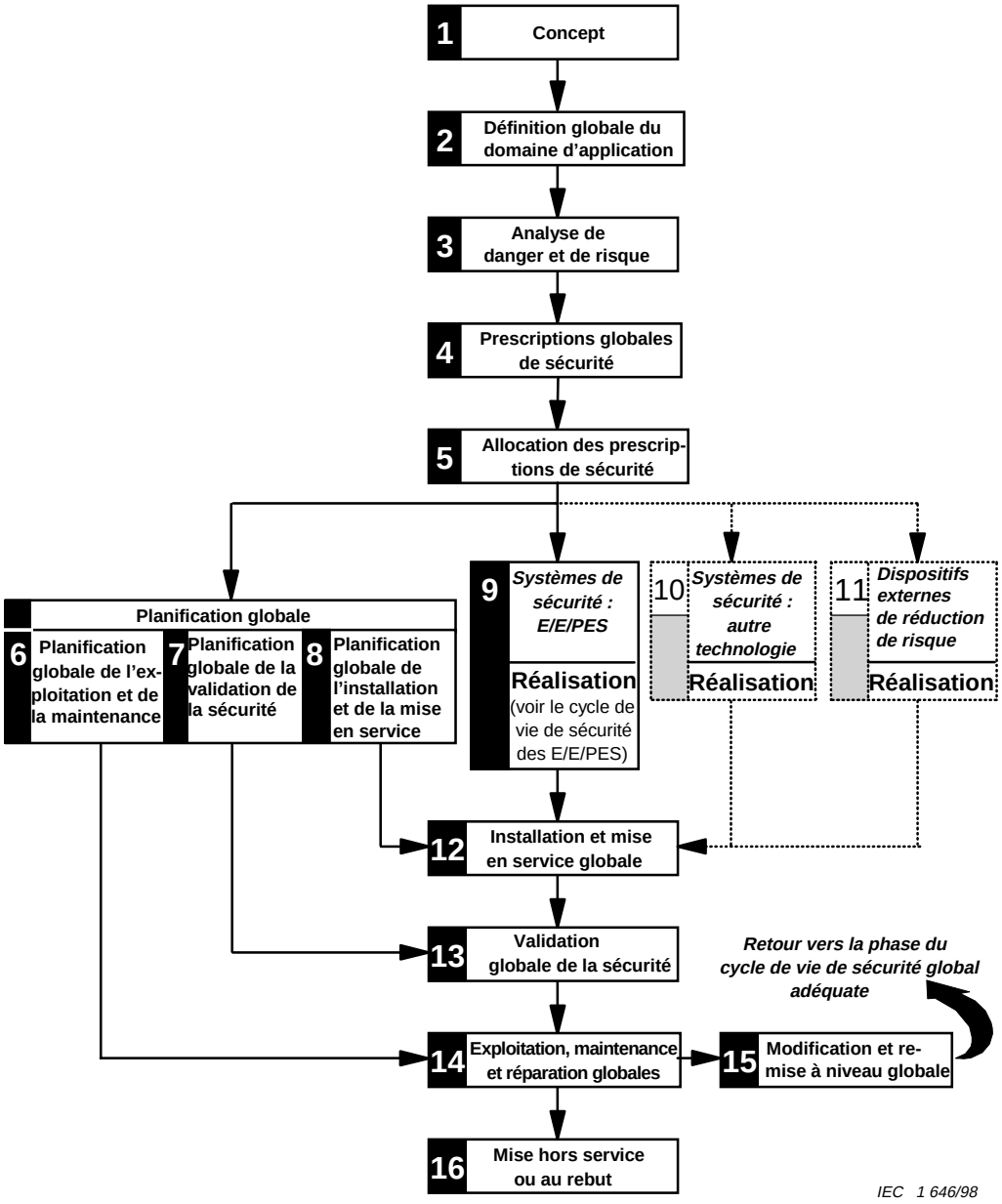
– other technology safety-related systems;

– external risk reduction facilities.

7.1.1.3 The portion of the overall safety lifecycle dealing with E/E/PE safety-related systems is expanded and shown in figure 3. This is termed the E/E/PES safety lifecycle and forms the technical framework for IEC 61508-2. The software safety lifecycle is shown in figure 4 and forms the technical framework for IEC 61508-3. The relationship of the overall safety lifecycle to the E/E/PES and software safety lifecycles for safety-related systems is shown in figure 5.

7.1.1.4 The overall, E/E/PES and software safety lifecycle figures (figures 2 to 4) are simplified views of reality and as such do not show all the iterations relating to specific phases or between phases. Iteration, however, is an essential and vital part of development through the overall, E/E/PES and software safety lifecycles.

7.1.1.5 Activities relating to the management of functional safety (clause 6), verification (7.18) and functional safety assessment (clause 8) are not shown on the overall, E/E/PES or software safety lifecycles. This has been done in order to reduce the complexity of the overall, E/E/PES and software safety lifecycle figures. These activities, where required, will need to be applied at the relevant phases of the overall, E/E/PES and software safety lifecycles.

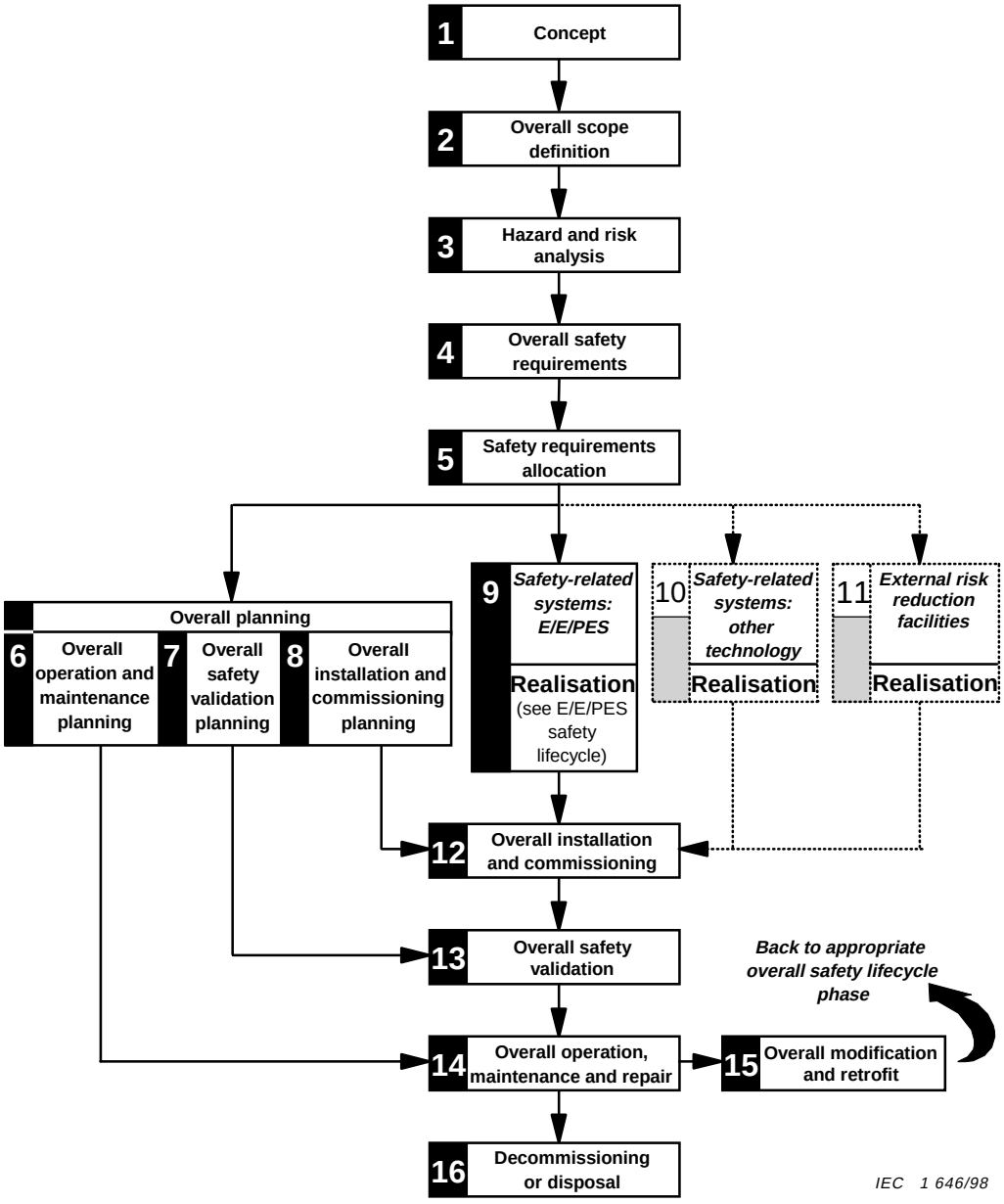


NOTE 1 – Les activités relatives à la ***vérification***, à la ***gestion de la sécurité fonctionnelle*** et à l'***évaluation de la sécurité fonctionnelle*** ne sont pas représentées pour des raisons de clarté, mais concernent toutes les phases globales du cycle de vie de sécurité des systèmes E/E/PE et du logiciel.

NOTE 2 – Les phases représentées par les étapes 10 et 11 sont en dehors du domaine de la présente norme.

NOTE 3 – La CEI 61508-2 et la CEI 61508-3 traitent de l'étape 9 (réalisation) mais elles traitent aussi, quand c'est opportun, des aspects d'électronique programmable (matériel et logiciel) des étapes 13, 14 et 15.

Figure 2 – Cycle de vie de sécurité global



NOTE 1 – Activities relating to ***verification***, ***management of functional safety*** and ***functional safety assessment*** are not shown for reasons of clarity but are relevent to all overall, E/E/PES and software safety lifecycle phases.

NOTE 2 – The phases represented by boxes 10 and 11 are outside the scope of this standard.

NOTE 3 – IEC 61508-2 and IEC 61508-3 deal with box 9 (realisation) but they also deal, where relevant, with the programmable electronic (hardware and software) aspects of boxes 13, 14 and 15.

Figure 2 – Overall safety lifecycle

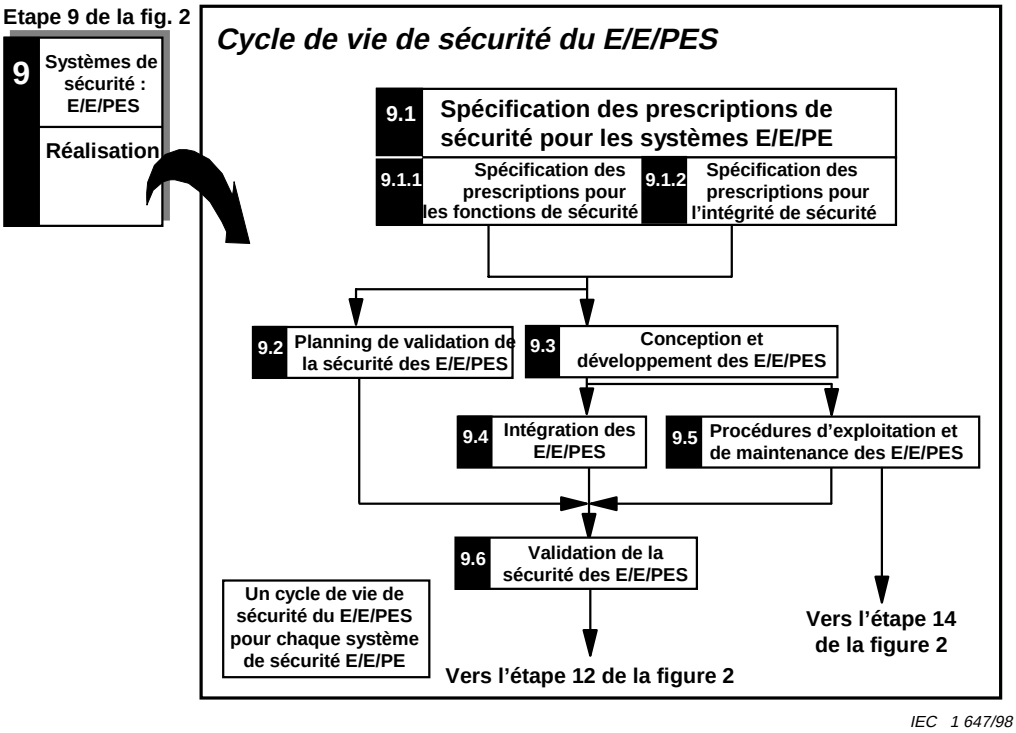


Figure 3 – Cycle de vie de sécurité du système E/E/PE (dans la phase de réalisation)

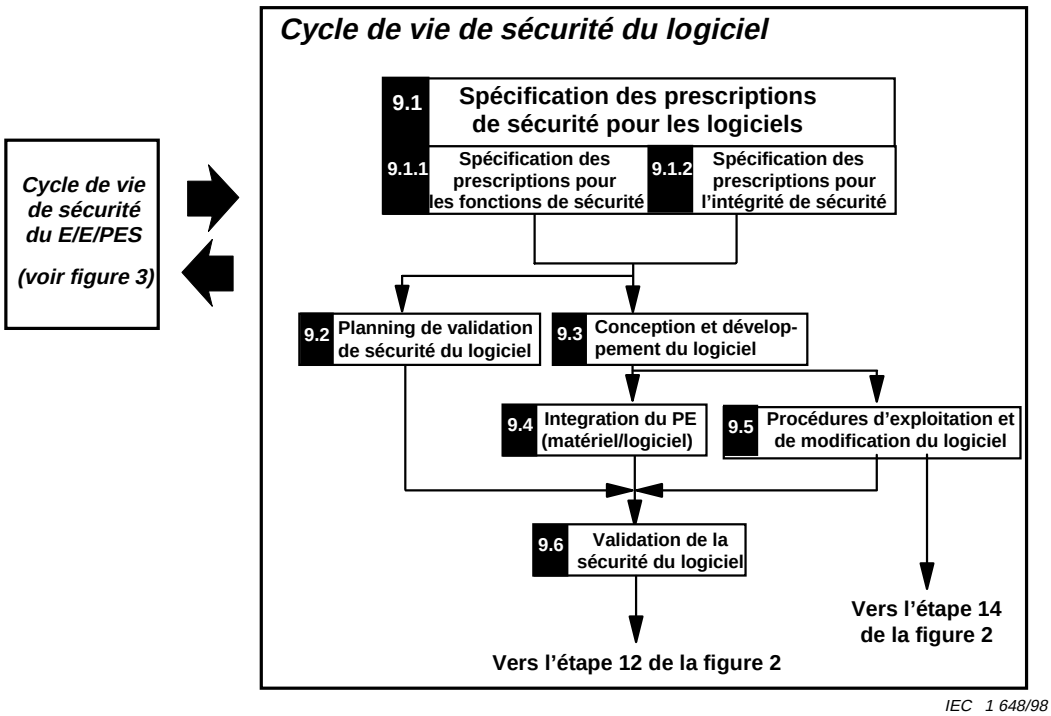


Figure 4 – Cycle de vie de sécurité du logiciel (dans la phase de réalisation)

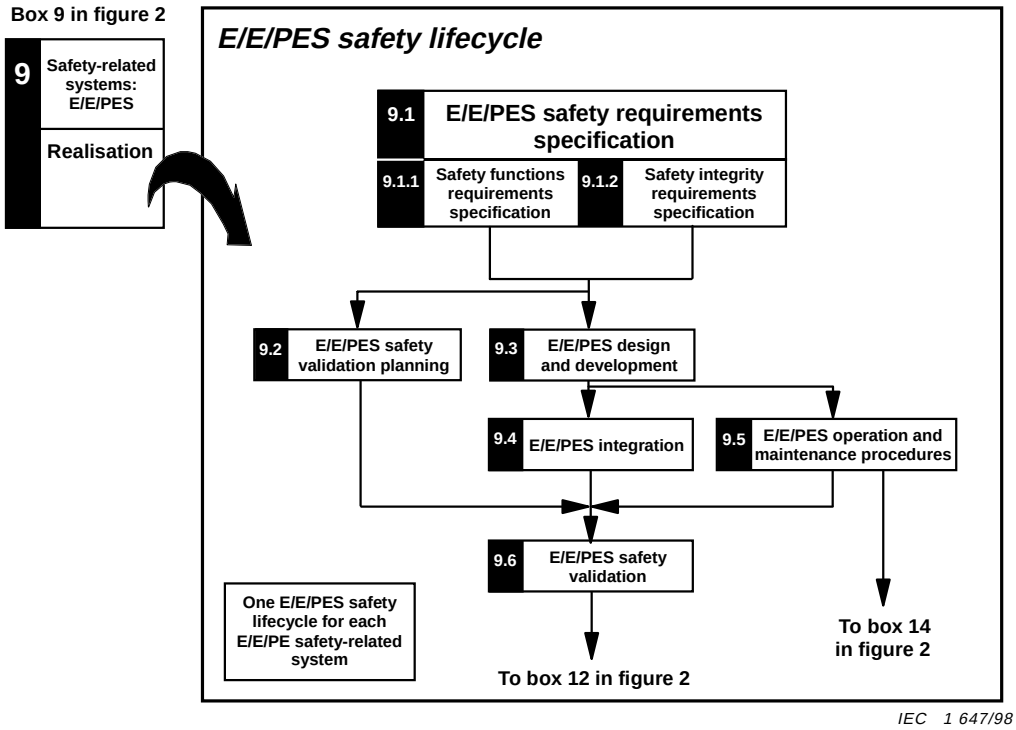


Figure 3 — E/E/PES safety lifecycle (in realisation phase)

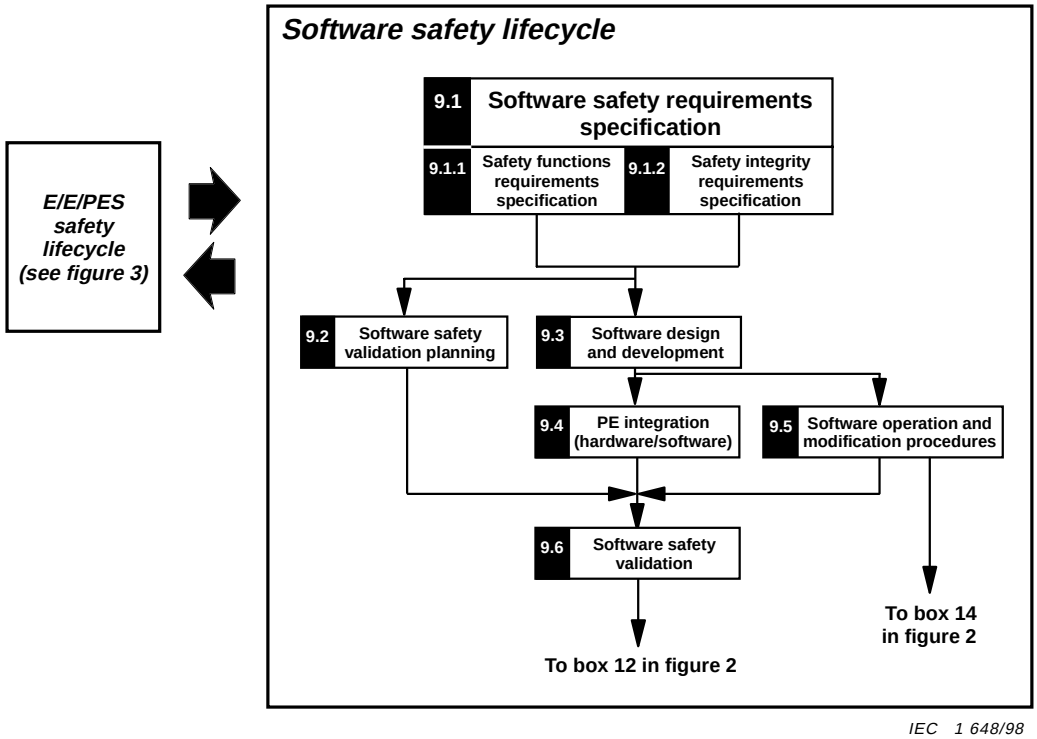


Figure 4 – Software safety lifecycle (in realisation phase)

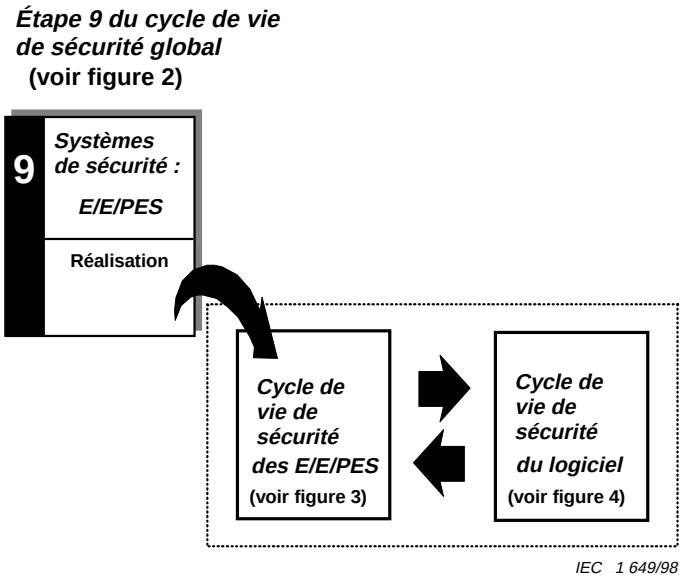


Figure 5 – Relations entre le cycle de vie de sécurité global et les cycles de vie de sécurité des E/E/PES et du logiciel

7.1.2 Objectifs et prescriptions: généralités

7.1.2.1 Les objectifs et prescriptions pour les phases du cycle de vie de sécurité global sont décrits dans les paragraphes 7.2 à 7.17. Les objectifs et prescriptions pour les phases du cycle de vie de sécurité des E/E/PES et du logiciel sont respectivement décrits dans la CEI 61508-2 et la CEI 61508-3.

NOTE – Les paragraphes 7.2 à 7.17 se rapportent aux «cases» (phases) spécifiques de la figure 2. La case correspondante est précisée dans une note au début des paragraphes.

7.1.2.2 Pour toutes les phases du cycle de vie de sécurité global, le tableau 1 indique

– les objectifs à atteindre;
– le domaine d'application de la phase;
– la référence du paragraphe contenant les prescriptions;
– les données d'entrée exigées par la phase;
– les données de sortie exigées pour être conforme aux prescriptions.

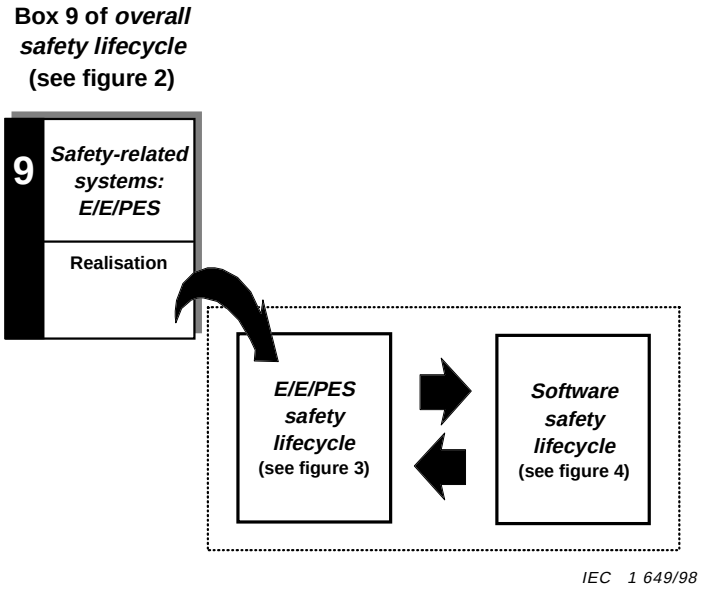


Figure 5 – Relationship of overall safety lifecycle to E/E/PES and software safety lifecycles

7.1.2 Objectives and requirements: general

7.1.2.1 The objectives and requirements for the overall safety lifecycle phases are contained in 7.2 to 7.17. The objectives and requirements for the E/E/PES and software safety lifecycle phases are contained in IEC 61508-2 and IEC 61508-3 respectively.

NOTE – 7.2 to 7.17 relate to specific boxes (phases) in figure 2. The specific box is referenced in notes to these subclauses.

7.1.2.2 For all phases of the overall safety lifecycle, table 1 indicates

– the objectives to be achieved;
– the scope of the phase;
– the reference to the subclause containing the requirements;
– the required inputs to the phase;
– the outputs required to comply with the requirements.

Tableau 1 – Cycle de vie de sécurité global: vue d'ensemble

Phase du cycle de vie de sécurité		Objectifs	Domaine	Prescriptions en	Entrées	Sorties
Numéro de case de la figure 2	**Titre**					
1	**Concept**	7.2.1: Développer un niveau de compréhension de l'EUC et son environnement (physique, légal, etc.) suffisant pour permettre aux autres activités du cycle de vie de sécurité d'être menées de façon satisfaisante.	L'EUC et son environnement (physique, légal, etc.).	7.2.2	Toute l'information appropriée nécessaire pour remplir les prescriptions de ce paragraphe.	L'information obtenue par 7.2.2.1 à 7.2.2.6.
2	**Définition globale du domaine d'application**	7.3.1: Déterminer les limites de l'EUC et du système de commande de l'EUC; Spécifier le domaine de l'analyse de danger et de risque (par exemple les processus dangereux, les dangers liés à l'environnement, etc.).	L'EUC et son environnement.	7.3.2	L'information obtenue par 7.2.2.1 à 7.2.2.6.	L'information obtenue par 7.3.2.1 à 7.3.2.5.
3	**Analyse de danger et de risque**	7.4.1: Déterminer les dangers et événements dangereux de l'EUC et du système de commande de l'EUC (dans tous les modes d'exploitation), pour toutes les situations raisonnablement prévisibles, y compris celles de défaillance et de mauvais usage; Déterminer les séquences d'événements menant aux événements dangereux déterminés; Déterminer les risques de l'EUC associés aux événements dangereux déterminés.	Le domaine dépendra de la phase atteinte dans les cycles de vie globaux de sécurité des E/E/PES et du logiciel (car il peut être nécessaire de mener plus d'une analyse de danger et de risque). Pour l'analyse préliminaire de danger et de risque, le domaine comprendra l'EUC, le système de commande de l'EUC et les facteurs humains.	7.4.2	L'information obtenue par 7.3.2.1 à 7.3.2.5.	La description et l'information relatives à l'analyse de danger et de risque.
4	**Prescriptions globales de sécurité**	7.5.1: Développer la spécification pour les prescriptions globales de sécurité, en termes de prescriptions de fonctions de sécurité et de prescriptions d'intégrité de sécurité, pour les systèmes de sécurité E/E/PE, les systèmes de sécurité basés sur une autre technologie et les dispositifs externes de réduction de risque, afin d'atteindre la sécurité fonctionnelle prescrite.	L'EUC, le système de commande de l'EUC et les facteurs humains.	7.5.2	La description et l'information relatives à l'analyse de danger et de risque.	Spécification pour les prescriptions globales de sécurité en termes de prescriptions de fonctions de sécurité et de prescriptions d'intégrité de sécurité.
5	**Allocation des prescriptions de sécurité**	7.6.1: Allouer les fonctions de sécurité, qui sont indiquées dans la spécification pour les prescriptions globales de sécurité (ensemble des prescriptions de fonctions de sécurité et des prescriptions d'intégrité de sécurité), aux systèmes de sécurité E/E/PE désignés, aux systèmes de sécurité basés sur une autre technologie et aux dispositifs externes de réduction de risque; Allouer un niveau d'intégrité de sécurité à chaque fonction de sécurité.	L'EUC, le système de commande de l'EUC et les facteurs humains.	7.6.2	Spécification pour les prescriptions globales de sécurité en termes de prescriptions de fonctions de sécurité et de prescriptions d'intégrité de sécurité.	Information et résultats de l'allocation des prescriptions de sécurité.

Table 1 – Overall safety lifecycle: overview

Safety lifecycle phase		Objectives	Scope	Require-ments sub-clause	Inputs	Outputs
Figure 2 box number	**Title**					
1	**Concept**	7.2.1: To develop a level of understanding of the EUC and its environment (physical, legislative etc.) sufficient to enable the other safety lifecycle activities to be satisfactorily carried out.	EUC and its environment (physical, legislative etc.).	7.2.2	All relevant information necessary to meet the requirements of the subclause.	Information acquired in 7.2.2.1 to 7.2.2.6.
2	**Overall scope definition**	7.3.1: To determine the boundary of the EUC and the EUC control system; To specify the scope of the hazard and risk analysis (for example process hazards, environmental hazards, etc.).	EUC and its environment.	7.3.2	Information acquired in 7.2.2.1 to 7.2.2.6.	Information acquired in 7.3.2.1 to 7.3.2.5.
3	**Hazard and risk analysis**	7.4.1: To determine the hazards and hazardous events of the EUC and the EUC control system (in all modes of operation), for all reasonably foreseeable circumstances including fault conditions and misuse; To determine the event sequences leading to the hazardous events determined; To determine the EUC risks associated with the hazardous events determined.	The scope will be dependent upon the phase reached in the overall, E/E/PES and software safety lifecycles (since it may be necessary for more than one hazard and risk analysis to be carried out). For the preliminary hazard and risk analysis, the scope will comprise the EUC, the EUC control system and human factors.	7.4.2	Information acquired in 7.3.2.1 to 7.3.2.5.	Description of, and information relating to, the hazard and risk analysis.
4	**Overall safety require-ments**	7.5.1: To develop the specification for the overall safety requirements, in terms of the safety functions requirements and safety integrity requirements, for the E/E/PE safety-related systems, other technology safety-related systems and external risk reduction facilities, in order to achieve the required functional safety.	EUC, the EUC control system and human factors.	7.5.2	Description of, and information relating to, the hazard and risk analysis.	Specification for the overall safety requirements in terms of the safety functions requirements and the safety integrity requirements.
5	**Safety require-ments allocation**	7.6.1: To allocate the safety functions, contained in the specification for the overall safety requirements (both the safety functions requirements and the safety integrity requirements), to the designated E/E/PE safety-related systems, other technology safety-related systems and external risk reduction facilities; To allocate a safety integrity level to each safety function.	EUC, the EUC control system and human factors.	7.6.2	Specification for the overall safety requirements in terms of the safety functions requirements and the safety integrity requirements.	Information and results of the safety requirements allocation.

Tableau 1 *(suite)*

Phase du cycle de vie de sécurité		Objectifs	Domaine	Prescriptions en	Entrées	Sorties
Numéro de case de la figure 2	**Titre**					
6	**Planification globale de l'exploitation et de la maintenance**	7.7.1: Développer un plan d'exploitation et de maintenance des systèmes de sécurité E/E/PE, pour assurer que la sécurité fonctionnelle prescrite est maintenue pendant l'exploitation et la maintenance.	L'EUC, le système de commande de l'EUC et les facteurs humains; les systèmes de sécurité E/E/PE.	7.7.2	Spécification pour les prescriptions globales de sécurité en termes de prescriptions de fonctions de sécurité et de prescriptions d'intégrité de sécurité.	Un plan d'exploitation et de maintenance des systèmes de sécurité E/E/PE.
7	**Planification globale de la validation de la sécurité**	7.8.1: Développer un plan pour faciliter la validation globale de la sécurité des systèmes de sécurité E/E/PE.	L'EUC, le système de commande de l'EUC et les facteurs humains; les systèmes de sécurité E/E/PE.	7.8.2	Spécification pour les prescriptions globales de sécurité en termes de prescriptions de fonctions de sécurité et de prescriptions d'intégrité de sécurité.	Un plan pour faciliter la validation des systèmes de sécurité E/E/PE.
8	**Planification globale de l'installation et de la mise en service**	7.9.1: Développer un plan pour que l'installation des systèmes de sécurité E/E/PE soit maîtrisée, en assurant que la sécurité fonctionnelle prescrite soit atteinte; Développer un plan pour que la mise en service des systèmes de sécurité E/E/PE soit maîtrisée, en assurant que la sécurité fonctionnelle prescrite soit atteinte.	L'EUC et le système de commande de l'EUC; les systèmes de sécurité E/E/PE.	7.9.2	Spécification pour les prescriptions globales de sécurité en termes de prescriptions de fonctions de sécurité et de prescriptions d'intégrité de sécurité.	Un plan pour l'installation des systèmes de sécurité E/E/PE; Un plan pour la mise en service des systèmes de sécurité E/E/PE.
9	**Systèmes de sécurité E/E/PE: réalisation**	7.10.1 et parties 2 et 3: Créer des systèmes de sécurité E/E/PE conformes à la spécification pour les prescriptions de sécurité des E/E/PES (comprenant la spécification pour les prescriptions des fonctions de sécurité des E/E/PES et la spécification pour les prescriptions d'intégrité de sécurité des E/E/PES).	Les systèmes de sécurité E/E/PE.	7.10.2, la CEI 61508-2 et la CEI 61508-3	Spécification pour les prescriptions de sécurité des E/E/PES.	Confirmation que chaque système de sécurité E/E/PE atteint la spécification des prescriptions de sécurité des E/E/PES.
10	**Systèmes de sécurité basés sur une autre technologie: réalisation**	7.11.1: Créer des systèmes de sécurité basés sur une autre technologie qui remplissent les prescriptions de fonctions de sécurité et les prescriptions d'intégrité de sécurité spécifiées pour de tels systèmes (en dehors du domaine de la présente norme).	Les systèmes de sécurité basés sur une autre technologie.	7.11.2	Spécification des prescriptions pour une autre technologie (en dehors du domaine de la présente norme et donc pas examinée plus en détail).	Confirmation que chaque système de sécurité basé sur une autre technologie atteint les prescriptions de sécurité de ce système.

Table 1 *(continued)*

Safety lifecycle phase		Objectives	Scope	Require-ments subclause	Inputs	Outputs
Figure 2 box number	**Title**					
6	**Overall operation and mainte-nance planning**	7.7.1: To develop a plan for operating and maintaining the E/E/PE safety-related systems, to ensure that the required functional safety is maintained during operation and maintenance.	EUC, the EUC control system and human factors; E/E/PE safety-related systems.	7.7.2	Specification for the overall safety requirements in terms of the safety functions requirements and the safety integrity requirements.	A plan for operating and maintaining the E/E/PE safety-related systems.
7	**Overall safety validation planning**	7.8.1: To develop a plan to facilitate the overall safety validation of the E/E/PE safety-related systems.	EUC, the EUC control system and human factors; E/E/PE safety-related systems.	7.8.2	Specification for the overall safety requirements in terms of the safety functions requirements and the safety integrity requirements.	A plan to facilitate the validation of the E/E/PE safety-related systems.
8	**Overall installa-tion and commis-sioning planning**	7.9.1: To develop a plan for the installation of the E/E/PE safety-related systems in a controlled manner, to ensure the required functional safety is achieved; To develop a plan for the commissioning of the E/E/PE safety-related systems in a controlled manner, to ensure the required functional safety is achieved.	EUC and the EUC control system; E/E/PE safety-related systems.	7.9.2	Specification for the overall safety requirements in terms of the safety functions requirements and the safety integrity requirements.	A plan for the installation of the E/E/PE safety-related systems; A plan for the commis-sioning of the E/E/PE safety-related systems.
9	**E/E/PE safety-related systems: realisation**	7.10.1 and parts 2 and 3: To create E/E/PE safety-related systems conforming to the specification for the E/E/PES safety requirements (comprising the specification for the E/E/PES safety functions requirements and the specification for the E/E/PES safety integrity requirements).	E/E/PE safety-related systems.	7.10.2, IEC 61508-2 and IEC 61508-3	Specification for the E/E/PES safety requirements.	Confirmation that each E/E/PE safety-related system meets the E/E/PES safety requirements specification.
10	**Other tech-nology safety-related systems: realisation**	7.11.1: To create other technology safety-related systems to meet the safety functions requirements and safety integrity requirements specified for such systems (outside the scope of this standard).	Other technology safety-related systems.	7.11.2	Other technology safety requirements specification (outside the scope and not considered further in this standard).	Confirmation that each other technology safety-related systems meets the safety requirements for that system.

Tableau 1 *(suite)*

Phase du cycle de vie de sécurité		Objectifs	Domaine	Prescriptions en	Entrées	Sorties
Numéro de case de la figure 2	**Titre**					
11	**Dispositifs externes de réduction de risque: réalisation**	7.12.1: Créer des dispositifs externes de réduction de risque qui remplissent les prescriptions de fonctions de sécurité et les prescriptions d'intégrité de sécurité spécifiées pour de tels dispositifs (en dehors du domaine de la présente norme).	Les dispositifs externes de réduction de risque.	7.12.2	Spécification des prescriptions pour les dispositifs externes de réduction de risque (en dehors du domaine de la présente norme et donc pas examinée plus en détail).	Confirmation que chaque dispositif externe de réduction de risque atteint les prescriptions de sécurité pour ce dispositif.
12	**Installation et mise en service globale**	7.13.1: Installer les systèmes de sécurité E/E/PE; Mettre en service les systèmes de sécurité E/E/PE.	L'EUC et le système de commande de l'EUC; Les systèmes de sécurité E/E/PE.	7.13.2	Un plan pour l'installation des systèmes de sécurité E/E/PE; Un plan pour la mise en service des systèmes de sécurité E/E/PE.	Des systèmes de sécurité E/E/PE complètement installés; Des systèmes de sécurité E/E/PE pleinement mis en service.
13	**Validation globale de la sécurité**	7.14.1: Valider le fait que les systèmes de sécurité E/E/PE remplissent la spécification pour les prescriptions globales de sécurité sur le plan des prescriptions globales de fonctions de sécurité et des prescriptions globales d'intégrité de sécurité, en tenant compte de l'allocation des prescriptions de sécurité, pour les systèmes de sécurité E/E/PE, effectuée conformément au 7.6.	L'EUC et le système de commande de l'EUC; Les systèmes de sécurité E/E/PE.	7.14.2	Plan de validation globale de la sécurité pour les systèmes de sécurité E/E/PE; Spécification pour les prescriptions globales de sécurité en termes de prescriptions de fonctions de sécurité et de prescriptions d'intégrité de sécurité; Allocation des prescriptions de sécurité.	Confirmation que tous les systèmes de sécurité E/E/PE remplissent la spécification pour les prescriptions globales de sécurité en termes de prescriptions de fonctions de sécurité et de prescriptions d'intégrité de sécurité, en tenant compte de l'allocation des prescriptions de sécurité pour les systèmes de sécurité E/E/PE.

Table 1 *(continued)*

Safety lifecycle phase		Objectives	Scope	Require-ments subclause	Inputs	Outputs
Figure 2 box number	**Title**					
11	**External risk reduction facilities: realisation**	7.12.1: To create external risk reduction facilities to meet the safety functions requirements and safety integrity requirements specified for such facilities (outside the scope of this standard).	External risk reduction facilities.	7.12.2	External risk reduction facilities safety requirements specification (outside the scope and not considered further in this standard).	Confirmation that each external risk reduction facility meets the safety requirements for that facility.
12	**Overall installa-tion and commis-sioning**	7.13.1: To install the E/E/PE safety-related systems; To commission the E/E/PE safety-related systems.	EUC and the EUC control system; E/E/PE safety-related systems.	7.13.2	A plan for the installation of the E/E/PE safety-related systems; A plan for the commis-sioning of the E/E/PE safety-related systems.	Fully installed E/E/PE safety-related systems; Fully commissioned E/E/PE safety-related systems.
13	**Overall safety validation**	7.14.1: To validate that the E/E/PE safety-related systems meet the specification for the overall safety requirements in terms of the overall safety functions requirements and the overall safety integrity requirements, taking into account the safety requirements allocation for the E/E/PE safety-related systems developed according to 7.6.	EUC and the EUC control system; E/E/PE safety-related systems.	7.14.2	Overall safety validation plan for the E/E/PE safety-related systems; Specification for the overall safety requirements in terms of the safety functions requirements and the safety integrity requirements; Safety requirements allocation.	Confirmation that all the E/E/PE safety-related systems meet the specification for the overall safety requirements in terms of the safety functions requirements and the safety integrity requirements, taking into account the safety requirements allocation for the E/E/PE safety-related systems.

Tableau 1 *(fin)*

Phase du cycle de vie de sécurité		Objectifs	Domaine	Prescriptions en	Entrées	Sorties
Numéro de case de la figure 2	**Titre**					
14	**Exploitation, maintenance et réparation globales**	7.15.1: Exploiter, maintenir et réparer les systèmes de sécurité E/E/PE de façon à maintenir la sécurité fonctionnelle prescrite.	L'EUC et le système de commande de l'EUC; Les systèmes de sécurité E/E/PE.	7.15.2	Plan global d'exploitation et de maintenance des systèmes de sécurité E/E/PE.	Réalisation permanente de la sécurité fonctionnelle prescrite pour les systèmes de sécurité E/E/PE; Une documentation chronologique de l'exploitation, de la réparation et de la maintenance des systèmes de sécurité E/E/PE.
15	**Modification et remise à niveau globales**	7.16.1: Assurer que la sécurité fonctionnelle pour les systèmes de sécurité E/E/PE est appropriée, à la fois pendant et après que la phase de modification et de remise à niveau ait lieu.	L'EUC et le système de commande de l'EUC; Les systèmes de sécurité E/E/PE.	7.16.2	Demande de modification ou de remise à niveau selon les procédures de gestion de la sécurité fonctionnelle.	Réalisation de la sécurité fonctionnelle prescrite pour les systèmes de sécurité E/E/PE, à la fois pendant et après que a phase de modification et de remise à niveau ait lieu.
16	**Mise hors service ou au rebut**	7.17.1: Assurer que la sécurité fonctionnelle pour les systèmes de sécurité E/E/PE est appropriée aux circonstances pendant et après les activités de mise hors service ou au rebut de l'EUC.	L'EUC et le système de commande de l'EUC; Les systèmes de sécurité E/E/PE.	7.17.2	Demande de mise hors service ou au rebut selon les procédures de gestion de la sécurité fonctionnelle.	Réalisation de la sécurité fonctionnelle prescrite pour les systèmes de sécurité E/E/PE à la fois pendant et après les activités de mise hors service ou au rebut; Une documentation chronologique des activités de mise hors service ou au rebut.

Table 1 *(concluded)*

Safety lifecycle phase		Objectives	Scope	Require-ments subclause	Inputs	Outputs
Figure 2 box number	**Title**					
14	**Overall operation, mainte-nance and repair**	7.15.1: To operate, maintain and repair the E/E/PE safety-related systems in order that the required functional safety is maintained.	EUC and the EUC control system; E/E/PE safety-related systems.	7.15.2	Overall operation and maintenance plan for the E/E/PE safety-related systems.	Continuing achievement of the required functional safety for the E/E/PE safety-related systems; Chronological documenta-tion of operation, repair and maintenance of the E/E/PE safety-related systems.
15	**Overall modifica-tion and retrofit**	7.16.1: To ensure that the functional safety for the E/E/PE safety-related systems is appropriate, both during and after the modification and retrofit phase has taken place.	EUC and the EUC control system; E/E/PE safety-related systems.	7.16.2	Request for modification or retrofit under the procedures for the management of functional safety.	Achievement of the required functional safety for the E/E/PE safety-related systems, both during and after the modification and retrofit phase has taken place; Chronological documenta-tion of operation, repair and maintenance of the E/E/PE safety-related systems.
16	**Decommis-sioning or disposal**	7.17.1: To ensure that the functional safety for the E/E/PE safety-related systems is appropriate in the circumstances during and after the activities of decommissioning or disposing of the EUC.	EUC and the EUC control system; E/E/PE safety-related systems.	7.17.2	Request for decommis-sioning or disposal under the procedures for the management of functional safety.	Achievement of the required functional safety for the E/E/PE safety-related systems both during and after the decommis-sioning or disposal activities; Chronological documenta-tion of the decommis-sioning or disposal activities.

7.1.3 Objectifs

7.1.3.1 Le premier objectif des prescriptions de ce paragraphe est de structurer, de façon systématique, les phases du cycle de vie de sécurité global qui doivent être considérées afin de réaliser la sécurité fonctionnelle prescrite des systèmes de sécurité E/E/PE.

7.1.3.2 Le second objectif des prescriptions de ce paragraphe est de documenter les informations clefs, relatives à la sécurité fonctionnelle des systèmes de sécurité E/E/PE, tout au long du cycle de vie de sécurité global.

NOTE – Voir l'article 5 et l'annexe A pour la structure de la documentation. La structure de la documentation peut tenir compte des procédures de l'entreprise et des habitudes de travail de secteurs d'application spécifiques.

7.1.4 Prescriptions

7.1.4.1 Le cycle de vie de sécurité global qui doit être utilisé comme base pour la déclaration de conformité à la présente norme est celui spécifié à la figure 2. Si un autre cycle de vie de sécurité global est utilisé, il doit être spécifié pendant la planification de la sécurité fonctionnelle, et tous les objectifs et prescriptions de chaque article ou paragraphe de la présente norme doivent être respectés.

NOTE – Le cycle de vie de sécurité du système E/E/PE et le cycle de vie de sécurité du logiciel (qui forment la phase de réalisation du cycle de vie de sécurité global) qui doivent être utilisés pour la déclaration de conformité sont spécifiés respectivement dans la CEI 61508-2 et la CEI 61508-3.

7.1.4.2 Les prescriptions pour la gestion de la sécurité fonctionnelle (voir article 6) doivent être menées en parallèle avec les phases du cycle de vie de sécurité global.

7.1.4.3 Chaque phase du cycle de vie de sécurité global doit être appliquée et les prescriptions respectées, le cas contraire devant être justifié.

7.1.4.4 Chaque phase du cycle de vie de sécurité global doit être divisée en activités élémentaires avec, pour chaque phase, la spécification du domaine d'application, des entrées et des sorties.

7.1.4.5 Le domaine et les entrées de chaque phase du cycle de vie de sécurité global doivent être tels que spécifié dans le tableau 1.

7.1.4.6 Sauf justification contraire donnée dans la planification de la sécurité fonctionnelle ou sauf spécification contraire dans la norme d'application sectorielle, les sorties de chaque phase du cycle de vie de sécurité global doivent être celles spécifiées dans le tableau 1.

7.1.4.7 Les sorties de chaque phase du cycle de vie de sécurité global doivent remplir les objectifs et prescriptions spécifiés pour chaque phase (voir 7.2 à 7.17).

7.1.4.8 Les prescriptions de vérification qui doivent être respectées pour chaque phase du cycle de vie de sécurité global sont spécifiées en 7.18.

7.1.3 Objectives

7.1.3.1 The first objective of the requirements of this subclause is to structure, in a systematic manner, the phases in the overall safety lifecycle that shall be considered in order to achieve the required functional safety of the E/E/PE safety-related systems.

7.1.3.2 The second objective of the requirements of this subclause is to document key information relevant to the functional safety of the E/E/PE safety-related systems throughout the overall safety lifecycle.

NOTE – See clause 5 and annex A for documentation structure. The documentation structure may take account of company procedures, and of the working practices of specific application sectors.

7.1.4 Requirements

7.1.4.1 The overall safety lifecycle that shall be used as the basis for claiming conformance to this standard is that specified in figure 2. If another overall safety lifecycle is used, it shall be specified during the functional safety planning, and all the objectives and requirements in each clause or subclause in this standard shall be met.

NOTE – The E/E/PES safety lifecycle and the software safety lifecycle (which form the realisation phase of the overall safety lifecycle) that shall be used in claiming conformance are specified in IEC 61508-2 and IEC 61508-3 respectively.

7.1.4.2 The requirements for the management of functional safety (see clause 6) shall run in parallel with the overall safety lifecycle phases.

7.1.4.3 Unless justified, each phase of the overall safety lifecycle shall be applied and the requirements met.

7.1.4.4 Each phase of the overall safety lifecycle shall be divided into elementary activities with the scope, inputs and outputs specified for each phase.

7.1.4.5 The scope and inputs for each overall safety lifecycle phase shall be as specified in table 1.

7.1.4.6 Unless justified in the functional safety planning or specified in the application sector standard, the outputs from each phase of the overall safety lifecycle shall be those specified in table 1.

7.1.4.7 The outputs from each phase of overall safety lifecycle shall meet the objectives and requirements specified for each phase (see 7.2 to 7.17).

7.1.4.8 The verification requirements that shall be met for each overall safety lifecycle phase are specified in 7.18.

7.2 Concept

NOTE – Cette phase correspond à la case 1 de la figure 2.

7.2.1 Objectif

L'objectif des prescriptions de ce paragraphe est de développer un niveau de compréhension suffisant de l'EUC et de son environnement (physique, légal, etc.) pour permettre de mener de façon satisfaisante les autres activités du cycle de vie de sécurité.

7.2.2 Prescriptions

7.2.2.1 Une connaissance approfondie de l'EUC, de ses fonctions de commande prescrites et de son environnement physique doit être acquise.

7.2.2.2 Les sources potentielles de dangers doivent être déterminées.

7.2.2.3 L'information sur les dangers déterminés doit être obtenue (toxicité, conditions explosives, corrosivité, réactivité, inflammabilité etc.).

7.2.2.4 L'information sur la législation applicable en matière de sécurité (nationale et internationale) doit être obtenue.

7.2.2.5 Les dangers dus aux interactions avec d'autres EUCs (installés ou devant être installés) à proximité de l'EUC doivent être considérés.

7.2.2.6 L'information et les résultats obtenus par les paragraphes 7.2.2.1 à 7.2.2.5 doivent être documentés.

7.3 Définition globale du domaine d'application

NOTE – Cette phase correspond à la case 2 de la figure 2.

7.3.1 Objectifs

7.3.1.1 Le premier objectif des prescriptions de ce paragraphe est de déterminer les limites de l'EUC et du système de commande de l'EUC.

7.3.1.2 Le second objectif des prescriptions de ce paragraphe est de spécifier le domaine de l'analyse de danger et de risque (par exemple les processus dangereux, les dangers liés à l'environnement, etc.).

7.3.2 Prescriptions

7.3.2.1 L'équipement physique, comprenant l'EUC et le système de commande de l'EUC, devant faire partie du domaine de l'analyse de danger et de risque doit être spécifié.

NOTE – Voir références [1] et [2] à l'annexe C.

7.3.2.2 Les événements extérieurs devant être pris en compte dans l'analyse de danger et de risque doivent être spécifiés.

7.3.2.3 Les sous-systèmes qui sont associés aux dangers doivent être spécifiés.

7.3.2.4 Le type d'événements initiateurs d'accidents qu'il est nécessaire de prendre en considération (par exemple les défaillances de composants, les anomalies de procédure, l'erreur humaine, les mécanismes à défaillance dépendante qui peuvent être à l'origine de séquences d'accident) doit être spécifié.

7.3.2.5 L'information et les résultats obtenus par les paragraphes 7.3.2.1 à 7.3.2.4 doivent être documentés.

7.2 Concept

NOTE – This phase is box 1 of figure 2.

7.2.1 Objective

The objective of the requirements of this subclause is to develop a level of understanding of the EUC and its environment (physical, legislative etc.) sufficient to enable the other safety lifecycle activities to be satisfactorily carried out.

7.2.2 Requirements

7.2.2.1 A thorough familiarity shall be acquired of the EUC, its required control functions and its physical environment.

7.2.2.2 The likely sources of hazards shall be determined.

7.2.2.3 Information about the determined hazards shall be obtained (toxicity, explosive conditions, corrosiveness, reactivity, flammability etc.).

7.2.2.4 Information about the current safety regulations (national and international) shall be obtained.

7.2.2.5 Hazards due to interaction with other EUCs (installed or to be installed) in the proximity of the EUC shall be considered.

7.2.2.6 The information and results acquired in 7.2.2.1 to 7.2.2.5 shall be documented.

7.3 Overall scope definition

NOTE – This phase is box 2 of figure 2.

7.3.1 Objectives

7.3.1.1 The first objective of the requirements of this subclause is to determine the boundary of the EUC and the EUC control system.

7.3.1.2 The second objective of the requirements of this subclause is to specify the scope of the hazard and risk analysis (for example process hazards, environmental hazards, etc.).

7.3.2 Requirements

7.3.2.1 The physical equipment, including the EUC and the EUC control system, to be included in the scope of the hazard and risk analysis shall be specified.

NOTE – See references [1] and [2] in annex C.

7.3.2.2 The external events to be taken into account in the hazard and risk analysis shall be specified.

7.3.2.3 The subsystems which are associated with the hazards shall be specified.

7.3.2.4 The type of accident-initiating events that need to be considered (for example component failures, procedural faults, human error, dependent failure mechanisms which can cause accident sequences to occur) shall be specified.

7.3.2.5 The information and results acquired in 7.3.2.1 to 7.3.2.4 shall be documented.

7.4 Analyse de danger et de risque

NOTE – Cette phase correspond à la case 3 de la figure 2.

7.4.1 Objectifs

7.4.1.1 Le premier objectif des prescriptions de ce paragraphe est de déterminer les dangers et événements dangereux de l'EUC et du système de commande de l'EUC (dans tous les modes d'exploitation), pour toutes les situations raisonnablement prévisibles, y compris celles de défaillance et de mauvais usage.

7.4.1.2 Le second objectif des prescriptions de ce paragraphe est de déterminer les séquences d'événements menant aux événements dangereux déterminés en 7.4.1.1.

7.4.1.3 Le troisième objectif des prescriptions de ce paragraphe est de déterminer les risques de l'EUC associés aux événements dangereux déterminés en 7.4.1.1.

NOTE 1 – Ce paragraphe est nécessaire afin que les prescriptions de sécurité pour les systèmes de sécurité E/E/PE soient basées systématiquement sur une approche basée sur le risque. Cela ne peut être fait qu'en considérant l'EUC et le système de commande de l'EUC.

NOTE 2 – Dans les cas d'applications où des hypothèses valides peuvent être faites sur les risques, les dangers potentiels, les événements dangereux et leurs conséquences, l'analyse prescrite dans ce paragraphe (et 7.5) peut être réalisée par les rédacteurs des versions d'application sectorielle de la présente norme, et peut être incluse dans des prescriptions graphiques simplifiées. Des exemples de telles méthodes sont donnés dans les annexes D et E de la CEI 61508-5.

7.4.2 Prescriptions

7.4.2.1 Une analyse de danger et de risque, qui doit prendre en compte l'information venant de la phase de définition globale du domaine d'application (voir 7.3), doit être menée. Si des décisions, prises lors d'étapes ultérieures des phases du cycle de vie de sécurité global du E/E/PES ou du logiciel, peuvent changer les bases sur lesquelles les premières décisions avaient été prises, alors une nouvelle analyse de danger et de risque doit être menée.

NOTE 1 – Pour plus de conseils, voir les références [1] et [2] à l'annexe C.

NOTE 2 – Il peut être nécessaire que plus d'une analyse de danger et de risque soit menée.

NOTE 3 – Comme exemple illustrant le besoin de poursuivre l'analyse de danger et de risque pendant tout le cycle de vie de sécurité global, considérons l'analyse d'un EUC qui incorpore une soupape de sécurité. Une analyse de danger et de risque peut déterminer deux séquences d'événements qui se rapportent respectivement à un défaut soupape fermée et à un défaut soupape ouverte, menant à une situation dangereuse. Cependant, lorsque la conception détaillée du système de commande de l'EUC commandant la soupape est analysé, un nouveau mode de défaillance, soupape oscillante, qui introduit une nouvelle séquence d'événements menant à une situation dangereuse peut être découvert.

7.4.2.2 L'attention doit être portée sur l'élimination des dangers.

NOTE – Bien qu'en dehors du domaine d'application de la présente norme, il est de la plus haute importance que les dangers identifiés de l'EUC soient éliminés à la source, par exemple par l'application de principes de sécurité intrinsèque et l'application des pratiques de bonne ingénierie.

7.4.2.3 Les dangers et événements dangereux de l'EUC et du système de commande de l'EUC doivent être déterminés selon toutes les circonstances envisageables (y compris les conditions de défaut et le mauvais usage raisonnablement prévisible). Cela doit comprendre tout problème pertinent lié au facteur humain, et doit porter une attention particulière aux modes d'exploitations anormaux ou peu fréquents de l'EUC.

NOTE – Pour le mauvais usage raisonnablement prévisible, voir 3.1.11 de la CEI 61508-4.

7.4.2.4 Les séquences d'événements conduisant aux événements dangereux déterminés en 7.4.2.3 doivent être déterminées.

NOTE – Il est en général profitable d'étudier si l'une des séquences d'événements peut être éliminée par des modifications dans la conception du procédé ou de l'équipement utilisé.

7.4 Hazard and risk analysis

NOTE – This phase is box 3 of figure 2.

7.4.1 Objectives

7.4.1.1 The first objective of the requirements of this subclause is to determine the hazards and hazardous events of the EUC and the EUC control system (in all modes of operation) for all reasonably foreseeable circumstances, including fault conditions and misuse.

7.4.1.2 The second objective of the requirements of this subclause is to determine the event sequences leading to the hazardous events determined in 7.4.1.1.

7.4.1.3 The third objective of the requirements of this subclause is to determine the EUC risks associated with the hazardous events determined in 7.4.1.1.

NOTE 1 – This subclause is necessary in order that the safety requirements for the E/E/PE safety-related systems are based on a systematic risk-based approach. This cannot be done unless the EUC and the EUC control system are considered.

NOTE 2 – In application areas where valid assumptions can be made about the risks, likely hazards, hazardous events and their consequences, the analysis required in this subclause (and 7.5) may be carried out by the developers of application sector versions of this standard, and may be embedded in simplified graphical requirements. Examples of such methods are given in annexes D and E of IEC 61508-5.

7.4.2 Requirements

7.4.2.1 A hazard and risk analysis shall be undertaken which shall take into account information from the overall scope definition phase (see 7.3). If decisions are taken at later stages in the overall, E/E/PES or software safety lifecycle phases which may change the basis on which the earlier decisions were taken, then a further hazard and risk analysis shall be undertaken.

NOTE 1 – For guidance see references [1] and [2] in annex C.

NOTE 2 – It may be necessary for more than one hazard and risk analysis to be carried out.

NOTE 3 – As an example of the need to continue hazard and risk analysis deep into the overall safety lifecycle, consider the analysis of an EUC that incorporates a safety-related valve. A hazard and risk analysis may determine two event sequences, that include valve fails closed and valve fails open, leading to hazardous events. However, when the detailed design of the EUC control system controlling the valve is analyzed, a new failure mode, valve oscillates, may be discovered which introduces a new event sequence leading to a hazardous event.

7.4.2.2 Consideration shall be given to the elimination of the hazards.

NOTE – Although not within the scope of this standard, it is of primary importance that determined hazards of the EUC are eliminated at source, for example by the application of inherent safety principles and the application of good engineering practice.

7.4.2.3 The hazards and hazardous events of the EUC and the EUC control system shall be determined under all reasonably foreseeable circumstances (including fault conditions and reasonably foreseeable misuse). This shall include all relevant human factor issues, and shall give particular attention to abnormal or infrequent modes of operation of the EUC.

NOTE – For reasonably foreseeable misuse see 3.1.11 of IEC 61508-4.

7.4.2.4 The event sequences leading to the hazardous events determined in 7.4.2.3 shall be determined.

NOTE – It is normally worthwhile to consider if any of the event sequences can be eliminated by modifications to the process design or equipment used.

7.4.2.5 La probabilité des événements dangereux en ce qui concerne les conditions spécifiées en 7.4.2.3 doit être évaluée.

NOTE – La probabilité d'un événement spécifique peut être exprimée quantitativement ou qualitativement (voir la CEI 61508-5).

7.4.2.6 Les conséquences potentielles associées aux événements dangereux déterminés en 7.4.2.3 doivent être déterminées.

7.4.2.7 Le risque de l'EUC doit être évalué ou estimé pour chaque événement dangereux déterminé.

7.4.2.8 Les prescriptions des paragraphes 7.4.2.1 à 7.4.2.7 peuvent être remplies par l'application de techniques soit qualitatives, soit quantitatives pour l'analyse de danger et de risque (voir la CEI 61508-5).

7.4.2.9 Le caractère approprié des techniques et le degré d'application de ces techniques dépendront d'un certain nombre de facteurs, tels que

– les dangers spécifiques et leurs conséquences;
– le secteur d'application et ses règles de l'art;
– les prescriptions légales et celles régissant la sécurité;
– le risque de l'EUC;
– la disponibilité de données précises servant de base à l'analyse de danger et de risque.

7.4.2.10 L'analyse de danger et de risque doit considérer les points suivants:

– chaque événement dangereux déterminé et les composants qui y contribuent;
– les conséquences et la probabilité des séquences d'événements auxquelles chaque événement dangereux est associé;
– la réduction de risque nécessaire pour chaque événement dangereux;
– les mesures prises pour réduire ou supprimer les risques et dangers;
– les hypothèses faites au cours de l'analyse des risques, y compris les taux de sollicitation probables et les taux de défaillance de l'équipement; toute prise en compte des contraintes d'exploitation ou de l'intervention humaine doit être détaillée;
– les références aux informations clefs (voir l'article 5 et l'annexe A) relatives aux systèmes de sécurité à chaque phase du cycle de vie de sécurité du système E/E/PE (par exemple les activités de vérification et de validation).

7.4.2.11 L'information et les résultats qui constituent l'analyse de danger et de risque doivent être documentés.

7.4.2.12 L'information et les résultats qui constituent l'analyse de danger et de risque doivent être maintenus pour l'EUC et le système de commande de l'EUC pendant tout le cycle de vie de sécurité global, depuis la phase d'analyse de danger et de risque jusqu'à la phase de mise hors service ou au rebut.

NOTE – La maintenance de l'information et des résultats depuis la phase d'analyse de danger et de risque est le moyen principal pour faire des progrès dans la résolution des problèmes liés à l'analyse de danger et de risque.

7.4.2.5 The likelihood of the hazardous events for the conditions specified in 7.4.2.3 shall be evaluated.

NOTE – The likelihood of a specific event may be expressed quantitatively or qualitatively (see IEC 61508-5).

7.4.2.6 The potential consequences associated with the hazardous events determined in 7.4.2.3 shall be determined.

7.4.2.7 The EUC risk shall be evaluated, or estimated, for each determined hazardous event.

7.4.2.8 The requirements of 7.4.2.1 to 7.4.2.7 can be met by the application of either qualitative or quantitative hazard and risk analysis techniques (see IEC 61508-5).

7.4.2.9 The appropriateness of the techniques, and the extent to which the techniques will need to be applied, will depend on a number of factors, including

– the specific hazards and the consequences;
– the application sector and its accepted good practices;
– the legal and safety regulatory requirements;
– the EUC risk;
– the availability of accurate data upon which the hazard and risk analysis is to be based.

7.4.2.10 The hazard and risk analysis shall consider the following:

– each determined hazardous event and the components that contribute to it;
– the consequences and likelihood of the event sequences with which each hazardous event is associated;
– the necessary risk reduction for each hazardous event;
– the measures taken to reduce or remove hazards and risks;
– the assumptions made during the analysis of the risks, including the estimated demand rates and equipment failure rates; any credit taken for operational constraints or human intervention shall be detailed;
– references to key information (see clause 5 and annex A) which relates to the safety-related systems at each E/E/PES safety lifecycle phase (for example verification and validation activities).

7.4.2.11 The information and results which constitute the hazard and risk analysis shall be documented.

7.4.2.12 The information and results which constitute the hazard and risk analysis shall be maintained for the EUC and the EUC control system throughout the overall safety lifecycle, from the hazard and risk analysis phase to the decommissioning or disposal phase.

NOTE – The maintenance of the information and results from the hazard and risk analysis phase is the principal means for establishing progress on the resolution of hazard and risk analysis issues.

7.5 Prescriptions globales de sécurité

NOTE – Cette phase correspond à la case 4 de la figure 2.

7.5.1 Objectif

L'objectif des prescriptions de ce paragraphe est de développer la spécification pour les prescriptions globales de sécurité, en termes de prescriptions de fonctions de sécurité et de prescriptions d'intégrité de sécurité, pour les systèmes de sécurité E/E/PE, les systèmes de sécurité basés sur une autre technologie et les dispositifs externes de réduction de risque, afin d'atteindre la sécurité fonctionnelle prescrite.

NOTE – Dans les cas d'applications où des hypothèses valides peuvent être faites sur les risques, les dangers potentiels, les événements dangereux et leurs conséquences, l'analyse prescrite dans ce paragraphe (et 7.4) peut être réalisée par les rédacteurs des versions d'application sectorielle de la présente norme, et peut être incluse dans des prescriptions graphiques simplifiées. Des exemples de telles méthodes sont donnés dans les annexes D et E de la CEI 61508-5.

7.5.2 Prescriptions

7.5.2.1 Les fonctions de sécurité nécessaires pour assurer la sécurité fonctionnelle prescrite pour chaque danger déterminé doivent être spécifiées. Cela doit constituer la spécification pour les prescriptions globales de fonctions de sécurité.

NOTE – Les fonctions de sécurité à exécuter ne seront pas, à ce niveau, spécifiées en des termes purement techniques car la méthode et la technologie de mise en œuvre des fonctions de sécurité ne seront connues que plus tard. Au cours de l'allocation des prescriptions de sécurité (voir 7.6), la description des fonctions de sécurité peut nécessiter une modification pour mieux correspondre à la méthode de mise en œuvre retenue.

7.5.2.2 La réduction de risque nécessaire doit être déterminée pour chaque événement dangereux déterminé. Cette détermination de la réduction de risque nécessaire peut être faite quantitativement et/ou qualitativement.

NOTE – La réduction de risque nécessaire est prescrite afin de déterminer les prescriptions d'intégrité de sécurité pour les systèmes de sécurité E/E/PE, les systèmes de sécurité basés sur une autre technologie et les dispositifs externes de réduction de risque. L'annexe C de la CEI 61508-5 met en évidence l'une des façons de déterminer la réduction de risque nécessaire lorsqu'une approche quantitative a été adoptée. Les annexes D et E de la CEI 61508-5 mettent en évidence des méthodes qualitatives, bien que dans les exemples cités, la réduction de risque nécessaire est incorporée implicitement plutôt qu'explicitement formulée.

7.5.2.3 Dans les situations où une norme internationale de secteur d'application existe, qui comprend des méthodes appropriées pour déterminer directement la réduction de risque nécessaire, alors de telles normes peuvent être utilisées pour satisfaire aux prescriptions de ce paragraphe.

7.5.2.4 Lorsque les défaillances du système de commande de l'EUC entraînent une sollicitation d'un ou plusieurs E/E/PE ou systèmes de sécurité basés sur une autre technologie et/ou dispositifs externes de réduction de risque, et lorsqu'il n'est pas prévu de désigner le système de commande de l'EUC comme étant un «système relatif à la sécurité», les prescriptions suivantes doivent être appliquées:

a) le taux de défaillance dangereuse revendiqué pour le système de commande de l'EUC doit s'appuyer sur les données acquises par l'un des moyens suivants:
   - une expérience en exploitation réelle du système de commande de l'EUC dans une application similaire;
   - une analyse de fiabilité menée conformément à une procédure reconnue;
   - une base de données industrielle sur la fiabilité des équipements génériques;

b) le taux de défaillance dangereuse qui peut être exigé pour le système de commande de l'EUC ne doit pas être inférieur à 10^{-5} défaillances dangereuses par heure;

NOTE 1 – Le fondement de cette prescription est que si le système de commande de l'EUC n'est pas désigné comme étant un système de sécurité, alors le taux de défaillance qui peut être exigé pour le système de commande de l'EUC ne doit pas être inférieur à la plus haute mesure cible de défaillance pour le niveau 1 d'intégrité de sécurité (qui est de 10^{-5} défaillances dangereuses par heure; voir tableau 3).

7.5 Overall safety requirements

NOTE – This phase is box 4 of figure 2.

7.5.1 Objective

The objective of the requirements of this subclause is to develop the specification for the overall safety requirements, in terms of the safety functions requirements and safety integrity requirements, for the E/E/PE safety-related systems, other technology safety-related systems and external risk reduction facilities, in order to achieve the required functional safety.

NOTE – In application areas where valid assumptions can be made about the risks, likely hazards, hazardous events and their consequences, the analysis required in this subclause (and 7.4) may be carried out by the developers of application sector versions of this standard, and may be embedded in simplified graphical requirements. Examples of such methods are given in annexes D and E of IEC 61508-5.

7.5.2 Requirements

7.5.2.1 The safety functions necessary to ensure the required functional safety for each determined hazard shall be specified. This shall constitute the specification for the overall safety functions requirements.

NOTE – The safety functions to be performed will not, at this stage, be specified in technology-specific terms since the method and technology of implementation of the safety functions will not be known until later. During the allocation of safety requirements (see 7.6), the description of the safety functions may need to be modified to reflect the specific method of implementation.

7.5.2.2 The necessary risk reduction shall be determined for each determined hazardous event. The necessary risk reduction may be determined in a quantitative and/or qualitative manner.

NOTE – The necessary risk reduction is required in order to determine the safety integrity requirements for the E/E/PE safety-related systems, other technology safety-related systems and external risk reduction facilities. Annex C of IEC 61508-5 outlines one way in which the necessary risk reduction may be determined when a quantitative approach has been adopted. Annexes D and E of IEC 61508-5 outline qualitative methods, although in the examples quoted the necessary risk reduction is incorporated implicitly rather than stated explicitly.

7.5.2.3 For situations where an application sector international standard exists, which includes appropriate methods for directly determining the necessary risk reduction, then such standards may be used to meet the requirements of this subclause.

7.5.2.4 Where failures of the EUC control system place a demand on one or more E/E/PE or other technology safety-related systems and/or external risk reduction facilities, and where the intention is not to designate the EUC control system as a safety-related system, the following requirements shall apply:

a) the dangerous failure rate claimed for the EUC control system shall be supported by data acquired through one of the following:
   - actual operating experience of the EUC control system in a similar application;
   - a reliability analysis carried out to a recognised procedure;
   - an industry database of reliability of generic equipment;

b) the dangerous failure rate that can be claimed for the EUC control system shall be not lower than 10^{-5} dangerous failures per hour;

NOTE 1 – The rationale of this requirement is that if the EUC control system is not designated as a safety-related system, then the failure rate that can be claimed for the EUC control system shall not be lower than the higher target failure measure for safety integrity level 1 (which is 10^{-5} dangerous failures per hour; see table 3).

c) tous les modes de défaillance dangereuse raisonnablement prévisibles du système de commande de l'EUC doivent être déterminés et pris en compte lors du développement de la spécification pour les prescriptions globales de sécurité;

d) le système de commande de l'EUC doit être séparé et indépendant des systèmes de sécurité E/E/PE, des systèmes de sécurité basés sur une autre technologie et des dispositifs externes de réduction de risque.

NOTE 2 – En partant du principe que les systèmes relatifs à la sécurité ont été conçus pour fournir une intégrité de sécurité adéquate en tenant compte du taux normal de sollicitation du système de commande de l'EUC, il ne sera alors pas nécessaire de désigner le système de commande de l'EUC comme étant un système relatif à la sécurité (et, par conséquent, ses fonctions ne seront pas désignées comme étant des fonctions de sécurité dans le contexte de la présente norme). Dans certaines applications, particulièrement là où une très haute intégrité de sécurité est prescrite, il peut être approprié de réduire le taux de sollicitation en concevant le système de commande de l'EUC de telle sorte qu'il ait un taux de défaillance plus faible que la normale. Dans de tels cas, si le taux de défaillance est plus petit que la plus haute limite d'objectif d'intégrité de sécurité pour le niveau 1 d'intégrité de sécurité (voir tableau 3), alors le système de commande devient un système relatif à la sécurité et les prescriptions de la présente norme s'appliquent.

7.5.2.5 Si les prescriptions de 7.5.2.4 a) à d) inclus ne peuvent être remplies, alors le système de commande de l'EUC doit être désigné comme étant un système relatif à la sécurité. Le niveau d'intégrité de sécurité alloué au système de commande de l'EUC doit être basé sur le taux de défaillance exigé pour le système de commande de l'EUC, conformément aux mesures cibles de défaillance spécifiées dans les tableaux 2 et 3. Dans de tels cas, les prescriptions de la présente norme, ayant rapport au niveau d'intégrité de sécurité alloué, doivent s'appliquer au système de commande de l'EUC.

NOTE 1 – Par exemple, si un taux de défaillance compris entre 10^{-6} et 10^{-5} défaillances par heure est exigé pour le système de commande de l'EUC, alors les prescriptions propres au niveau 1 d'intégrité de sécurité nécessiteraient d'être remplies.

NOTE 2 – Voir aussi 7.6.2.10.

7.5.2.6 Les prescriptions d'intégrité de sécurité, sur le plan de la réduction de risque nécessaire, doivent être spécifiées pour chaque fonction de sécurité. Cela doit constituer la spécification pour les prescriptions globales d'intégrité de sécurité.

NOTE – La spécification des prescriptions d'intégrité de sécurité est une étape intermédiaire vers la détermination des niveaux d'intégrité de sécurité pour les fonctions de sécurité devant être mises en œuvre par les systèmes de sécurité E/E/PE. Certaines méthodes qualitatives utilisées pour déterminer les niveaux d'intégrité de sécurité (voir annexes D et E de la CEI 61508-5) passent directement des paramètres de risque aux niveaux d'intégrité de sécurité. Dans de tels cas, la réduction de risque nécessaire est indiquée implicitement plutôt qu'explicitement car cette réduction est incluse dans la méthode elle-même.

7.5.2.7 La spécification pour les fonctions de sécurité (voir 7.5.2.1) et la spécification pour les prescriptions d'intégrité de sécurité (voir 7.5.2.6) doivent constituer ensemble la spécification pour les prescriptions globales de sécurité.

7.6 Allocation des prescriptions de sécurité

NOTE – Cette phase correspond à la case 5 de la figure 2.

7.6.1 Objectifs

7.6.1.1 Le premier objectif des prescriptions de ce paragraphe est d'allouer les fonctions de sécurité, qui sont indiquées dans la spécification pour les prescriptions globales de sécurité (ensemble des prescriptions de fonctions de sécurité et des prescriptions d'intégrité de sécurité), aux systèmes de sécurité E/E/PE désignés, aux systèmes de sécurité basés sur une autre technologie et aux dispositifs externes de réduction de risque.

NOTE – On considère, nécessairement, les systèmes de sécurité basés sur une autre technologie et les dispositifs externes de réduction de risque car l'allocation des systèmes de sécurité E/E/PE ne peut être effectuée tant que ces autres mesures de réduction de risque n'ont pas été prises en compte.

7.6.1.2 Le second objectif des prescriptions de ce paragraphe est d'allouer un niveau d'intégrité de sécurité à chaque fonction de sécurité.

NOTE – Les prescriptions d'intégrité de sécurité, telles que spécifiées en 7.5, sont spécifiées en termes de réduction de risque.

c) all reasonably foreseeable dangerous failure modes of the EUC control system shall be determined and taken into account in developing the specification for the overall safety requirements;

d) the EUC control system shall be separate and independent from the E/E/PE safety-related systems, other technology safety-related systems and external risk reduction facilities.

NOTE 2 – Providing the safety-related systems have been designed to provide adequate safety integrity, taking into account the normal demand rate from the EUC control system, it will not be necessary to designate the EUC control system as a safety-related system (and, therefore, its functions will not be designated as safety functions within the context of this standard). In some applications, particularly where very high safety integrity is required, it may be appropriate to reduce the demand rate by designing the EUC control system to have a lower than normal failure rate. In such cases, if the failure rate is less than the higher limit target safety integrity for safety integrity level 1 (see table 3), then the control system will become safety-related and the requirements in this standard will apply.

7.5.2.5 If the requirements of 7.5.2.4 a) to d) inclusive cannot be met, then the EUC control system shall be designated as a safety-related system. The safety integrity level allocated to the EUC control system shall be based on the failure rate that is claimed for the EUC control system in accordance with the target failure measures specified in tables 2 and 3. In such cases, the requirements in this standard, relevant to the allocated safety integrity level, shall apply to the EUC control system.

NOTE 1 – For example, if a failure rate of between 10^{-6} and 10^{-5} failures per hour is claimed for the EUC control system, then the requirements appropriate to safety integrity level 1 would need to be met.

NOTE 2 – See also 7.6.2.10.

7.5.2.6 The safety integrity requirements, in terms of the necessary risk reduction, shall be specified for each safety function. This shall constitute the specification for the overall safety integrity requirements.

NOTE – The specification of the safety integrity requirements is an interim stage towards the determination of the safety integrity levels for the safety functions to be implemented by the E/E/PE safety-related systems. Some of the qualitative methods used to determine the safety integrity levels (see annexes D and E of IEC 61508-5) progress directly from the risk parameters to the safety integrity levels. In such cases, the necessary risk reduction is implicitly rather than explicitly stated because it is incorporated in the method itself.

7.5.2.7 The specification for the safety functions (see 7.5.2.1) and the specification for the safety integrity requirements (see 7.5.2.6) shall together constitute the specification for the overall safety requirements.

7.6 Safety requirements allocation

NOTE – This phase is box 5 of figure 2.

7.6.1 Objectives

7.6.1.1 The first objective of the requirements of this subclause is to allocate the safety functions, contained in the specification for the overall safety requirements (both the safety functions requirements and the safety integrity requirements), to the designated E/E/PE safety-related systems, other technology safety-related systems and external risk reduction facilities.

NOTE – Other technology safety-related systems and external risk reduction facilities are considered, of necessity, since the allocation to E/E/PE safety-related systems cannot be done unless these other risk reduction measures are taken into account.

7.6.1.2 The second objective of the requirements of this subclause is to allocate a safety integrity level to each safety function.

NOTE – The safety integrity requirements, as specified in 7.5, are specified in terms of risk reduction.

7.6.2 Prescriptions

7.6.2.1 Les systèmes de sécurité désignés qui seront utilisés pour atteindre la sécurité fonctionnelle prescrite doivent être spécifiés. La réduction de risque nécessaire peut être atteinte grâce à

– des dispositifs externes de réduction de risque;

– des systèmes de sécurité E/E/PE;

– des systèmes de sécurité basés sur une autre technologie.

NOTE – Ce paragraphe ne s'applique que si l'un (au moins) des systèmes de sécurité est un E/E/PES.

7.6.2.2 Lors de l'allocation des fonctions de sécurité aux systèmes de sécurité E/E/PE désignés, aux systèmes de sécurité basés sur une autre technologie et aux dispositifs externes de réduction de risque, les compétences et les ressources disponibles pendant toutes les phases du cycle de vie de sécurité global doivent être considérées.

NOTE 1 – On sous-estime souvent l'ampleur des implications de l'utilisation de systèmes relatifs à la sécurité employant une technologie complexe. Par exemple, la mise en oeuvre de technologies complexes nécessite un niveau supérieur de compétence à chaque étape, depuis la spécification jusqu'à l'exploitation et la maintenance. L'utilisation d'autres solutions technologiques, plus simples, peut avoir la même efficacité tout en présentant plusieurs avantages du fait de la complexité réduite.

NOTE 2 – La disponibilité des compétences et ressources pour l'exploitation et la maintenance, ainsi que pour l'environnement d'exploitation, peut revêtir une importance critique dès qu'il s'agit d'assurer la sécurité fonctionnelle prescrite pendant l'exploitation.

7.6.2.3 Chaque fonction de sécurité, avec sa prescription d'intégrité de sécurité associée, définie conformément au paragraphe 7.5, doit être allouée aux systèmes de sécurité E/E/PE désignés en prenant compte de la réduction de risque réalisée par les systèmes de sécurité basés sur une autre technologie et les dispositifs externes de réduction de risque, de façon que la réduction de risque nécessaire pour cette fonction de sécurité soit atteinte. Cette allocation est itérative, et s'il se trouve que la réduction de risque nécessaire ne peut être atteinte, alors l'architecture doit être modifiée et l'allocation répétée.

NOTE 1 – Chaque fonction de sécurité, associée avec sa prescription d'intégrité de sécurité, spécifiée sur le plan de la réduction de risque nécessaire (voir 7.5), sera allouée à un ou plusieurs systèmes de sécurité E/E/PE, aux systèmes de sécurité basés sur une autre technologie et aux dispositifs externes de réduction de risque. La décision d'allouer une fonction de sécurité spécifique à un ou bien plusieurs systèmes relatifs à la sécurité dépendra d'un ensemble de facteurs, mais plus particulièrement de la réduction de risque devant être réalisée par cette fonction de sécurité. Plus la réduction de risque prescrite est grande, plus il est probable que la fonction soit répartie sur plus d'un système relatif à la sécurité.

NOTE 2 – La figure 6 présente l'approche adoptée dans ce paragraphe pour l'allocation des prescriptions de sécurité.

7.6.2.4 L'allocation indiquée en 7.6.2.3 doit être réalisée d'une façon telle que toutes les fonctions de sécurité soient allouées et que les prescriptions d'intégrité de sécurité soient remplies pour chaque fonction de sécurité (sous réserve de la prépondérance des prescriptions spécifiées en 7.6.2.10).

7.6.2.5 Les prescriptions d'intégrité de sécurité pour chaque fonction de sécurité doivent être qualifiées afin d'indiquer, pour chaque paramètre d'intégrité de sécurité cible, s'il correspond à

– la probabilité moyenne de défaillance à exécuter, lors d'une sollicitation, les fonctions pour lesquelles il a été conçu (pour un mode de fonctionnement à faible sollicitation) ou

– la probabilité d'une défaillance dangereuse par heure (pour un mode de fonctionnement continu ou à forte sollicitation).

7.6.2 Requirements

7.6.2.1 The designated safety-related systems that are to be used to achieve the required functional safety shall be specified. The necessary risk reduction may be achieved by

– external risk reduction facilities;

– E/E/PE safety-related systems;

– other technology safety-related systems.

NOTE – This subclause is applicable only if one of the safety-related systems is an E/E/PES.

7.6.2.2 In allocating safety functions to the designated E/E/PE safety-related systems, other technology safety-related systems and external risk reduction facilities, the skills and resources available during all phases of the overall safety lifecycle shall be considered.

NOTE 1 – The full implications of using safety-related systems employing complex technology are often underestimated. For example, the implementation of complex technology requires a higher level of competence at all stages, from specification up to operation and maintenance. The use of other, simpler, technology solutions may be equally effective and may have several advantages because of the reduced complexity.

NOTE 2 – The availability of skills and resources for operation and maintenance, and the operating environment, may be critical to achieving the required functional safety in actual operation.

7.6.2.3 Each safety function, with its associated safety integrity requirement developed according to 7.5, shall be allocated to the designated E/E/PE safety-related systems, taking into account the risk reductions achieved by the other technology safety-related systems and external risk reduction facilities, so the necessary risk reduction for that safety function is achieved. This allocation is iterative, and if it is found that the necessary risk reduction cannot be met, then the architecture shall be modified and the allocation repeated.

NOTE 1 – Each safety function, with its associated safety integrity requirement specified in terms of the necessary risk reduction (from 7.5), will be allocated to one or more E/E/PE safety-related systems, to other technology safety-related systems, and to external risk reduction facilities. The decision to allocate a specific safety function across one or more safety-related systems will depend on a number of factors, but particularly on the risk reduction to be achieved by the safety function. The larger the risk reduction required, the more likely the function will be spread over more than one safety-related system.

NOTE 2 – Figure 6 indicates the approach adopted in this subclause to safety requirements allocation.

7.6.2.4 The allocation indicated in 7.6.2.3 shall be done in such a way that all safety functions are allocated and the safety integrity requirements are met for each safety function (subject to the overriding requirements specified in 7.6.2.10).

7.6.2.5 The safety integrity requirements for each safety function shall be qualified to indicate whether each target safety integrity parameter is either

– the average probability of failure to perform its design function on demand (for a low demand mode of operation), or

– the probability of a dangerous failure per hour (for a high demand or continuous mode of operation).

7.6.2.6 L'allocation des prescriptions d'intégrité de sécurité doit être réalisée en utilisant les techniques appropriées à la combinaison des probabilités.

NOTE – L'allocation des prescriptions de sécurité peut être réalisée de manière qualitative et/ou quantitative.

7.6.2.7 L'allocation doit être faite en tenant compte de la possibilité de défaillances d'origine commune. S'il est prévu de traiter indépendamment lors de l'allocation, les systèmes de sécurité E/E/PE, les systèmes de sécurité basés sur une autre technologie et les dispositifs externes de réduction de risque, ils doivent alors

– être fonctionnellement diversifiés (c'est-à-dire utiliser des approches totalement différentes pour atteindre les mêmes résultats);

– être basés sur d'autres technologies (c'est-à-dire utiliser différents types d'équipement pour atteindre les même résultats);

NOTE 1 – Il faut reconnaître que, aussi diverse que soit la technologie, dans le cas de systèmes à haut niveau d'intégrité de sécurité avec des conséquences particulièrement graves en cas de défaillance, des précautions spéciales seront à prendre à l'encontre d'événements ayant une origine commune à faible probabilité, par exemple le crash d'un avion et les tremblements de terre.

– ne pas partager en commun des parties, services ou systèmes annexes (par exemple l'alimentation en énergie) dont la défaillance pourrait conduire à un mode de défaillance dangereuse de tous les systèmes;

– ne pas partager de procédures communes d'exploitation, de maintenance ou de test;

– être physiquement séparés de façon à ce que des défaillances prévisibles n'affectent pas les systèmes de sécurité redondants ni les dispositifs externes de réduction de risques.

NOTE 2 – La présente norme traite spécifiquement de l'allocation des prescriptions d'intégrité de sécurité aux systèmes de sécurité E/E/PE, et les prescriptions sont spécifiées en indiquant comment ce doit être réalisé. L'allocation des prescriptions d'intégrité de sécurité aux systèmes de sécurité basés sur une autre technologie et aux dispositifs externes de réduction de risque n'est donc pas traitée en détail dans la présente norme.

7.6.2.6 The allocation of the safety integrity requirements shall be carried out using appropriate techniques for the combination of probabilities.

NOTE – Safety requirements allocation may be carried out in a qualitative and/or quantitative manner.

7.6.2.7 The allocation shall proceed taking into account the possibility of common cause failures. If the E/E/PE safety-related systems, the other technology safety-related systems and the external risk reduction facilities are to be treated as independent for the allocation, they shall

– be functionally diverse (i.e. use totally different approaches to achieve the same results);

– be based on diverse technologies (i.e. use different types of equipment to achieve the same results);

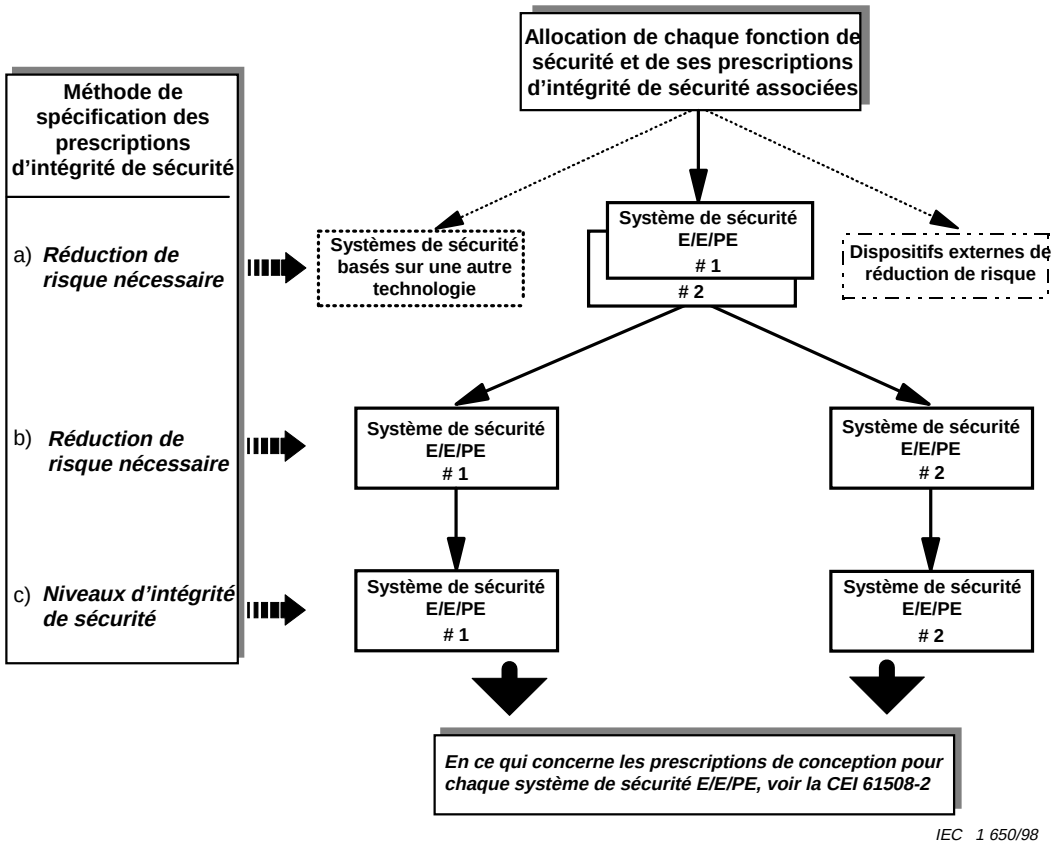
NOTE 1 – It has to be recognised that, however diverse the technology, in the case of high safety integrity systems with particularly severe consequences in the event of failure, special precautions will have to be taken against low probability common cause events, for example aircraft crashes and earthquakes.

– not share common parts, services or support systems (for example power supplies) whose failure could result in a dangerous mode of failure of all systems;

– not share common operational, maintenance or test procedures;

– be physically separated such that foreseeable failures do not affect redundant safety-related systems and external risk reduction facilities.

NOTE 2 – This standard is specifically concerned with the allocation of the safety integrity requirements to the E/E/PE safety-related systems, and requirements are specified as to how this shall be done. The allocation of safety integrity requirements to other technology safety-related systems and to external risk reduction facilities is therefore not considered in detail in this standard.



NOTE 1 – Les prescriptions d'intégrité de sécurité sont associées à chaque fonction de sécurité avant l'allocation (cf. 7.5.2.6).

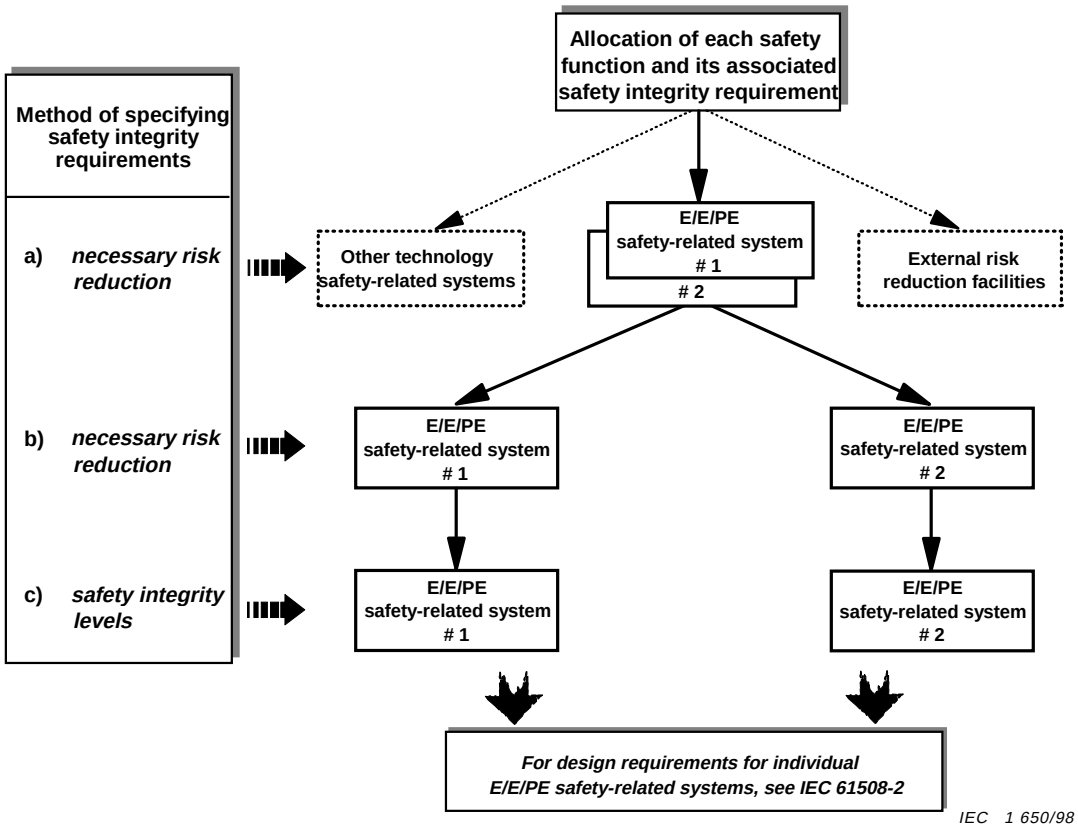
NOTE 2 – Une fonction de sécurité peut être allouée sur plusieurs systèmes de sécurité.

Figure 6 – Allocation des prescriptions de sécurité aux systèmes de sécurité E/E/PE, systèmes de sécurité basés sur une autre technologie et dispositifs externes de réduction de risque

7.6.2.8 Si toutes les prescriptions du paragraphe 7.6.2.7 ne peuvent être satisfaites, alors les systèmes de sécurité E/E/PE, les systèmes de sécurité basés sur une autre technologie et les dispositifs externes de réduction de risque ne doivent pas être considérés comme indépendants, dans le cadre des objectifs de l'allocation d'intégrité de sécurité, sauf si la réalisation d'une analyse a montré qu'ils étaient suffisamment indépendants (du point de vue de l'intégrité de sécurité).

NOTE 1 – Pour plus d'informations sur l'analyse des défaillances dépendantes, voir les références [9] et [10] en annexe C.

NOTE 2 – La notion d'indépendance suffisante est établie en démontrant que la probabilité d'une défaillance dépendante est suffisamment faible par rapport aux prescriptions globales d'intégrité de sécurité pour les systèmes de sécurité E/E/PE.



NOTE 1 – Safety integrity requirements are associated with each safety function before allocation (see 7.5.2.6).

NOTE 2 – A safety function may be allocated across more than one safety-related system.

Figure 6 – Allocation of safety requirements to the E/E/PE safety-related systems, other technology safety-related systems and external risk reduction facilities

7.6.2.8 If not all of the requirements in 7.6.2.7 can be met then the E/E/PE safety-related systems, the other technology safety-related systems, and the external risk reduction facilities shall not be treated as independent, for the purposes of the safety integrity allocation, unless an analysis has been carried out which shows that they are sufficiently independent (from a safety integrity viewpoint).

NOTE 1 – For further information on dependent failures analysis see references [9] and [10] in annex C.

NOTE 2 – Sufficient independence is established by showing that the probability of a dependent failure is sufficiently low in comparison with the overall safety integrity requirements for the E/E/PE safety-related systems.

7.6.2.9 Lorsque l'allocation a suffisamment progressé, les prescriptions d'intégrité de sécurité, pour chaque fonction de sécurité allouée au(x) système(s) de sécurité E/E/PE, doivent être spécifiées sur le plan des niveaux d'intégrité de sécurité conformément aux tableaux 2 et 3, et être qualifiées de façon à indiquer si le paramètre d'intégrité de sécurité cible est soit

– la probabilité moyenne de défaillance à exécuter, lors d'une sollicitation, les fonctions pour lesquelles il a été conçu (pour un mode de fonctionnement à faible sollicitation) soit
– la probabilité d'une défaillance dangereuse par heure (pour un mode de fonctionnement continu ou à forte sollicitation).

NOTE 1 – Préalablement à cette étape, les prescriptions d'intégrité de sécurité ont été spécifiées en termes de réduction de risque (voir 7.5).

NOTE 2 – Les tableaux 2 et 3 contiennent les mesures cibles de défaillance pour les niveaux d'intégrité de sécurité. On accepte qu'il ne sera pas possible de prédire quantitativement l'intégrité de sécurité de tous les aspects des systèmes de sécurité E/E/PE. Les techniques, mesures et jugements qualitatifs seront à réaliser avec les précautions nécessaires pour atteindre les mesures cibles de défaillance. Cela est particulièrement vrai dans le cas d'une intégrité de sécurité systématique (voir 3.5.4 de la CEI 61508-4).

Tableau 2 – Niveaux d'intégrité de sécurité: mesures cibles de défaillance pour une fonction de sécurité fonctionnant en mode de faible sollicitation

Niveau d'intégrité de sécurité	**Mode de fonctionnement à faible sollicitation** (Probabilité moyenne de défaillance à exécuter, lors d'une sollicitation, la fonction pour laquelle il a été conçu)
4	$\geq 10^{-5}$ à $< 10^{-4}$
3	$\geq 10^{-4}$ à $< 10^{-3}$
2	$\geq 10^{-3}$ à $< 10^{-2}$
1	$\geq 10^{-2}$ à $< 10^{-1}$
NOTE – Voir notes 3 à 9 ci-dessous pour l'interprétation détaillée de ce tableau.	

Tableau 3 – Niveaux d'intégrité de sécurité: mesures cibles de défaillance pour une fonction de sécurité fonctionnant en mode continu ou de forte sollicitation

Niveau d'intégrité de sécurité	**Mode de fonctionnement continu ou à forte sollicitation** (Probabilité d'une défaillance dangereuse par heure)
4	$\geq 10^{-9}$ à $< 10^{-8}$
3	$\geq 10^{-8}$ à $< 10^{-7}$
2	$\geq 10^{-7}$ à $< 10^{-6}$
1	$\geq 10^{-6}$ à $< 10^{-5}$
NOTE – Voir notes 3 à 9 ci-dessous pour l'interprétation détaillée de ce tableau.	

NOTE 3 – Voir 3.5.12 de la CEI 61508-4 pour la définition des termes «mode de fonctionnement à faible sollicitation», et «continu ou à forte sollicitation».

NOTE 4 – Le paramètre du tableau 3 pour un mode de fonctionnement continu ou à forte sollicitation, la «probabilité d'une défaillance dangereuse par heure», est parfois appelé «fréquence des défaillances dangereuses», ou «taux de défaillance dangereuse», en nombre de défaillances dangereuses par heure.

NOTE 5 – Lorsqu'un système de sécurité E/E/PE doit être exploité dans un mode de fonctionnement continu ou à forte sollicitation, pour une durée et pour une mission déterminée pendant laquelle aucune réparation ne peut avoir lieu, le niveau d'intégrité de sécurité nécessaire pour une fonction de sécurité donnée peut se déduire comme suit. Déterminer la probabilité de défaillance de la fonction de sécurité pendant la durée de la mission et diviser cette probabilité par la durée de la mission afin d'obtenir la probabilité de défaillance par heure; utiliser alors le tableau 3 pour en déduire le niveau prescrit d'intégrité de sécurité.

7.6.2.9 When the allocation has sufficiently progressed, the safety integrity requirements, for each safety function allocated to the E/E/PE safety-related system(s), shall be specified in terms of the safety integrity level in accordance with tables 2 and 3 and be qualified to indicate whether the target safety integrity parameter is either

– the average probability of failure to perform its design function on demand (for a low demand mode of operation), or

– the probability of a dangerous failure per hour (for a high demand or continuous mode of operation).

NOTE 1 – Prior to this step, the safety integrity requirements were specified in terms of the risk reduction (see 7.5).

NOTE 2 – Tables 2 and 3 contain the target failure measures for the safety integrity levels. It is accepted that it will not be possible to predict quantitatively the safety integrity of all aspects of E/E/PE safety-related systems. Qualitative techniques, measures and judgements will have to be made with respect to the precautions necessary to meet the target failure measures. This is particularly true in the case of systematic safety integrity (see 3.5.4 of IEC 61508-4).

Table 2 – Safety integrity levels: target failure measures for a safety function operating in low demand mode of operation

Safety integrity level	**Low demand mode of operation** (Average probability of failure to perform its design function on demand)
4	$\geq 10^{-5}$ to $< 10^{-4}$
3	$\geq 10^{-4}$ to $< 10^{-3}$
2	$\geq 10^{-3}$ to $< 10^{-2}$
1	$\geq 10^{-2}$ to $< 10^{-1}$
NOTE – See notes 3 to 9 below for details on interpreting this table.	

Table 3 – Safety integrity levels: target failure measures for a safety function operating in high demand or continuous mode of operation

Safety integrity level	**High demand or continuous mode of operation** (Probability of a dangerous failure per hour)
4	$\geq 10^{-9}$ to $< 10^{-8}$
3	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-6}$ to $< 10^{-5}$
NOTE – See notes 3 to 9 below for details on interpreting this table.	

NOTE 3 – See 3.5.12 of IEC 61508-4 for definition of the terms low demand mode and high demand or continuous mode of operation.

NOTE 4 – The parameter in table 3 for high demand or continuous mode of operation, probability of a dangerous failure per hour, is sometimes referred to as the frequency of dangerous failures, or dangerous failure rate, in units of dangerous failures per hour.

NOTE 5 – For an E/E/PE safety-related system operating in high demand or continuous mode of operation which is required to operate for a defined mission time during which no repair can take place, the required safety integrity level for a safety function can be derived as follows. Determine the required probability of failure of the safety function during the mission time and divide this by the mission time, to give a required probability of failure per hour, then use table 3 to derive the required safety integrity level.

NOTE 6 – La présente norme définit une limite inférieure pour les mesures cibles de défaillance, dans un mode de défaillance dangereux, qui peut être exigée. Celles-ci sont spécifiées comme étant les limites inférieures pour le niveau 4 d'intégrité de sécurité (c'est-à-dire une probabilité moyenne de défaillance de 10^{-5} à exécuter, lors d'une sollicitation, la fonction pour laquelle il a été conçu, ou une probabilité de défaillance dangereuse de 10^{-9} par heure). Il peut être possible de concevoir des systèmes de sécurité ayant des valeurs plus basses pour les mesures cibles de défaillance dans le cas de systèmes non complexes, mais on estime que les chiffres de ces tableaux représentent la limite de ce qui peut être réalisé à l'heure actuelle pour des systèmes relativement complexes (par exemple des systèmes électroniques programmables relatifs à la sécurité).

NOTE 7 – Les mesures cibles de défaillance qui peuvent être exigées quand deux ou plusieurs systèmes de sécurité E/E/PE sont utilisés peuvent être meilleures que celles indiquées aux tableaux 2 et 3, à partir du moment où des niveaux adéquats d'indépendance sont réalisés.

NOTE 8 – Il est important de noter que les mesures de défaillance pour les niveaux d'intégrité de sécurité 1, 2, 3 et 4 sont des mesures cibles de défaillance. On accepte qu'il sera possible de quantifier et d'appliquer des techniques de prédiction de fiabilité permettant d'évaluer si les mesures cibles de défaillance ont été atteintes, seulement pour l'intégrité de sécurité du matériel (voir 3.5.5 de la CEI 61508-4). Les techniques et jugements qualitatifs sont à réaliser avec les précautions nécessaires pour atteindre les mesures cibles de défaillance en ce qui concerne l'intégrité de sécurité systématique (voir 3.5.4 de la CEI 61508-4).

NOTE 9 – Les prescriptions d'intégrité de sécurité pour chaque fonction de sécurité doivent être qualifiées de façon à indiquer si le paramètre d'intégrité de sécurité cible est soit

– la probabilité moyenne de défaillance à exécuter, lors d'une sollicitation, les fonctions pour lesquelles il a été conçu (pour un mode de fonctionnement à faible sollicitation) soit

– la probabilité d'une défaillance dangereuse par heure (pour un mode de fonctionnement continu ou à forte sollicitation).

7.6.2.10 Pour ce qui est d'un système de sécurité E/E/PE qui met en œuvre des fonctions de sécurité ayant des niveaux d'intégrité de sécurité différents, et sauf s'il peut être démontré qu'il y a une indépendance suffisante dans la mise en œuvre de ses fonctions de sécurité, les parties du matériel et du logiciel relatives à la sécurité où il n'y a pas une indépendance suffisante dans leur mise en œuvre doivent être traitées comme si elles faisaient partie de la fonction de sécurité ayant le plus haut niveau d'intégrité de sécurité. Par conséquent, les prescriptions applicables au plus haut niveau d'intégrité de sécurité correspondant doivent s'appliquer à toutes ces parties.

NOTE – Voir également 7.4.2.4 de la partie 2 et 7.4.2.8 de la partie 3.

7.6.2.11 Une architecture (de système) qui ne comprend qu'un et un seul système de sécurité E/E/PE de niveau 4 d'intégrité de sécurité ne doit être permise que si les critères du point a) ou des points b) et c) (ensemble) ci-dessous sont remplis:

a) la mesure cible de défaillance d'intégrité de sécurité a été démontrée de façon explicite, par une combinaison des méthodes analytiques et des tests appropriés;

b) on possède une importante expérience en exploitation des composants utilisés au sein du système de sécurité E/E/PE; cette expérience doit avoir été acquise dans un environnement similaire et, au moins, avoir été utilisée dans un système de niveau de complexité comparable;

c) on possède suffisamment de données de défaillance du matériel, obtenues sur les composants utilisés au sein du système de sécurité E/E/PE, pour permettre une confiance suffisante sur la mesure cible de défaillance d'intégrité de sécurité du matériel qui sera exigée. Il convient d'utiliser des données appropriées à l'environnement proposé, l'application et le niveau de complexité.

7.6.2.12 Aucun système de sécurité E/E/PE unique ne doit se voir allouer une mesure cible de défaillance d'intégrité de sécurité inférieure à celle spécifiée dans les tableaux 2 et 3. C'est-à-dire que pour les systèmes de sécurité fonctionnant en

– mode de fonctionnement à faible sollicitation, la limite inférieure est fixée pour une probabilité moyenne de défaillance de 10^{-5} à exécuter, lors d'une sollicitation, la fonction pour laquelle il a été conçu;

– mode de fonctionnement continu ou à forte sollicitation, la limite inférieure est fixée pour une probabilité de défaillance dangereuse de 10^{-9} par heure.

NOTE 6 – This standard sets a lower limit on the target failure measures, in a dangerous mode of failure, that can be claimed. These are specified as the lower limits for safety integrity level 4 (i.e. an average probability of failure of 10^{-5} to perform its design function on demand, or a probability of a dangerous failure of 10^{-9} per hour). It may be possible to achieve designs of safety-related systems with lower values for the target failure measures for non-complex systems, but it is considered that the figures in the table represent the limit of what can be achieved for relatively complex systems (for example programmable electronic safety-related systems) at the present time.

NOTE 7 – The target failure measures that can be claimed when two or more E/E/PE safety-related systems are used may be better than those indicated in tables 2 and 3 providing that adequate levels of independence are achieved.

NOTE 8 – It is important to note that the failure measures for safety integrity levels 1, 2, 3 and 4 are target failure measures. It is accepted that only with respect to the hardware safety integrity (see 3.5.5 of IEC 61508-4) will it be possible to quantify and apply reliability prediction techniques in assessing whether the target failure measures have been met. Qualitative techniques and judgements have to be made with respect to the precautions necessary to meet the target failure measures with respect to the systematic safety integrity (see 3.5.4 of IEC 61508-4).

NOTE 9 – The safety integrity requirements for each safety function shall be qualified to indicate whether each target safety integrity parameter is either

– the average probability of failure to perform its design function on demand (for a low demand mode of operation), or

– the probability of a dangerous failure per hour (for a high demand or continuous mode of operation).

7.6.2.10 For an E/E/PE safety-related system that implements safety functions of different safety integrity levels, unless it can be shown there is sufficient independence of implementation between these particular safety functions, those parts of the safety-related hardware and software where there is insufficient independence of implementation shall be treated as belonging to the safety function with the highest safety integrity level. Therefore, the requirements applicable to the highest relevant safety integrity level shall apply to all those parts.

NOTE – See also 7.4.2.4 of part 2 and 7.4.2.8 of part 3.

7.6.2.11 An architecture that is comprised of only a single E/E/PE safety-related system of safety integrity level 4 shall be permitted only if the criteria in either a) or both b) and c) below are met:

a) there has been an explicit demonstration, by a combination of appropriate analytical methods and testing, of the target safety integrity failure measure;

b) there has been extensive operating experience of the components used as part of the E/E/PE safety-related system; such experience shall have been gained in a similar environment and, as a minimum, have been used in a system of comparable complexity level;

c) there is sufficient hardware failure data, obtained from components used as part of the E/E/PE safety-related system, to allow sufficient confidence in the hardware safety integrity target failure measure that is to be claimed. The data should be relevant to the proposed environment, application and complexity level.

7.6.2.12 No single E/E/PE safety-related system shall be allocated a target safety integrity failure measure lower than specified in tables 2 and 3. That is, for safety-related systems operating in

– a low demand mode of operation, the lower limit is set at an average probability of failure of 10^{-5} to perform its design function on demand;

– a high demand or continuous mode of operation, the lower limit is set at a probability of a dangerous failure of 10^{-9} per hour.

7.6.2.13 L'information et les résultats de l'allocation des prescriptions de sécurité acquise dans les paragraphes 7.6.2.1 à 7.6.2.12, en même temps que toutes les hypothèses et les justifications effectuées, doivent être documentés.

NOTE – Pour chaque système de sécurité E/E/PE, il est recommandé d'avoir suffisamment d'information sur les fonctions de sécurité et leurs niveaux d'intégrité de sécurité associés. Cette information formera la base des prescriptions de sécurité pour les systèmes de sécurité E/E/PE développés dans la CEI 61508-2.

7.7 Planification globale de l'exploitation et de la maintenance

NOTE 1 – Cette phase correspond à la case 6 de la figure 2.

NOTE 2 – Un exemple de modèle d'activités en exploitation et maintenance est présenté à la figure 7.

NOTE 3 – Un exemple de modèle de gestion de l'exploitation et de la maintenance est présenté à la figure 8.

7.7.1 Objectif

L'objectif des prescriptions de ce paragraphe est de développer un plan d'exploitation et de maintenance des systèmes de sécurité E/E/PE, pour assurer que la sécurité fonctionnelle prescrite est maintenue pendant l'exploitation et la maintenance.

7.7.2 Prescriptions

7.7.2.1 Un plan doit être préparé. Il doit spécifier les aspects suivants:

a) les activités systématiques qui doivent être réalisées pour maintenir la sécurité fonctionnelle prescrite des systèmes de sécurité E/E/PE;

b) les activités et contraintes qui sont nécessaires (par exemple lors du démarrage, de l'exploitation normale, des tests systématiques, des perturbations prévisibles, des anomalies et de l'arrêt) pour éviter un état de non-sécurité, pour réduire les sollicitations du système de sécurité E/E/PE ou pour réduire les conséquences des événements dangereux;

NOTE 1 – Les contraintes, conditions et actions suivantes se rapportent aux systèmes de sécurité E/E/PE:

– contraintes sur l'exploitation de l'EUC pendant une anomalie ou une défaillance des systèmes de sécurité E/E/PE;

– contraintes sur l'exploitation de l'EUC pendant la maintenance des systèmes de sécurité E/E/PE;

– lorsque des contraintes sur l'exploitation de l'EUC peuvent être supprimées;

– les procédures pour le retour à une exploitation normale;

– les procédures pour confirmer que l'exploitation normale a été rétablie;

– les circonstances pendant lesquelles les fonctions du système de sécurité E/E/PE peuvent être shuntées (by-pass) pour le démarrage, pour une exploitation spéciale ou pour des tests;

– les procédures à suivre avant, pendant et après le shuntage des systèmes de sécurité E/E/PE, y compris les procédures d'engagement de travaux et les niveaux d'autorisation.

c) les documents montrant les résultats d'audits et de tests de sécurité fonctionnelle, qui ont besoin d'être conservés;

d) les documents sur les incidents dangereux et tout incident pouvant potentiellement créer un événement dangereux qui ont besoin d'être conservés;

e) le domaine des activités de maintenance (que l'on distingue des activités de modification);

f) les actions à entreprendre lorsqu'un danger survient;

g) le contenu de la documentation chronologique des activités d'exploitation et de maintenance (voir 7.15).

NOTE 2 – La majorité des systèmes de sécurité E/E/PE ont des modes de défaillance qui ne peuvent être découverts que par des tests lors de la maintenance systématique. Dans de tels cas, si les tests ne sont pas effectués à une fréquence suffisante, l'intégrité de sécurité prescrite du système de sécurité E/E/PE ne sera pas atteinte. Lorsque les tests sont exécutés en ligne (on-line), il peut être nécessaire de désactiver temporairement le système de sécurité E/E/PE. Il convient de ne considérer cette possibilité que si la probabilité d'une sollicitation se produisant pendant ce temps est très faible. Lorsque l'on ne peut s'en assurer, il peut être nécessaire d'installer des capteurs et actionneurs supplémentaires pour maintenir la sécurité fonctionnelle prescrite pendant le test.

7.6.2.13 The information and results of the safety requirements allocation acquired in subclauses 7.6.2.1 to 7.6.2.12, together with any assumptions and justifications made, shall be documented.

NOTE – For each E/E/PE safety-related system, there should be sufficient information on the safety functions and their associated safety integrity levels. This information will form the basis of the safety requirements for the E/E/PE safety-related systems developed in IEC 61508-2.

7.7 Overall operation and maintenance planning

NOTE 1 – This phase is box 6 of figure 2.

NOTE 2 – An example of an operation and maintenance activities model is shown in figure 7.

NOTE 3 – An example of an operations and maintenance management model is shown in figure 8.

7.7.1 Objective

The objective of the requirements of this subclause is to develop a plan for operating and maintaining the E/E/PE safety-related systems, to ensure that the required functional safety is maintained during operation and maintenance.

7.7.2 Requirements

7.7.2.1 A plan shall be prepared which shall specify the following:

a) the routine actions which need to be carried out to maintain the required functional safety of the E/E/PE safety-related systems;

b) the actions and constraints that are necessary (for example during start-up, normal operation, routine testing, foreseeable disturbances, faults and shutdown) to prevent an unsafe state, to reduce the demands on the E/E/PE safety-related system, or reduce the consequences of the hazardous events;

NOTE 1 – The following constraints, conditions and actions are relevant to E/E/PE safety-related systems:

– constraints on the EUC operation during a fault or failure of the E/E/PE safety-related systems;

– constraints on the EUC operation during maintenance of the E/E/PE safety-related systems;

– when constraints on the EUC operation may be removed;

– the procedures for returning to normal operation;

– the procedures for confirming that normal operation has been achieved;

– the circumstances under which the E/E/PE safety-related system functions may be by-passed for start-up, for special operation or for testing;

– the procedures to be followed before, during and after by-passing E/E/PE safety-related systems, including permit to work procedures and authority levels.

c) the documentation which needs to be maintained showing results of functional safety audits and tests;

d) the documentation which needs to be maintained on hazardous incidents and all incidents with the potential to create a hazardous event;

e) the scope of the maintenance activities (as distinct from the modification activities);

f) the actions to be taken in the event of hazards occurring;

g) the contents of the chronological documentation of operation and maintenance activities (see 7.15).

NOTE 2 – The majority of E/E/PE safety-related systems have some failure modes which can be revealed only by testing during routine maintenance. In such cases, if testing is not carried out at sufficient frequency, the required safety integrity of the E/E/PE safety-related system will not be achieved. Where testing is carried out on-line, it may be necessary to disable the E/E/PE safety-related system on a temporary basis. This should be considered only if the probability of a demand occurring during this time is remote. Where this cannot be ensured, it may be necessary to install additional sensors and actuators to maintain the required functional safety during testing.

NOTE 3 – Ce paragraphe s'applique à un fournisseur de logiciel qui est tenu de fournir l'information et les procédures avec le produit logiciel qui permettra à l'utilisateur d'assurer la sécurité fonctionnelle prescrite pendant l'exploitation et la maintenance d'un système de sécurité. Cela comprend les procédures préparatoires pour toute modification de logiciel susceptible d'être effectuée en conséquence d'une prescription d'exploitation ou de maintenance (voir aussi en 7.6 de la CEI 61508-3). La mise en œuvre de ces procédures est traitée dans les paragraphes 7.15 et 7.8 de la CEI 61508-3. Les procédures préparatoires pour les futurs changements de logiciel susceptibles d'être effectués en conséquence d'une prescription de modification pour un système de sécurité sont traitées dans les paragraphes 7.16 et 7.6 de la CEI 61508-3. La mise en œuvre de ces procédures est traité dans les paragraphes 7.16 et 7.8 de la CEI 61508-2.

NOTE 4 – Il convient de tenir compte des procédures d'exploitation et de maintenance développées pour satisfaire aux prescriptions de la CEI 61508-2 et de la CEI 61508-3.

7.7.2.2 Il convient de déterminer, par une analyse systématique, les activités de maintenance systématique qui sont réalisées pour déterminer les défaillances non révélées.

NOTE – Si des défaillances non révélées ne sont pas détectées, cela peut

– conduire à une défaillance du fonctionnement lors d'une sollicitation, dans le cas de systèmes de sécurité E/E/PE, de systèmes de sécurité basés sur une autre technologie ou de dispositifs externes de réduction de risque;

– générer des sollicitations des systèmes de sécurité E/E/PE, des systèmes de sécurité basés sur une autre technologie ou des dispositifs externes de réduction de risque, dans le cas de systèmes non relatifs à la sécurité.

7.7.2.3 Le plan pour la maintenance des systèmes de sécurité E/E/PE doit être agréé par les personnes responsables ultérieurement de l'exploitation et de la maintenance des systèmes de sécurité E/E/PE, des systèmes de sécurité basés sur une autre technologie, des dispositifs externes de réduction de risque et des systèmes non relatifs à la sécurité qui peuvent potentiellement solliciter les systèmes de sécurité.

7.8 Planification globale de la validation de la sécurité

NOTE – Cette phase correspond à la case 7 de la figure 2.

7.8.1 Objectif

L'objectif des prescriptions de ce paragraphe est de développer un plan pour faciliter la validation globale de la sécurité des systèmes de sécurité E/E/PE.

7.8.2 Prescriptions

7.8.2.1 Un plan contenant les aspects suivants doit être développé:

a) les détails concernant les dates de la validation;

b) les détails concernant les personnes en charge de la validation;

c) la spécification des modes pertinents d'exploitation de l'EUC, avec leurs relations au système de sécurité E/E/PE, comprenant, lorsque c'est approprié
   - les préparatifs d'utilisation, y compris la configuration et les réglages;
   - le démarrage;
   - l'apprentissage;
   - le mode automatique;
   - le mode manuel;
   - le mode semi-automatique;
   - le régime établi;
   - la remise à zéro;
   - l'arrêt;
   - la maintenance;
   - les conditions anormales raisonnablement prévisibles;

d) la spécification des systèmes de sécurité E/E/PE qui ont besoin d'être validés pour chaque mode d'exploitation de l'EUC avant que ne commence la mise en service;

NOTE 3 – This subclause applies to a supplier of software who is required to provide information and procedures with the software product that will allow the user to ensure the required functional safety during the operation and maintenance of a safety-related system. This includes preparing procedures for any software modification that could come about as a consequence of an operational or maintenance requirement (see also 7.6 of IEC 61508-3). Implementing these procedures is covered by 7.15 and 7.8 of IEC 61508-3. Preparing procedures for future software changes that will come about as a consequence of a modification requirement for a safety-related system are dealt with in 7.16 and 7.6 of IEC 61508-3. Implementing those procedures is covered by 7.16 and 7.8 of IEC 61508-2.

NOTE 4 – Account should be taken of the operation and maintenance procedures developed to meet the requirements in IEC 61508-2 and IEC 61508-3.

7.7.2.2 The routine maintenance activities which are carried out to detect unrevealed faults should be determined by a systematic analysis.

NOTE – If unrevealed faults are not detected, they may

– in the case of E/E/PE safety-related systems, other technology safety-related systems or external risk reduction facilities, lead to a failure to operate on demand;

– in the case of non-safety-related systems, lead to demands on the E/E/PE safety-related systems, other technology safety-related systems, or external risk reduction facilities.

7.7.2.3 The plan for maintaining the E/E/PE safety-related systems shall be agreed upon with those responsible for the future operation and maintenance of the E/E/PE safety-related systems, the other technology safety-related systems, the external risk reduction facilities, and the non-safety-related systems that have the potential to place demands on the safety-related systems.

7.8 Overall safety validation planning

NOTE – This phase is box 7 of figure 2.

7.8.1 Objective

The objective of the requirements of this subclause is to develop a plan to facilitate the overall safety validation of the E/E/PE safety-related systems.

7.8.2 Requirements

7.8.2.1 A plan shall be developed which shall include the following:

a) details of when the validation shall take place;

b) details of those who shall carry out the validation;

c) specification of the relevant modes of the EUC operation with their relationship to the E/E/PE safety-related system, including where applicable
   - preparation for use, including setting and adjustment;
   - start up;
   - teach;
   - automatic;
   - manual;
   - semi-automatic;
   - steady state of operation;
   - re-setting;
   - shut down;
   - maintenance;
   - reasonably foreseeable abnormal conditions;

d) specification of the E/E/PE safety-related systems which need to be validated for each mode of EUC operation before commissioning commences;

e) la stratégie technique pour la validation (par exemple les méthodes analytiques, les tests statistiques, etc.);

f) les mesures, techniques et procédures qui doivent être utilisées pour confirmer que l'allocation des fonctions de sécurité a été réalisée correctement; cela inclut la confirmation que chaque fonction de sécurité est en conformité

   – avec la spécification pour les prescriptions globales de fonctions de sécurité, et

   – avec la spécification pour les prescriptions globales d'intégrité de sécurité;

g) la référence spécifique à chaque élément contenu dans les données de sortie de 7.5 et 7.6;

h) l'environnement prescrit dans lequel les activités de validation doivent se dérouler (par exemple, pour des tests, cela comprendrait les outils calibrés et les équipements de test);

i) les critères d'acceptation et de rejet;

j) les politiques et procédures d'évaluation des résultats de la validation, particulièrement des défaillances.

NOTE – Pendant la planification de la validation globale, il convient de tenir compte des travaux planifiés pour la validation de sécurité des E/E/PES et pour la validation du logiciel, tels que prescrits dans la CEI 61508-2 et la CEI 61508-3. Il est important de s'assurer que les interactions entre toutes les mesures de réduction de risque sont prises en compte et que toutes les fonctions de sécurité (telles que spécifiées dans les sorties de 7.5) ont été réalisées.

7.8.2.2 L'information provenant de 7.8.2.1 doit être documentée et doit constituer le plan pour la validation globale de la sécurité des systèmes de sécurité E/E/PE.

7.9 Planification globale de l'installation et de la mise en service

NOTE – Cette phase correspond à la case 8 de la figure 2.

7.9.1 Objectifs

7.9.1.1 Le premier objectif des prescriptions de ce paragraphe est de développer un plan pour que l'installation des systèmes de sécurité E/E/PE soit maîtrisée, pour assurer que la sécurité fonctionnelle prescrite soit atteinte.

7.9.1.2 Le second objectif des prescriptions de ce paragraphe est de développer un plan pour que la mise en service des systèmes de sécurité E/E/PE soit maîtrisée, pour assurer que la sécurité fonctionnelle prescrite soit atteinte.

7.9.2 Prescriptions

7.9.2.1 Un plan pour l'installation des systèmes de sécurité E/E/PE doit être développé, spécifiant

– le programme d'installation;

– la personne responsable des différentes parties de l'installation;

– les procédures pour l'installation;

– la séquence d'intégration des différents éléments;

– les critères permettant de déclarer que tout ou partie des systèmes de sécurité E/E/PE sont prêts pour l'installation et permettant de déclarer que les activités d'installation sont terminées;

– les procédures pour la résolution des défaillances et incompatibilités.

e) the technical strategy for the validation (for example analytical methods, statistical tests, etc.);

f) the measures, techniques and procedures that shall be used for confirming that the allocation of safety functions has been carried out correctly; this shall include confirmation that each safety function conforms

   – with the specification for the overall safety functions requirements, and

   – to the specification for the overall safety integrity requirements;

g) specific reference to each element contained in the outputs from 7.5 and 7.6;

h) the required environment in which the validation activities are to take place (for example, for tests this would include calibrated tools and equipment);

i) the pass and fail criteria;

j) the policies and procedures for evaluating the results of the validation, particularly failures.

NOTE – In planning the overall validation, account should be taken of the work planned for E/E/PES safety validation and software validation as required by IEC 61508-2 and IEC 61508-3. It is important to ensure that the interactions between all risk reduction measures are considered and all safety functions (as specified in the outputs of 7.5) have been achieved.

7.8.2.2 The information from 7.8.2.1 shall be documented and shall constitute the plan for the overall safety validation of the E/E/PE safety-related systems.

7.9 Overall installation and commissioning planning

NOTE – This phase is box 8 of figure 2.

7.9.1 Objectives

7.9.1.1 The first objective of the requirements of this subclause is to develop a plan for the installation of the E/E/PE safety-related systems in a controlled manner, to ensure that the required functional safety is achieved.

7.9.1.2 The second objective of the requirements of this subclause is to develop a plan for the commissioning of the E/E/PE safety-related systems in a controlled manner, to ensure the required functional safety is achieved.

7.9.2 Requirements

7.9.2.1 A plan for the installation of the E/E/PE safety-related systems shall be developed, specifying

– the installation schedule;

– those responsible for different parts of the installation;

– the procedures for the installation;

– the sequence in which the various elements are integrated;

– the criteria for declaring all or parts of the E/E/PE safety-related systems ready for installation and for declaring installation activities complete;

– procedures for the resolution of failures and incompatibilities.

7.9.2.2 Un plan pour la mise en service des systèmes de sécurité E/E/PE doit être développé, spécifiant

– le programme de la mise en service;
– la personne responsable des différentes parties de la mise en service;
– les procédures pour la mise en service;
– les relations avec les différentes étapes de l'installation;
– les relations avec la validation.

7.9.2.3 La planification globale de l'installation et de la mise en service doit être documentée.

7.10 Réalisation: E/E/PES

NOTE – Cette phase correspond à la case 9 de la figure 2 et aux cases 9.1 à 9.6 des figures 3 et 4.

7.10.1 Objectif

L'objectif des prescriptions de ce paragraphe est de créer des systèmes de sécurité E/E/PE conformes à la spécification pour les prescriptions de sécurité des E/E/PES (comprenant la spécification pour les prescriptions des fonctions de sécurité des E/E/PES et la spécification pour les prescriptions d'intégrité de sécurité des E/E/PES). Voir la CEI 61508-2 et la CEI 61508-3.

7.10.2 Prescriptions

Les prescriptions qui doivent être remplies sont contenues dans la CEI 61508-2 et la CEI 61508-3.

7.11 Réalisation: autre technologie

NOTE – Cette phase correspond à la case 10 de la figure 2.

7.11.1 Objectif

L'objectif des prescriptions de ce paragraphe est de créer des systèmes de sécurité basés sur une autre technologie qui remplissent les prescriptions de fonctions de sécurité et les prescriptions d'intégrité de sécurité spécifiées pour de tels systèmes.

7.11.2 Prescriptions

La spécification permettant de satisfaire aux prescriptions de fonctions de sécurité et les prescriptions d'intégrité de sécurité pour les systèmes de sécurité basés sur une autre technologie n'est pas traitée par la présente norme.

NOTE – Les systèmes de sécurité basés sur une autre technologie sont basés sur une technologie autre qu'électrique/électronique/électronique programmable (par exemple hydraulique, pneumatique, etc.). Les systèmes de sécurité basés sur une autre technologie ont été inclus dans le cycle de vie de sécurité global, avec les dispositifs externes de réduction de risque, pour des raisons d'exhaustivité (voir 7.12).

7.12 Réalisation: dispositifs externes de réduction de risque

NOTE – Cette phase correspond à la case 11 de la figure 2.

7.12.1 Objectif

L'objectif des prescriptions de ce paragraphe est de créer des dispositifs externes de réduction de risque qui remplissent les prescriptions de fonctions de sécurité et les prescriptions d'intégrité de sécurité spécifiées pour de tels dispositifs.

7.9.2.2 A plan for the commissioning of the E/E/PE safety-related systems shall be developed, specifying:

– the commissioning schedule;
– those responsible for different parts of the commissioning;
– the procedures for the commissioning;
– the relationships to the different steps in the installation;
– the relationships to the validation.

7.9.2.3 The overall installation and commissioning planning shall be documented.

7.10 Realisation: E/E/PES

NOTE – This phase is box 9 of figure 2 and boxes 9.1 to 9.6 of figures 3 and 4.

7.10.1 Objective

The objective of the requirements of this subclause is to create E/E/PE safety-related systems conforming to the specification for the E/E/PES safety requirements (comprising the specification for the E/E/PES safety functions requirements and the specification for the E/E/PES safety integrity requirements). See IEC 61508-2 and IEC 61508-3.

7.10.2 Requirements

The requirements that shall be met are contained in IEC 61508-2 and IEC 61508-3.

7.11 Realisation: other technology

NOTE – This phase is box 10 of figure 2.

7.11.1 Objective

The objective of the requirements of this subclause is to create other technology safety-related systems to meet the safety functions requirements and safety integrity requirements specified for such systems.

7.11.2 Requirements

The specification to meet the safety functions requirements and safety integrity requirements for other technology safety-related systems is not covered in this standard.

NOTE – Other technology safety-related systems are based on a technology other than electrical/electronic/programmable electronic (for example hydraulic, pneumatic etc.). The other technology safety-related systems have been included in the overall safety lifecycle, together with the external risk reduction facilities, for completeness (see 7.12).

7.12 Realisation: external risk reduction facilities

NOTE – This phase is box 11 of figure 2.

7.12.1 Objective

The objective of the requirements of this subclause is to create external risk reduction facilities to meet the safety functions requirements and safety integrity requirements specified for such facilities.

7.12.2 Prescriptions

La spécification permettant de remplir les prescriptions de fonctions de sécurité et les prescriptions d'intégrité de sécurité pour les dispositifs externes de réduction de risque n'est pas traitée par la présente norme.

NOTE – Les dispositifs externes de réduction de risque ont été inclus dans le cycle de vie de sécurité global, avec les systèmes de sécurité basés sur une autre technologie, pour des raisons d'exhaustivité (voir 7.11).

7.13 Installation et mise en service globales

NOTE – Cette phase correspond à la case 12 de la figure 2.

7.13.1 Objectifs

7.13.1.1 Le premier objectif des prescriptions de ce paragraphe est d'installer les systèmes de sécurité E/E/PE.

7.13.1.2 Le second objectif des prescriptions de ce paragraphe est d'assurer la mise en service des systèmes de sécurité E/E/PE.

7.13.2 Prescriptions

7.13.2.1 Les activités d'installation doivent être réalisées conformément au plan pour l'installation des systèmes de sécurité E/E/PE.

7.13.2.2 L'information documentée pendant l'installation doit comprendre

– un dossier sur les activités d'installation;
– la résolution des défaillances et incompatibilités.

7.13.2.3 Les activités de mise en service doivent être réalisées conformément au plan pour la mise en service des systèmes de sécurité E/E/PE.

7.13.2.4 L'information documentée pendant la mise en service doit comprendre

– un dossier sur les activités de mise en service;
– les références des rapports de défaillance;
– la résolution des défaillances et incompatibilités.

7.14 Validation globale de la sécurité

NOTE – Cette phase correspond à la case 13 de la figure 2.

7.14.1 Objectif

L'objectif des prescriptions de ce paragraphe est de valider le fait que les systèmes de sécurité E/E/PE remplissent la spécification pour les prescriptions globales de sécurité sur le plan des prescriptions globales de fonctions de sécurité et des prescriptions globales d'intégrité de sécurité, en tenant compte de l'allocation des prescriptions de sécurité, pour les systèmes de sécurité E/E/PE, effectuée conformément à 7.6.

7.14.2 Prescriptions

7.14.2.1 Les activités de validation doivent être réalisées conformément au plan de validation globale de la sécurité pour les systèmes de sécurité E/E/PE.

7.14.2.2 Tout équipement utilisé pour des mesures quantitatives, dans le cadre des activités de validation, doit être étalonné vis-à-vis d'une spécification se référant à une norme nationale ou à la spécification du vendeur.

7.12.2 Requirements

The specification to meet the safety functions requirements and safety integrity requirements for the external risk reduction facilities is not covered in this standard.

NOTE – The external risk reduction facilities have been included in the overall safety lifecycle, together with the other technology safety-related systems for completeness (see 7.11).

7.13 Overall installation and commissioning

NOTE – This phase is box 12 of figure 2.

7.13.1 Objectives

7.13.1.1 The first objective of the requirements of this subclause is to install the E/E/PE safety-related systems.

7.13.1.2 The second objective of the requirements of this subclause is to commission the E/E/PE safety-related systems.

7.13.2 Requirements

7.13.2.1 Installation activities shall be carried out in accordance with the plan for the installation of the E/E/PE safety-related systems.

7.13.2.2 The information documented during installation shall include

– documentation of installation activities;
– resolution of failures and incompatibilities.

7.13.2.3 Commissioning activities shall be carried out in accordance with the plan for the commissioning of the E/E/PE safety-related systems.

7.13.2.4 The information documented during commissioning shall include

– documentation of commissioning activities;
– references to failure reports;
– resolution of failures and incompatibilities.

7.14 Overall safety validation

NOTE – This phase is box 13 of figure 2.

7.14.1 Objective

The objective of the requirements of this subclause is to validate that the E/E/PE safety-related systems meet the specification for the overall safety requirements in terms of the overall safety functions requirements and overall safety integrity requirements, taking into account the safety requirements allocation for the E/E/PE safety-related systems developed according to 7.6.

7.14.2 Requirements

7.14.2.1 Validation activities shall be carried out in accordance with the overall safety validation plan for the E/E/PE safety-related systems.

7.14.2.2 All equipment used for quantitative measurements as part of the validation activities shall be calibrated against a specification traceable to a national standard or to the vendor specification.

7.14.2.3 L'information documentée pendant la validation doit comprendre

– un dossier, sous forme chronologique, des activités de validation;
– la version de la spécification pour les prescriptions globales de sécurité qui a été utilisée;
– la fonction de sécurité qui a été validée (par test ou par analyse);
– les outils et l'équipement utilisés, ainsi que les données d'étalonnage;
– les résultats des activités de validation;
– l'identification de la configuration de l'entité testée, les procédures appliquées et l'environnement de test;
– les décalages entre les résultats escomptés et les résultats réels.

7.14.2.4 Lorsque des différences surviennent entre les résultats escomptés et les résultats réels, l'analyse faite et les décisions prises concernant la poursuite de la validation ou bien l'émission d'une demande de modification et le retour à une partie antérieure de la validation doivent être documentées.

7.15 Exploitation, maintenance et réparation globales

NOTE 1 – Cette phase correspond à la case 14 de la figure 2.

NOTE 2 – Les mesures d'organisation dont il est question dans ce paragraphe permettent la mise en œuvre efficace des prescriptions techniques et ont pour unique but la réalisation et le maintien de la sécurité fonctionnelle des systèmes de sécurité E/E/PE. Les prescriptions techniques nécessaires pour maintenir la sécurité fonctionnelle seront normalement spécifiées dans une partie de la documentation donnée par le fournisseur du système de sécurité E/E/PE.

NOTE 3 – Les prescriptions de sécurité fonctionnelle pendant les activités de maintenance et de réparation peuvent être différentes de celles prescrites pendant l'exploitation.

NOTE 4 – Il ne faut pas supposer que les procédures de tests développées pour l'installation et la mise en service initiale puissent être utilisées sans vérifier leur validité et leur praticabilité dans le contexte d'une exploitation «on line» de l'EUC.

7.15.1 Objectif

L'objectif des prescriptions de ce paragraphe est d'exploiter, maintenir et réparer les systèmes de sécurité E/E/PE de façon à maintenir la sécurité fonctionnelle prescrite.

7.15.2 Prescriptions

7.15.2.1 Ce qui suit doit être mis en œuvre:

– le plan pour la maintenance des systèmes de sécurité E/E/PE;
– les procédures d'exploitation, de maintenance et de réparation pour les systèmes de sécurité E/E/PE (voir la CEI 61508-2);
– les procédures d'exploitation et de maintenance pour le logiciel (voir la CEI 61508-3).

7.15.2.2 La mise en œuvre des points cités en 7.15.2.1 doit comprendre le démarrage des actions suivantes:

– la mise en œuvre des procédures;
– le suivi des programmes de maintenance;
– la maintenance des documents;
– la conduite périodique d'audits de la sécurité fonctionnelle (voir 6.2.1 k));
– la documentation des modifications qui ont été effectuées sur les systèmes de sécurité E/E/PE.

NOTE 1 – Un exemple de modèle d'activités d'exploitation et de maintenance est présenté à la figure 7.

NOTE 2 – Un exemple de modèle de gestion de l'exploitation et de la maintenance est présenté à la figure 8.

7.14.2.3 The information documented during validation shall include

– documentation in chronological form of the validation activities;
– the version of the specification for the overall safety requirements being used;
– the safety function being validated (by test or by analysis);
– tools and equipment used, along with calibration data;
– the results of the validation activities;
– configuration identification of the item under test, the procedures applied and the test environment;
– discrepancies between expected and actual results.

7.14.2.4 When discrepancies occur between expected and actual results, the analysis made, and the decisions taken on whether to continue the validation or issue a change request and return to an earlier part of the validation, shall be documented.

7.15 Overall operation, maintenance and repair

NOTE 1 – This phase is box 14 of figure 2.

NOTE 2 – The organizational measures dealt with in this subclause provide for the effective implementation of the technical requirements and are solely aimed at the achievement and maintenance of functional safety of the E/E/PE safety-related systems. The technical requirements necessary for maintaining functional safety will normally be specified as part of the information provided by the supplier of the E/E/PE safety-related system.

NOTE 3 – The functional safety requirements during the maintenance and repair activities may be different from those required during operation.

NOTE 4 – It must not be assumed that test procedures developed for initial installation and commissioning can be used without checking their validity and practicability in the context of on-line EUC operations.

7.15.1 Objective

The objective of the requirements of this subclause is to operate, maintain and repair the E/E/PE safety-related systems in order that the required functional safety is maintained.

7.15.2 Requirements

7.15.2.1 The following shall be implemented:

– the plan for maintaining the E/E/PE safety-related systems;
– the operation, maintenance and repair procedures for the E/E/PE safety-related systems (see IEC 61508-2);
– the operation and maintenance procedures for software (see IEC 61508-3).

7.15.2.2 Implementation of the items specified in 7.15.2.1 shall include initiation of the following actions:

– the implementation of procedures;
– the following of maintenance schedules;
– the maintaining of documentation;
– the carrying out, periodically, of functional safety audits (see 6.2.1 k));
– the documenting of modifications that have been made to the E/E/PE safety-related systems.

NOTE 1 – An example of an operation and maintenance activities model is shown in figure 7.

NOTE 2 – An example of an operations and maintenance management model is shown in figure 8.

7.15.2.3 La documentation chronologique de l'exploitation, des réparations et de la maintenance des systèmes de sécurité E/E/PE doit être entretenue et doit contenir les informations suivantes:

– les résultats des tests et audits de la sécurité fonctionnelle;

– un enregistrement de l'heure et de l'origine des sollicitations des systèmes de sécurité E/E/PE (en exploitation réelle), ainsi que la réponse des systèmes de sécurité E/E/PE lorsqu'ils ont été soumis à ces sollicitations, et les anomalies découvertes lors de la maintenance systématique;

– un enregistrement des modifications apportées à l'EUC, au système de commande de l'EUC et aux systèmes de sécurité E/E/PE.

7.15.2.4 Les prescriptions exactes concernant la documentation chronologique dépendront de la spécificité de l'application et doivent, lorsque cela est approprié, être détaillées dans les normes d'application sectorielle.

7.15.2.3 Chronological documentation of operation, repair and maintenance of the E/E/PE safety-related systems shall be maintained which shall contain the following information:

– the results of functional safety audits and tests;

– documentation of the time and cause of demands on the E/E/PE safety-related systems (in actual operation), together with the performance of the E/E/PE safety-related systems when subject to those demands, and the faults found during routine maintenance;

– documentation of modifications that have been made to the EUC, to the EUC control system and to the E/E/PE safety-related systems.

7.15.2.4 The exact requirements for chronological documentation will be dependent on the specific application and shall, where relevant, be detailed in application sector standards.

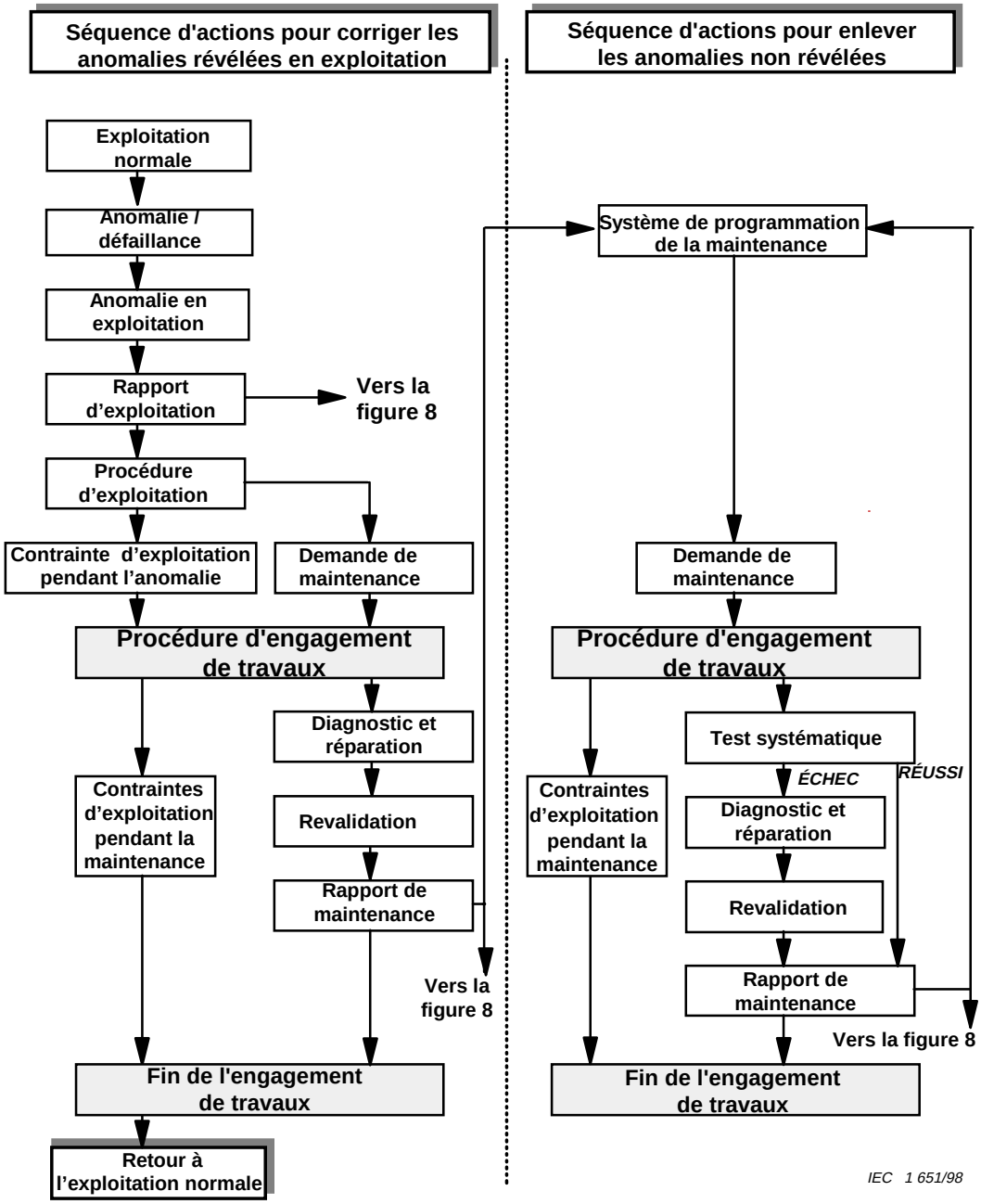


Figure 7 – Exemple de modèle d'activités d'exploitation et de maintenance

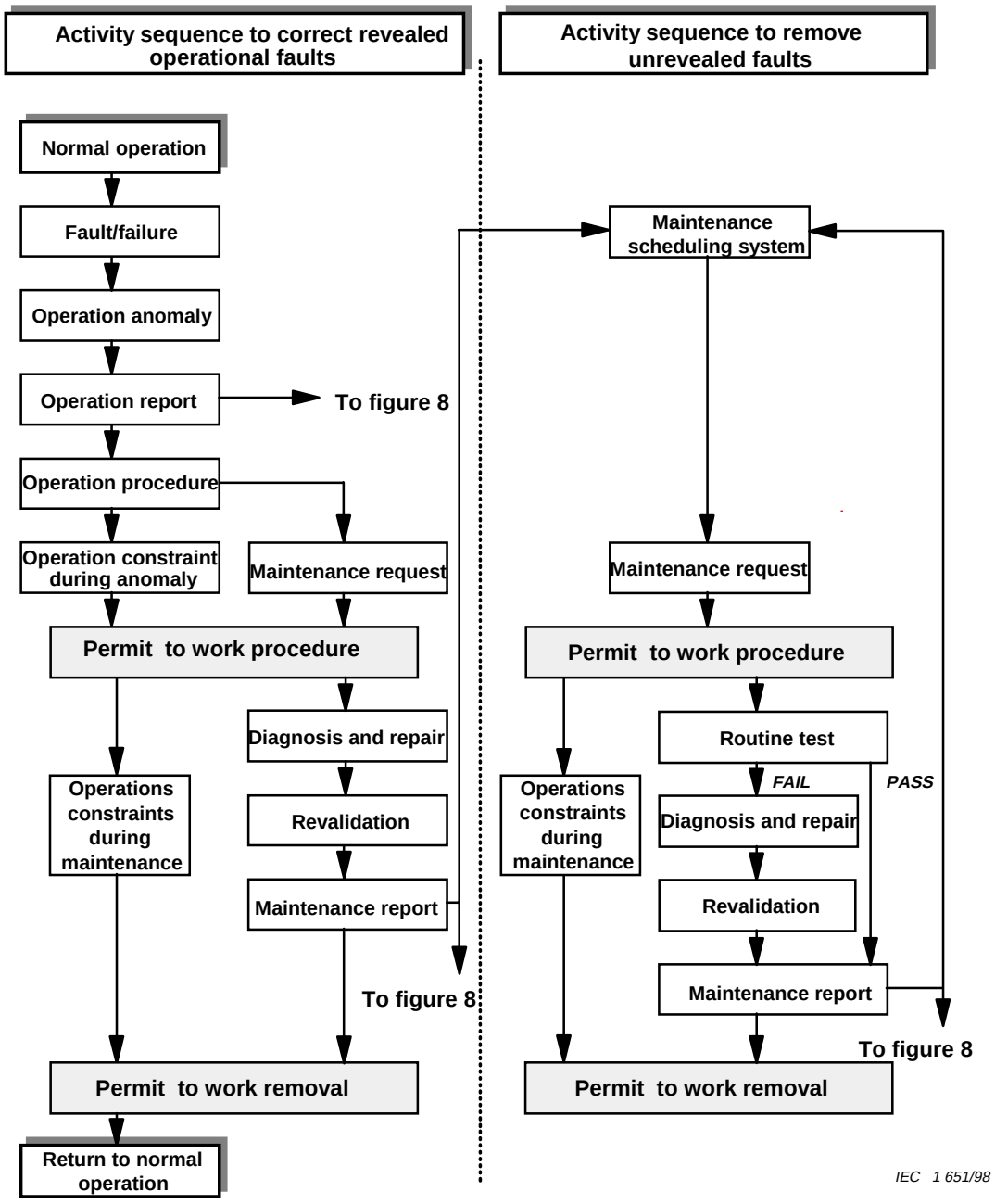


Figure 7 – Example operations and maintenance activities model

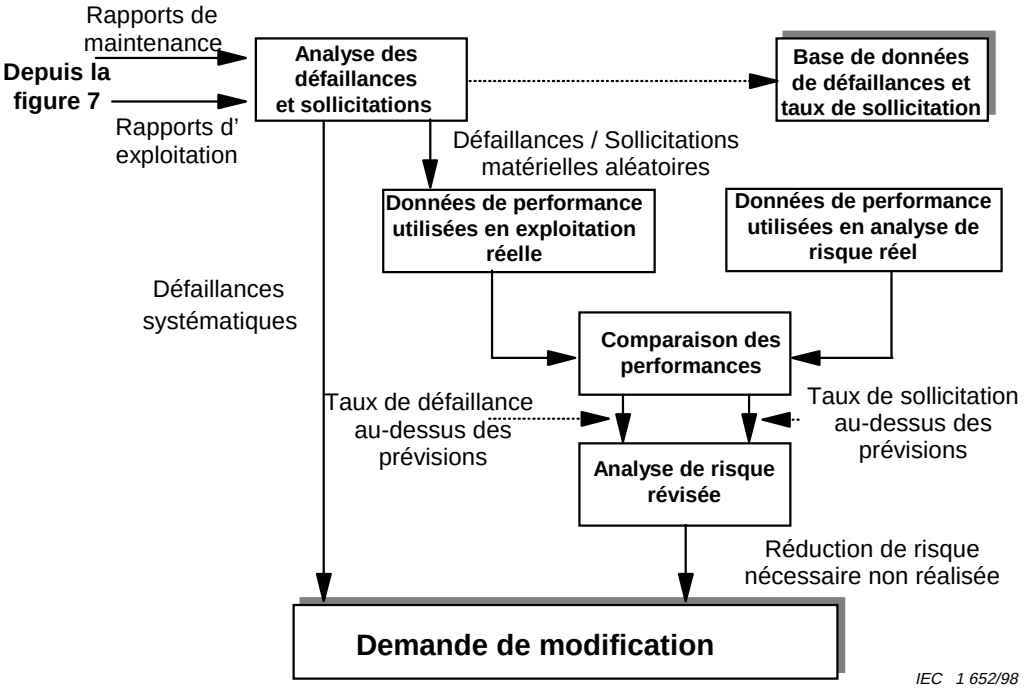


Figure 8 – Exemple de modèle de gestion de l'exploitation et de la maintenance

7.16 Modification et remise à niveau globales

NOTE 1 – Cette phase correspond à la case 15 de la figure 2.

NOTE 2 – Les mesures d'organisation dont il est question dans ce paragraphe permettent la mise en œuvre efficace des prescriptions techniques et ont pour unique but la réalisation et le maintien de la sécurité fonctionnelle des système de sécurité E/E/PE. Les prescriptions techniques nécessaires pour maintenir la sécurité fonctionnelle doivent normalement être spécifiées dans une partie de la documentation donnée par le fournisseur du système de sécurité E/E/PE.

7.16.1 Objectif

L'objectif des prescriptions de ce paragraphe est d'assurer que la sécurité fonctionnelle pour les systèmes de sécurité E/E/PE est appropriée, à la fois pendant et après que la phase de modification et de remise à niveau a eu lieu.

7.16.2 Prescriptions

7.16.2.1 Avant d'entreprendre toute modification ou remise à niveau, les procédures doivent être prévues (voir 6.2.1).

NOTE – Un exemple de modèle de procédure pour les modifications est présenté à la figure 9.

7.16.2.2 La phase de modification et de remise à niveau ne doit pouvoir être initiée que par l'émission d'une demande officielle selon les procédures pour la gestion de la sécurité fonctionnelle (voir l'article 6). Cette demande doit détailler les points suivants:

– les dangers déterminés qui peuvent être concernés;

– la modification proposée (à la fois matérielle et logicielle);

– les motifs de cette modification.

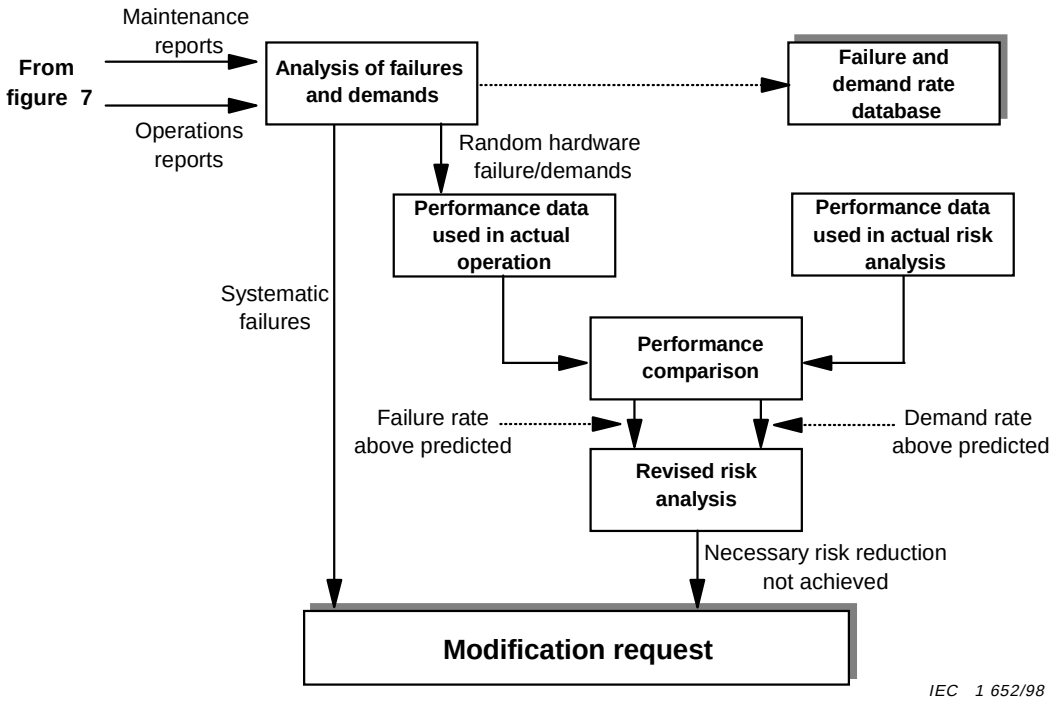


Figure 8 – Example operation and maintenance management model

7.16 Overall modification and retrofit

NOTE 1 – This phase is box 15 of figure 2.

NOTE 2 – The organizational measures dealt with in this subclause provide for the effective implementation of the technical requirements, and are solely aimed at the achievement and maintenance of functional safety of the E/E/PE safety-related systems. The technical requirements necessary for maintaining functional safety will normally be specified as part of the information provided by the supplier of the E/E/PE safety-related system.

7.16.1 Objective

The objective of the requirements of this subclause is to ensure that the functional safety for the E/E/PE safety-related systems is appropriate, both during and after the modification and retrofit phase has taken place.

7.16.2 Requirements

7.16.2.1 Prior to carrying out any modification or retrofit activity, procedures shall be planned (see 6.2.1).

NOTE – An example of a modification procedure model is shown in figure 9.

7.16.2.2 The modification and retrofit phase shall be initiated only by the issue of an authorized request under the procedures for the management of functional safety (see clause 6). The request shall detail the following:

– the determined hazards which may be affected;

– the proposed change (both hardware and software);

– the reasons for the change.

NOTE – Les motifs de cette demande de modification peuvent provenir, par exemple

– d'une sécurité fonctionnelle inférieure à celle spécifiée;

– de la découverte d'anomalie systématique;

– d'une législation nouvelle ou amendée en matière de sécurité;

– des modifications de l'EUC ou de son utilisation;

– d'une modification des prescriptions globales de sécurité;

– de l'analyse des performances d'exploitation et de maintenance, indiquant que la performance est en dessous des objectifs;

– des audits systématiques de la sécurité fonctionnelle.

7.16.2.3 Une analyse d'impact doit être réalisée. Elle doit comprendre une évaluation de l'impact sur la sécurité fonctionnelle de tout système de sécurité E/E/PE, des activités de modification ou de remise à niveau proposées. L'évaluation doit inclure une analyse de danger et de risque suffisante pour déterminer l'étendue et la profondeur que devront couvrir les phases globales ultérieures du cycle de vie de sécurité du E/E/PES ou du logiciel. L'évaluation doit aussi prendre en compte l'impact des autres activités de modification ou de remise à niveau menées en parallèle, et doit également prendre en compte la sécurité fonctionnelle à la fois pendant et après que les activités de modification et de remise à niveau ont eu lieu.

7.16.2.4 Les résultats obtenus en 7.16.2.3 doivent être documentés.

7.16.2.5 L'autorisation d'effectuer les activités de modification ou de remise à niveau demandées doit dépendre des résultats de l'analyse d'impact.

7.16.2.6 Toute modification ayant un impact sur la sécurité fonctionnelle de tout système de sécurité E/E/PE doit entraîner un retour à la phase globale appropriée du cycle de vie des logiciels ou systèmes de sécurité E/E/PE. Toutes les phases suivantes doivent alors être exécutées en respectant les procédures spécifiées pour chaque phase spécifique, conformément aux prescriptions de la présente norme.

NOTE 1 – Il peut être nécessaire de mettre en œuvre une analyse complète de danger et de risque, qui pourra générer des besoins de niveaux d'intégrité de sécurité qui sont différents de ceux actuellement spécifiés pour les systèmes de sécurité E/E/PE.

NOTE 2 – Il ne faut pas supposer que les procédures de tests développées pour l'installation et la mise en service initiale puissent être utilisées sans vérifier leur validité et leur praticabilité dans le contexte d'une exploitation «on-line» de l'EUC.

7.16.2.7 Une documentation chronologique doit être établie et tenue à jour. Elle doit contenir les détails de toutes les modifications et remises à niveau, et doit faire référence

– aux demandes de modifications ou remises à niveau;

– aux analyses d'impact;

– à la revérification et revalidation des données et résultats;

– à tous les documents affectés par ces activités de modification et de remise à niveau.

NOTE – The reason for the request for the modification could arise from, for example,

– functional safety below that specified;
– systematic fault experience;
– new or amended safety legislation;
– modifications to the EUC or its use;
– modification to the overall safety requirements;
– analysis of operations and maintenance performance, indicating that the performance is below target;
– routine functional safety audits.

7.16.2.3 An impact analysis shall be carried out which shall include an assessment of the impact of the proposed modification or retrofit activity on the functional safety of any E/E/PE safety-related system. The assessment shall include a hazard and risk analysis sufficient to determine the breadth and depth to which subsequent overall, E/E/PES or software safety lifecycle phases will need to be undertaken. The assessment shall also consider the impact of other concurrent modification or retrofit activities, and shall also consider the functional safety both during and after the modification and retrofit activities have taken place.

7.16.2.4 The results described in 7.16.2.3 shall be documented.

7.16.2.5 Authorization to carry out the required modification or retrofit activity shall be dependent on the results of the impact analysis.

7.16.2.6 All modifications which have an impact on the functional safety of any E/E/PE safety-related system shall initiate a return to an appropriate phase of the overall, E/E/PES or software safety lifecycles. All subsequent phases shall then be carried out in accordance with the procedures specified for the specific phases in accordance with the requirements in this standard.

NOTE 1 – It may be necessary to implement a full hazard and risk analysis which may generate a need for safety integrity levels that are different to those currently specified for the E/E/PE safety-related systems.

NOTE 2 – It must not be assumed that test procedures developed for initial installation and commissioning can be used without checking their validity and practicability in the context of on-line EUC operations.

7.16.2.7 Chronological documentation shall be established and maintained which shall document details of all modifications and retrofits, and shall include references to

– the modification or retrofit request;
– the impact analysis;
– reverification and revalidation of data and results;
– all documents affected by the modification and retrofit activity.

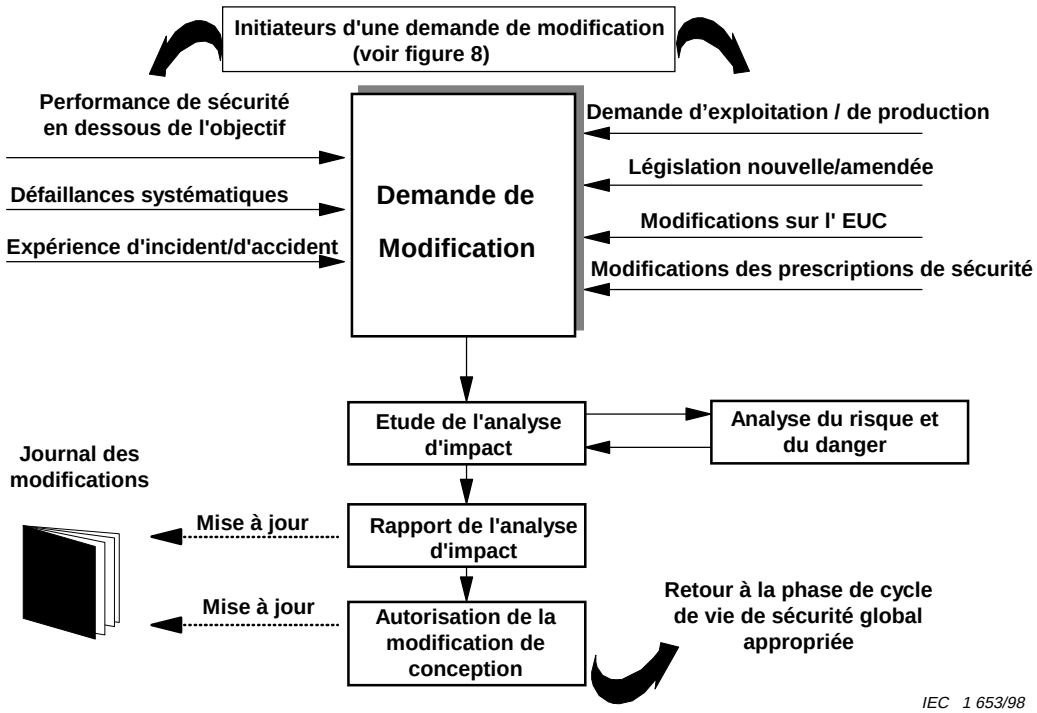


Figure 9 – Exemple de modèle de procédure pour les modifications

7.17 Mise hors service ou au rebut

NOTE – Cette phase correspond à la case 16 de la figure 2.

7.17.1 Objectif

L'objectif des prescriptions de ce paragraphe est d'assurer que la sécurité fonctionnelle pour les systèmes de sécurité E/E/PE est appropriée aux circonstances pendant et après les activités de mise hors service ou au rebut de l'EUC.

7.17.2 Prescriptions

7.17.2.1 Avant d'entreprendre toute activité de mise hors service ou au rebut, une analyse d'impact doit être réalisée. Elle doit comprendre une évaluation de l'impact de l'activité proposée de mise hors service ou au rebut sur la sécurité fonctionnelle de tout système de sécurité E/E/PE associé à l'EUC. L'analyse d'impact doit aussi prendre en compte les EUCs adjacents et l'impact sur leurs systèmes de sécurité E/E/PE. L'évaluation doit inclure une analyse de danger et de risque suffisante pour déterminer l'étendue et la profondeur que devront couvrir les phases globales ultérieures du cycle de vie de sécurité du E/E/PES ou du logiciel.

7.17.2.2 Les résultats obtenus en 7.17.2.1 doivent être documentés.

7.17.2.3 La phase de mise hors service ou au rebut ne doit pouvoir être initiée que par l'émission d'une demande officielle selon les procédures pour la gestion de la sécurité fonctionnelle (voir article 6).

7.17.2.4 L'autorisation d'effectuer la mise hors service ou au rebut demandée doit dépendre des résultats de l'analyse d'impact.

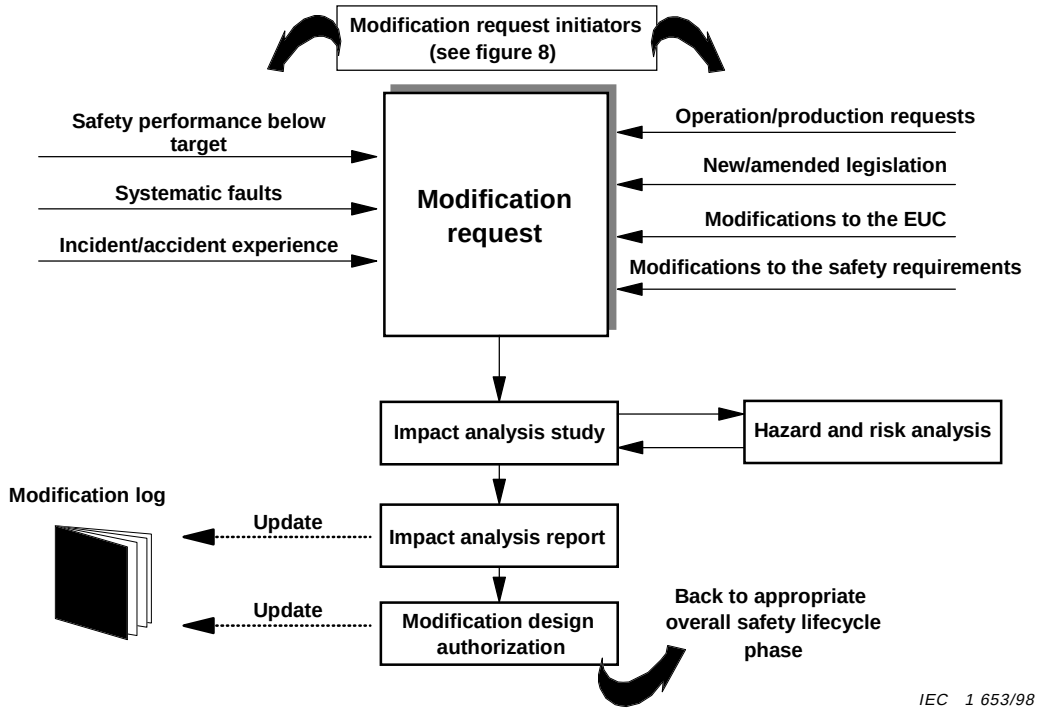


Figure 9 – Example modification procedure model

7.17 Decommissioning or disposal

NOTE – This phase is box 16 of figure 2.

7.17.1 Objective

The objective of the requirements of this subclause is to ensure that the functional safety for the E/E/PE safety-related systems is appropriate for the circumstances during and after the activities of decommissioning or disposing of the EUC.

7.17.2 Requirements

7.17.2.1 Prior to any decommissioning or disposal activity, an impact analysis shall be carried out which shall include an assessment of the impact of the proposed decommissioning or disposal activity on the functional safety of any E/E/PE safety-related system associated with the EUC. The impact analysis shall also consider adjacent EUCs and the impact on their E/E/PE safety-related systems. The assessment shall include a hazard and risk analysis sufficient to determine the necessary breadth and depth of subsequent overall E/E/PES or software safety lifecycle phases.

7.17.2.2 The results described in 7.17.2.1 shall be documented.

7.17.2.3 The decommissioning or disposal phase shall only be initiated by the issue of an authorized request under the procedures for the management of functional safety (see clause 6).

7.17.2.4 Authorization to carry out the required decommissioning or disposal shall be dependent on the results of the impact analysis.

7.17.2.5 Avant d'entreprendre la mise hors service ou au rebut, un plan doit être préparé. Il doit comporter les procédures pour

– l'arrêt définitif des systèmes de sécurité E/E/PE;

– le démantèlement des systèmes de sécurité E/E/PE.

7.17.2.6 Si l'une des activités de mise hors service ou au rebut exerce un impact sur la sécurité fonctionnelle de tout système de sécurité E/E/PE, cela doit entraîner un retour à la phase globale appropriée du cycle de vie des logiciels ou systèmes de sécurité E/E/PE. Toutes les phases suivantes doivent alors être exécutées conformément aux procédures spécifiées dans la présente norme pour les niveaux d'intégrité de sécurité spécifiés pour les systèmes de sécurité E/E/PE.

NOTE 1 – Il peut être nécessaire de mettre en œuvre une analyse complète de danger et de risque, qui pourra générer un besoin de niveau différent d'intégrité de sécurité pour les systèmes de sécurité E/E/PE.

NOTE 2 – Les prescriptions de sécurité fonctionnelle pendant la phase de mise hors service ou au rebut peuvent être différentes de celles prescrites lors de la phase d'exploitation.

7.17.2.7 Une documentation chronologique doit être établie et tenue à jour. Elle doit contenir les documents détaillant le processus de mise hors service ou au rebut, et doit faire référence:

– au plan utilisé pour les activités de mise hors service ou au rebut;

– à l'analyse d'impact.

7.18 Vérification

7.18.1 Objectif

L'objectif des prescriptions de ce paragraphe est de démontrer, pour chaque phase des cycles de vie globaux de sécurité des E/E/PES et du logiciel (par des revues, analyses et/ou tests), que les données de sortie remplissent à tous les égards les objectifs et prescriptions spécifiés pour cette phase.

7.18.2 Prescriptions

7.18.2.1 Pour chaque phase des cycles de vie globaux de sécurité des E/E/PES et du logiciel, un plan pour la vérification doit être établi en parallèle avec le développement de cette phase.

7.18.2.2 Le plan de vérification doit documenter ou faire référence aux critères, techniques, outils devant être utilisés par les activités de vérification.

7.18.2.3 La vérification doit être réalisée conformément au plan de vérification.

NOTE – La sélection des techniques et des mesures pour la vérification, et le degré d'indépendance pour les activités de vérification, dépendra d'un certain nombre de facteurs et peut être spécifié dans les normes d'application sectorielle.

Ces facteurs pourraient inclure, par exemple

– la taille du projet;

– le degré de complexité;

– le degré d'innovation de la conception;

– le degré d'innovation de la technologie.

7.18.2.4 L'information sur les activités de vérification doit être collectée et documentée comme preuve que la phase en cours de vérification a été, en tout point, correctement réalisée.

7.17.2.5 Prior to decommissioning or disposal taking place a plan shall be prepared which shall include procedures for

– the closing down of the E/E/PE safety-related systems;

– dismantling the E/E/PE safety-related systems.

7.17.2.6 If any decommissioning or disposal activity has an impact on the functional safety of any E/E/PE safety-related system, this shall initiate a return to the appropriate phase of the overall, E/E/PES or software safety lifecycles. All subsequent phases shall then be carried out in accordance with the procedures specified in this standard for the specified safety integrity levels for the E/E/PE safety-related systems.

NOTE 1 – It may be necessary to implement a full hazard and risk analysis which may generate a need for a different safety integrity level for the E/E/PE safety-related systems.

NOTE 2 – The functional safety requirements during the decommissioning or disposal phase may be different from those required during the operational phase.

7.17.2.7 Chronological documentation shall be established and maintained which shall document details of the decommissioning or disposal activities and shall include references to

– the plan used for the decommissioning or disposal activities;

– the impact analysis.

7.18 Verification

7.18.1 Objective

The objective of the requirements of this subclause is to demonstrate, for each phase of the overall, E/E/PES and software safety lifecycles (by review, analysis and/or tests), that the outputs meet in all respects the objectives and requirements specified for the phase.

7.18.2 Requirements

7.18.2.1 For each phase of the overall, E/E/PES and software safety lifecycles, a plan for the verification shall be established concurrently with the development for the phase.

7.18.2.2 The verification plan shall document or refer to the criteria, techniques, tools to be used in the verification activities.

7.18.2.3 The verification shall be carried out according to the verification plan.

NOTE – Selection of techniques and measures for verification, and the degree of independence for the verification activities, will depend upon a number of factors and may be specified in application sector standards.

The factors could include, for example

– size of project;

– degree of complexity;

– degree of novelty of design;

– degree of novelty of technology.

7.18.2.4 Information on the verification activities shall be collected and documented as evidence that the phase being verified has, in all respects, been satisfactorily completed.

8 Evaluation de la sécurité fonctionnelle

8.1 Objectif

L'objectif des prescriptions de cet article est d'enquêter et d'élaborer un jugement sur la sécurité fonctionnelle réalisée par les systèmes de sécurité E/E/PE.

8.2 Prescriptions

8.2.1 Une ou plusieurs personnes doivent être désignées pour exécuter une évaluation de la sécurité fonctionnelle afin d'élaborer un jugement sur la sécurité fonctionnelle réalisée par les systèmes de sécurité E/E/PE.

8.2.2 Les responsables de cette évaluation de la sécurité fonctionnelle doivent pouvoir contacter toutes les personnes impliquées dans toute activité du cycle de vie de sécurité global du E/E/PES ou du logiciel, et avoir accès à toute information et tout équipement (matériel et logiciel) pertinents.

8.2.3 L'évaluation de la sécurité fonctionnelle doit être appliquée à toutes les phases des cycles de vie globaux de sécurité des E/E/PES et du logiciel. Les responsables de l'évaluation de la sécurité fonctionnelle doivent prendre en compte les activités menées, et les données de sorties obtenues au cours de chaque phase des cycles de vie globaux de sécurité des E/E/PES et du logiciel, et juger dans quelle mesure les objectifs et prescriptions de la présente norme ont été remplis.

8.2.4 L'évaluation de la sécurité fonctionnelle doit être menée tout au long des cycles de vie globaux des E/E/PES et du logiciel et peut être réalisée après chaque phase du cycle de vie de sécurité ou après un ensemble de phases du cycle de vie de sécurité, sous réserve de la prescription prioritaire requérant qu'une évaluation de la sécurité fonctionnelle soit réalisée avant que les dangers déterminés soient présents.

8.2.5 Si des outils sont utilisés lors de la conception ou de l'évaluation pour toute activité du cycle de vie de sécurité global du E/E/PES ou du logiciel, il convient de les soumettre eux-mêmes à une évaluation de la sécurité fonctionnelle.

NOTE 1 – Comme exemple d'outil, citons les systèmes de CAO/FAO, les compilateurs et les systèmes cibles principaux.

NOTE 2 – Le degré d'évaluation de l'utilisation de ces outils dépendra de leur impact sur la sécurité fonctionnelle des systèmes de sécurité E/E/PE.

8.2.6 L'évaluation de la sécurité fonctionnelle doit tenir compte des points suivants:

– le travail effectué depuis l'évaluation de la sécurité fonctionnelle précédente (qui, normalement, aura englobé les phases précédentes du cycle de vie de sécurité);

– les plans ou la stratégie pour la mise en œuvre ultérieure d'évaluations de la sécurité fonctionnelle des cycles de vie de sécurité globaux des E/E/PES et du logiciel;

– les recommandations des évaluations de la sécurité fonctionnelle précédentes, et l'étendue des changements réalisés depuis.

8.2.7 Les activités d'évaluation de la sécurité fonctionnelle pour les différentes phases des cycles de vie de sécurité globaux des E/E/PES et du logiciel doivent être cohérentes et planifiées.

8 Functional safety assessment

8.1 Objective

The objective of the requirements of this clause is to investigate and arrive at a judgement on the functional safety achieved by the E/E/PE safety-related systems.

8.2 Requirements

8.2.1 One or more persons shall be appointed to carry out a functional safety assessment in order to arrive at a judgement of the functional safety achieved by the E/E/PE safety-related systems.

8.2.2 Those carrying out the functional safety assessment shall have access to all persons involved in any overall, E/E/PES or software safety lifecycle activity and all relevant information and equipment (both hardware and software).

8.2.3 The functional safety assessment shall be applied to all phases throughout the overall, E/E/PES and software safety lifecycles. Those carrying out the functional safety assessment shall consider the activities carried out and the outputs obtained during each phase of the overall, E/E/PES and software safety lifecycles and judge the extent to which the objectives and requirements in this standard have been met.

8.2.4 The functional safety assessment shall be carried out throughout the overall, E/E/PES and software lifecycles, and may be carried out after each safety lifecycle phase or after a number of safety lifecycle phases, subject to the overriding requirement that a functional safety assessment shall be undertaken prior to the determined hazards being present.

8.2.5 If tools are used as part of design or assessment for any overall, E/E/PES or software safety lifecycle activity, they should themselves be subject to the functional safety assessment.

NOTE 1 – Example tools are CAD/CAM systems, compilers and host target systems.

NOTE 2 – The degree to which the use of such tools will need to be evaluated will depend upon their impact on the functional safety of the E/E/PE safety-related systems.

8.2.6 The functional safety assessment shall consider the following:

– the work done since the previous functional safety assessment (which will normally have covered previous safety lifecycle phases);
– the plans or strategy for implementing further functional safety assessments of the overall, E/E/PES and software safety lifecycles;
– the recommendations of the previous functional safety assessments and the extent to which changes have been made.

8.2.7 The functional safety assessment activities for the different phases of the overall, E/E/PES and software safety lifecycles shall be consistent and planned.

8.2.8 Le plan pour l'évaluation de la sécurité fonctionnelle doit spécifier

– les responsables de l'évaluation de la sécurité fonctionnelle;
– les résultats de chaque évaluation de la sécurité fonctionnelle;
– le domaine de l'évaluation de la sécurité fonctionnelle;

NOTE – Lors de la définition du domaine de l'évaluation de la sécurité fonctionnelle, il sera nécessaire de spécifier les documents, et leur statut, qui seront utilisés comme données d'entrées pour chaque activité d'évaluation.

– les organismes de sécurités impliqués;
– les ressources nécessaires;
– le degré d'indépendance des responsables de l'évaluation de la sécurité fonctionnelle;
– la compétence des responsables de l'évaluation de la sécurité fonctionnelle vis-à-vis de l'application.

8.2.9 Avant d'entreprendre l'évaluation de la sécurité fonctionnelle, le plan pour l'évaluation de la sécurité fonctionnelle doit être approuvé par les responsables de l'évaluation de la sécurité fonctionnelle et par les responsables de la gestion de la sécurité fonctionnelle pour les phases du cycle de vie de sécurité devant être évaluées.

8.2.10 En conclusion de l'évaluation de la sécurité fonctionnelle, des recommandations doivent être émises pour l'acceptation, l'acceptation conditionnelle ou le rejet.

8.2.11 Les responsables de l'évaluation de la sécurité fonctionnelle doivent être compétents pour les activités entreprises, et il est recommandé de prêter attention aux facteurs pour l'évaluation de la compétence indiqués en annexe B.

8.2.12 Sauf si une norme d'application sectorielle internationale indique le contraire, le degré minimal d'indépendance des responsables de l'évaluation de la sécurité fonctionnelle doit être tel que spécifié dans les tableaux 4 et 5. Les recommandations des tableaux sont les suivantes.

– HR: le degré d'indépendance spécifié est Hautement Recommandé comme étant un minimum pour la «conséquence» spécifiée (tableau 4) ou le niveau d'intégrité de sécurité (tableau 5). En cas d'adoption d'un degré d'indépendance inférieur, il convient d'expliquer en détail pourquoi on n'a pas utilisé le degré HR.
– NR: le degré d'indépendance spécifié est considéré comme insuffisant et est nettement Non Recommandé pour la «conséquence» spécifiée (tableau 4) ou le niveau d'intégrité de sécurité (tableau 5). En cas d'adoption de ce degré d'indépendance, il convient d'expliquer en détail les motifs de ce choix.
– -: le degré d'indépendance spécifié n'a de recommandation ni pour ni contre son adoption.

NOTE 1 – Avant l'application du tableau 4, il sera nécessaire de définir les catégories de «conséquences», en tenant compte des bonnes pratiques habituelles du secteur d'application. Les «conséquences» sont celles qui pourraient se produire en cas de défaillance des systèmes de sécurité E/E/PE alors que leur fonctionnement est requis.

NOTE 2 – Selon l'organisation de l'entreprise et l'expertise au sein de cette entreprise, il se peut que la prescription s'appliquant aux personnes et services indépendants doive être remplie par l'utilisation d'une organisation extérieure. Inversement, les entreprises qui ont des organisations internes qualifiées pour l'évaluation du risque et son application aux systèmes de sécurité, qui sont indépendantes et séparées (par l'intermédiaire de la hiérarchie et autres moyens) de celles responsables du développement principal, peuvent être capables d'utiliser leurs ressources propres pour remplir les prescriptions s'appliquant à une organisation indépendante.

NOTE 3 – Voir 3.8.10, 3.8.11 et 3.8.12 de la CEI 61508-4 pour les définitions, respectivement, des «personnes indépendantes», du «service indépendant» et de l'«organisation indépendante».

8.2.8 The plan for the functional safety assessment shall specify

– those to undertake the functional safety assessment;

– the outputs from each functional safety assessment;

– the scope of the functional safety assessment;

NOTE – In establishing the scope of the functional safety assessment, it will be necessary to specify the documents, and their status, which are to be used as inputs for each assessment activity.

– the safety bodies involved;

– the resources required;

– the level of independence of those undertaking the functional safety assessment;

– the competence of those undertaking the functional safety assessment relative to the application.

8.2.9 Prior to a functional safety assessment taking place, the plan for the functional safety assessment shall be approved by those carrying out the functional safety assessment and by those responsible for the management of functional safety for the safety lifecycle phases being assessed.

8.2.10 At the conclusion of the functional safety assessment, recommendations shall be produced for acceptance, qualified acceptance or rejection.

8.2.11 Those carrying out the functional safety assessment shall be competent for the activities to be undertaken, and notice should be taken of the factors for assessing competence in annex B.

8.2.12 Unless otherwise stated in application sector international standards, the minimum level of independence of those carrying out the functional safety assessment shall be as specified in tables 4 and 5. The recommendations in the tables are as follows.

– HR: the level of independence specified is highly recommended as a minimum for the specified consequence (table 4) or safety integrity level (table 5). If a lower level of independence is adopted then the rationale for not using the HR level should be detailed.

– NR: the level of independence specified is considered insufficient and is positively not recommended for the specified consequence (table 4) or safety integrity level (table 5). If this level of independence is adopted then the rationale for using it should be detailed.

– -: the level of independence specified has no recommendation for or against being used.

NOTE 1 – Prior to the application of table 4, it will be necessary to define the consequence categories, taking into account current good practices in the application sector. The consequences are those that would arise in the event of failure, when required to operate, of the E/E/PE safety-related systems.

NOTE 2 – Depending upon the company organization and expertise within the company, the requirement for independent persons and departments may have to be met by using an external organization. Conversely, companies that have internal organizations skilled in risk assessment and the application of safety-related systems, which are independent of and separate (by ways of management and other resources) from those responsible for the main development, may be able to use their own resources to meet the requirements for an independent organization.

NOTE 3 – See 3.8.10, 3.8.11 and 3.8.12 of IEC 61508-4 for definitions of independent person, independent department, and independent organization respectively.

8.2.13 Dans le cadre des tableaux 4 et 5, soit HR1, soit HR2 est à retenir (pas les deux), en fonction d'un certain nombre de facteurs propres à l'application. Si HR1 est retenu, alors il convient de considérer HR2 comme n'étant pas une prescription; si HR2 est retenu, alors il convient de considérer HR1 comme valant NR (non recommandé). S'il n'existe pas de normes d'application sectorielle, il convient d'expliquer en détail les raisons du choix de HR1 ou HR2. Les facteurs qui tendront à rendre HR2 plus approprié que HR1 sont

– manque d'expérience antérieure d'une conception du système similaire;
– niveau de complexité plus élevé;
– plus grande nouveauté de la conception;
– plus grande nouveauté de la technologie;
– manque de normalisation des particularités de conception.

8.2.14 Dans le cadre du tableau 5, les degrés minimaux d'indépendance doivent être basés sur la fonction de sécurité, exécutée par le système de sécurité E/E/PE, qui possède le plus haut niveau d'intégrité de sécurité.

Tableau 4 – Degrés minimaux d'indépendance des responsables de l'évaluation de la sécurité fonctionnelle (phases du cycle de vie de sécurité global 1 à 8 et 12 à 16 incluse (voir figure 2))

Degré minimal d'indépendance	Conséquence (voir note 2)			
	A	B	C	D
Personne indépendante	HR	HR1	NR	NR
Service indépendant	–	HR2	HR1	NR
Organisation indépendante (voir note 2 de 8.2.12)	–	–	HR2	HR
NOTE 1 – Voir 8.2.12 (notes comprises) et 8.2.13 pour les détails d'interprétation de ce tableau. NOTE 2 – Les conséquences typiques peuvent être: conséquence A – petite blessure (par exemple perte temporaire de fonction); conséquence B – blessure grave et permanente d'une ou plusieurs personnes, mort d'une personne; conséquence C – mort de quelques personnes; conséquence D – nombreuses personnes tuées.				

Tableau 5 – Degrés minimaux d'indépendance des responsables de l'évaluation de la sécurité fonctionnelle (phase 9 du cycle de vie de sécurité global, incluant toutes les phases des cycles de vie de sécurité du E/E/PES et du logiciel (voir figures 2, 3 et 4))

Degré minimaux d'indépendance	Niveau d'intégrité de sécurité			
	1	2	3	4
Personne indépendante	HR	HR1	NR	NR
Service indépendant	–	HR2	HR1	NR
Organisation indépendante (voir note 2 de 8.2.12)	–	–	HR2	HR
NOTE – Voir 8.2.12 (notes comprises), 8.2.13 et 8.2.14 pour les détails d'interprétation de ce tableau.				

8.2.13 In the context of tables 4 and 5, either HR[1] or HR[2] is applicable (not both), depending on a number of factors specific to the application. If HR[1] is applicable then HR[2] should be read as no requirement; if HR[2] is applicable then HR[1] should be read as NR (not recommended). If no application sector standard exists, the rationale for choosing HR[1] or HR[2] should be detailed. Factors that will tend to make HR[2] more appropriate than HR[1] are

– lack of previous experience with a similar design;
– greater degree of complexity;
– greater degree of novelty of design;
– greater degree of novelty of technology;
– lack of degree of standardization of design features.

8.2.14 In the context of table 5, the minimum levels of independence shall be based on the safety function, carried out by the E/E/PE safety-related system, that has the highest safety integrity level.

Table 4 – Minimum levels of independence of those carrying out functional safety assessment (overall safety lifecycle phases 1 to 8 and 12 to 16 inclusive (see figure 2))

Minimum level of independence	Consequence (see note 2)			
	A	B	C	D
Independent person	HR	HR[1]	NR	NR
Independent department	–	HR[2]	HR[1]	NR
Independent organization (see note 2 of 8.2.12)	–	–	HR[2]	HR
NOTE 1 – See 8.2.12 (including notes) and 8.2.13 for details on interpreting this table. NOTE 2 – Typical consequences could be: consequence A – minor injury (for example temporary loss of function); consequence B – serious permanent injury to one or more persons, death to one person; consequence C – death to several people; consequence D – very many people killed.				

Table 5 – Minimum levels of independence of those carrying out functional safety assessment (overall safety lifecycle phase 9, including all phases of E/E/PES and software safety lifecycles (see figures 2, 3 and 4))

Minimum level of Independence	Safety integrity level			
	1	2	3	4
Independent person	HR	HR[1]	NR	NR
Independent department	–	HR[2]	HR[1]	NR
Independent organization (see note 2 of 8.2.12)	–	–	HR[2]	HR
NOTE – See 8.2.12 (including notes), 8.2.13 and 8.2.14 for details on interpreting this table.				

Annexe A
(informative)

Exemple de structure de documentation

A.1 Généralités

Cette annexe propose un exemple de structure de documentation et une méthode de spécification des documents pour structurer l'information afin de remplir les prescriptions de l'article 5. La documentation se doit de contenir l'information nécessaire et suffisante à l'exécution efficace de

– chaque phase des cycles de vie de sécurité globaux des E/E/PES et du logiciel;

– la gestion de la sécurité fonctionnelle (article 6);

– les évaluations de la sécurité fonctionnelle (article 8).

La constitution de l'information suffisante dépendra d'un certain nombre de facteurs, y compris la complexité et la taille des systèmes de sécurité E/E/PE et les prescriptions relatives à des applications spécifiques. La documentation nécessaire peut être spécifiée dans des normes d'application sectorielle internationales.

La somme d'information dans chaque document peut aller de quelques lignes à quelques pages, et l'ensemble complet d'information peut être divisé et présenté dans plusieurs documents physiques (matériels) ou un seul document physique. Là aussi, la structure physique de la documentation dépendra de la complexité et de la taille des systèmes de sécurité E/E/PE et tiendra compte des procédures de l'entreprise ainsi que les habitudes de travail du secteur d'application spécifique.

L'exemple de structure de documentation indiqué dans cette annexe est proposé pour illustrer une façon parmi d'autres de structurer l'information et la façon dont les documents pourraient être titrés. Voir la référence [4]* de l'annexe C pour de plus amples détails.

Un document est une quantité structurée d'informations destinée à la perception humaine, pouvant être échangée unitairement entre des utilisateurs et/ou des systèmes (voir ISO 8613-1) [5]*. Ce terme ne s'applique donc pas seulement aux documents au sens courant, mais aussi à des concepts comme les fichiers de données et les bases de données d'information.

Dans la présente norme, le terme «document» est généralement compris au sens «d'information» plutôt que documents physiques, sauf si le contraire est explicitement indiqué ou si le contexte de l'article ou du paragraphe dans lequel il est employé amène un autre sens. Les documents peuvent être disponibles sous différentes formes pour la présentation à l'homme (par exemple sur papier, film ou tout support de données pouvant être présenté sur des écrans).

L'exemple de structure de documentation de cette annexe spécifie les documents en deux parties:

– **le type de document**;

– **l'activité ou l'objet**.

_____

* Les chiffres entre crochets se réfèrent à la bibliographie donnée en annexe C.

Annex A
(informative)

Example documentation structure

A.1 General

This annex provides an example documentation structure and method for specifying the documents for structuring the information in order to meet the requirements in clause 5. The documentation has to contain sufficient information necessary to effectively perform

– each phase of the overall, E/E/PES and software safety lifecycles;
– the management of functional safety (clause 6);
– functional safety assessments (clause 8).

What constitutes sufficient information will be dependent upon a number of factors, including the complexity and size of the E/E/PE safety-related systems and the requirements relating to the specific application. The necessary documentation may be specified in application specific international standards.

The amount of information in each document may vary from a few lines to many pages, and the complete set of information may be divided and presented in many physical documents or one physical document. The physical documentation structure will again depend upon the size and complexity of the E/E/PE safety-related systems, and will take into account company procedures and the working practices of the specific application sector.

The example documentation structure indicated in this annex has been provided to illustrate one particular way in which the information could be structured and the way the documents could be titled. See reference [4]* in annex C for more details.

A document is a structured amount of information intended for human perception, that may be interchanged as a unit between users and/or systems (see ISO 8613-1) [5]*. The term applies therefore not only to documents in the traditional sense, but also to concepts such as data files and database information.

In this standard, the term document is understood normally to mean information rather than physical documents, unless this is explicitly declared or understood in the context of the clause or subclause in which it is stated. Documents may be available in different forms for human presentation (for example on paper, film or any data medium to be presented on screens or displays).

The example documentation structure in this annex specifies documents in two parts:

– **document kind**;
– **activity or object**.

_____

* Figures in square brackets refer to the bibliography given in annex C.

Le type de document est défini dans la CEI 61355 [3] et caractérise le contenu du document, par exemple une «description de fonction» ou un «diagramme de circuit». L'activité ou l'objet décrit le domaine du contenu, par exemple «système de commande de pompe».

Les types de documents de base spécifiés dans la présente annexe sont

– **spécification** – spécifie une fonction, performance ou activité prescrite (par exemple une spécification de prescriptions);
– **description** – spécifie une fonction, un projet, un fonctionnement ou activité prévu ou réel (par exemple une description de fonction);
– **instruction** – spécifie en détail les instructions expliquant quand, comment réaliser certains travaux (par exemple une instruction d'opérateur);
– **plan** – spécifie le plan expliquant quand, comment par qui des activités spécifiques doivent être réalisées (par exemple un plan de maintenance);
– **diagramme** – spécifie la fonction à l'aide d'un diagramme (symboles et lignes) représentant les signaux entre les symboles;
– **liste** – fournit l'information sous la forme d'une liste (par exemple liste de codes, de signaux);
– **journal** – fournit l'information sur les événements sous la forme d'un enregistrement chronologique;
– **rapport** – décrit les résultats d'activités telles que les enquêtes, les évaluations, les tests, etc. (par exemple un rapport de test);
– **demande** – fournit une description des actions demandées et qui doivent être approuvées et spécifiées ultérieurement (par exemple demande de maintenance).

Les types basiques de document peuvent avoir un suffixe, tel que spécification de **prescriptions** ou spécification de **test**, qui caractérise d'avantage le contenu.

A.2 Structure du document du cycle de vie de sécurité

Les tableaux A.1, A.2 et A.3 fournissent un exemple de structure de documentation pour structurer l'information afin de satisfaire aux prescriptions spécifiées à l'article 5. Les tableaux indiquent la phase du cycle de vie de sécurité qui est principalement associée aux documents (généralement la phase dans laquelle ils sont élaborés). Les noms donnés aux documents dans les tableaux sont en accord avec la syntaxe esquissée en A.1.

En plus des documents listés dans les tableaux A.1, A.2 et A.3, il peut y avoir des documents supplémentaires donnant une information détaillée supplémentaire ou une information structurée dans un but spécifique, par exemple des listes de pièces, des listes de signaux, des listes de câbles, des tableaux de câblage, des diagrammes de boucle, des listes de variables.

NOTE – Comme exemples de telles variables, citons les valeurs pour les régulateurs, les valeurs d'alarme pour les variables, les priorités dans l'exécution des tâches par l'ordinateur. Certaines valeurs des variables peuvent être données avant la livraison du système, d'autres peuvent être données lors de la mise en service ou de la maintenance.

The document kind is defined in the IEC 61355 [3] and characterizes the content of the document, for example function description or circuit diagram. The activity or object describes the scope of the content, for example pump control system.

The basic document kinds specified in this annex are

– **specification** – specifies a required function, performance or activity (for example requirements specification);
– **description** – specifies a planned or actual function, design, performance or activity (for example function description);
– **instruction** – specifies in detail the instructions as to when and how to perform certain jobs (for example operator instruction);
– **plan** – specifies the plan as to when, how and by whom specific activities shall be performed (for example maintenance plan);
– **diagram** – specifies the function by means of a diagram (symbols and lines) representing signals between the symbols;
– **list** – provides information in a list form (for example code list, signal list);
– **log** – provides information on events in a chronological log form;
– **report** – describes the results of activities such as investigations, assessments, tests etc. (for example test report);
– **request** – provides a description of requested actions that have to be approved and further specified (for example maintenance request).

The basic document kind may have a prefix, such as **requirements** specification or **test** specification, which further characterizes the content.

A.2 Safety lifecycle document structure

Tables A.1, A.2 and A.3 provide an example documentation structure for structuring the information in order to meet the requirements specified in clause 5. The tables indicate the safety lifecycle phase that is mainly associated with the documents (usually the phase in which they are developed). The names given to the documents in the tables is in accordance with the scheme outlined in A.1.

In addition to the documents listed in tables A.1, A.2 and A.3, there may be supplementary documents giving detailed additional information or information structured for a specific purpose, for example parts lists, signal lists, cable lists, wiring tables, loop diagrams, list of variables.

NOTE – Examples of such variables are values for regulators, alarm values for variables, priorities in the execution of tasks in the computer. Some of the values of the variables could be given before the delivery of the system, others could be given during commissioning or maintenance.

Tableau A.1 – Exemple de structure de documentation pour l'information relative au cycle de vie de sécurité global

Phase du cycle de vie de sécurité global	Information
Concept	Description (concept global)
Définition globale du domaine d'application	Description (définition globale du domaine d'application)
Analyse de danger et de risque	Description (analyse de danger et de risque)
Prescriptions globales de sécurité	Spécification (prescriptions globales de sécurité, comprenant: fonctions de sécurité globales et intégrité de sécurité globale)
Allocation des prescriptions de sécurité	Description (allocation des prescriptions de sécurité)
Planification globale de l'exploitation et de la maintenance	Plan (exploitation et maintenance globales)
Planification globale de la validation de la sécurité	Plan (validation globale de la sécurité)
Planification globale de l'installation et de la mise en service	Plan (installation globale); Plan (mise en service globale)
Réalisation	Réalisation des systèmes de sécurité E/E/PE (voir la CEI 61508-2 et la CEI 61508-3)
Installation et mise en service globales	Rapport (installation globale); Rapport (mise en service globale)
Validation globale de la sécurité	Rapport (validation globale de la sécurité)
Exploitation et maintenance globales	Journal (exploitation et maintenance globales)
Modification et remise à niveau globales	Demande (modification globale); Rapport (analyse d'impact des modification et remise à niveau globales); Journal (modification et remise à niveau globales)
Mise hors service ou au rebut	Rapport (analyse d'impact de la mise hors service ou au rebut globale); Plan (mise hors service ou au rebut globale); Journal (mise hors service ou au rebut globale)
Concerne toutes les phases	Plan (sécurité); Plan (vérification); Rapport (vérification); Plan (évaluation de la sécurité fonctionnelle); Rapport (évaluation de la sécurité fonctionnelle)

Table A.1 – Example documentation structure for information related to the overall safety lifecycle

Overall safety lifecycle phase	Information
Concept	Description (overall concept)
Overall scope definition	Description (overall scope definition)
Hazard and risk analysis	Description (hazard and risk analysis)
Overall safety requirements	Specification (overall safety requirements, comprising: overall safety functions and overall safety integrity)
Safety requirements allocation	Description (safety requirements allocation)
Overall operation and maintenance planning	Plan (overall operation and maintenance)
Overall safety validation planning	Plan (overall safety validation)
Overall installation and commissioning planning	Plan (overall installation); Plan (overall commissioning)
Realisation	Realisation of E/E/PE safety-related systems (see IEC 61508-2 and IEC 61508-3)
Overall installation and commissioning	Report (overall installation); Report (overall commissioning)
Overall safety validation	Report (overall safety validation)
Overall operation and maintenance	Log (overall operation and maintenance)
Overall modification and retrofit	Request (overall modification); Report (overall modification and retrofit impact analysis); Log (overall modification and retrofit)
Decommissioning or disposal	Report (overall decommissioning or disposal impact analysis); Plan (overall decommissioning or disposal); Log (overall decommissioning or disposal)
Concerning all phases	Plan (safety); Plan (verification); Report (verification); Plan (functional safety assessment); Report (functional safety assessment)

Tableau A.2 – Exemple de structure de documentation pour l'information relative au cycle de vie de sécurité du système E/E/PE

Phase du cycle de vie de sécurité du système E/E/PE	Information
Prescriptions de sécurité des E/E/PES	Spécification (Prescriptions de sécurité des E/E/PES, comprenant: fonctions de sécurité E/E/PES et l'intégrité de sécurité du E/E/PES)
Planification de la validation du E/E/PES	Plan (validation de la sécurité du E/E/PES)
Conception et développement du E/E/PES	
Architecture du E/E/PES	Description (conception de l'architecture du E/E/PES, comprenant: l'architecture du matériel et l'architecture du logiciel); Spécification (tests d'intégration de l'électronique programmable); Spécification (tests d'intégration du matériel électronique programmable et non électronique programmable)
Architecture du matériel	Description (conception de l'architecture matérielle); Spécification (tests d'intégration de l'architecture matérielle)
Conception du module matériel	Spécification (conception des modules matériels); Spécifications (test des modules matériels)
Construction et/ou achat de composants	Modules matériels; Rapport (test des modules matériels)
Intégration de l'électronique programmable	Rapport (test d'intégration de l'électronique programmable et du logiciel) (voir tableau A.3)
Intégration du E/E/PES	Rapport (test d'intégration de l'électronique programmable et autre matériel)
Procédures d'exploitation et maintenance du E/E/PES	Instruction (utilisateur); Instruction (exploitation et maintenance)
Validation de la sécurité du E/E/PES	Rapport (validation de la sécurité du E/E/PES)
Modification du E/E/PES	Instruction (procédures de modification du E/E/PES); Demande (modification du E/E/PES); Rapport (analyse d'impact d'une modification du E/E/PES); Journal (modification du E/E/PES)
Concerne toutes les phases	Plan (sécurité du E/E/PES); Plan (vérification du E/E/PES); Rapport (vérification du E/E/PES); Plan (évaluation de la sécurité fonctionnelle du E/E/PES); Rapport (évaluation de la sécurité fonctionnelle du E/E/PES)

Table A.2 – Example documentation structure for information related to the E/E/PES safety lifecycle

E/E/PES safety lifecycle phase	Information
E/E/PES safety requirements	Specification (E/E/PES safety requirements, comprising: E/E/PES safety functions and E/E/PES safety integrity)
E/E/PES validation planning	Plan (E/E/PES safety validation)
E/E/PES design and development	
E/E/PES architecture	Description (E/E/PES architecture design, comprising: hardware architecture and software architecture); Specification (programmable electronic integration tests); Specification (integration tests of programmable electronic and non programmable electronic hardware)
Hardware architecture	Description (hardware architecture design); Specification (hardware architecture integration tests)
Hardware module design	Specification (hardware modules design); Specifications (hardware modules test)
Component construction and/or procurement	Hardware modules; Report (hardware modules test)
Programmable electronic integration	Report (programmable electronic and software integration test) (see table A.3)
E/E/PES integration	Report (programmable electronic and other hardware integration test)
E/E/PES operation and maintenance procedures	Instruction (user); Instruction (operation and maintenance)
E/E/PES safety validation	Report (E/E/PES safety validation)
E/E/PES modification	Instruction (E/E/PES modification procedures); Request (E/E/PES modification); Report (E/E/PES modification impact analysis); Log (E/E/PES modification)
Concerning all phases	Plan (E/E/PES safety); Plan (E/E/PES verification); Report (E/E/PES verification); Plan (E/E/PES functional safety assessment); Report (E/E/PES functional safety assessment)

Tableau A.3 – Exemple de structure de documentation pour l'information relative au cycle de vie de sécurité du logiciel

Phase du cycle de vie de sécurité du logiciel	Information
Prescriptions de sécurité logicielle	Spécification (prescriptions de sécurité logicielle, comprenant: les fonctions de sécurité du logiciel et l'intégrité de sécurité du logiciel)
Planification de la validation de la sécurité logicielle	Plan (validation de la sécurité logicielle)
Conception et développement du logiciel	
Architecture logicielle	Description (conception de l'architecture logicielle) (voir tableau A.2 pour la description de la conception de l'architecture matérielle); Spécification (tests d'intégration de l'architecture logicielle); Spécification (test d'intégration de l'électronique programmable et du logiciel); Instruction (outils de développement et manuel de codage)
Conception du système logiciel	Description (conception du système logiciel); Spécification (tests d'intégration du système logiciel)
Conception du module logiciel	Spécification (conception du module logiciel); Spécification (tests du module logiciel)
Codage	Liste (code source); Rapport (test du module logiciel); Rapport (revue de code)
Tests du module logiciel	Rapport (test du module logiciel)
Intégration du logiciel	Rapport (test d'intégration du module logiciel); Rapport (test d'intégration du système logiciel); Rapport (test d'intégration de l'architecture logicielle)
Intégration de l'électronique programmable	Rapport (test d'intégration de l'électronique programmable et du logiciel)
Procédures d'exploitation et de maintenance du logiciel	Instruction (utilisateur); Instruction (exploitation et maintenance)
Validation de la sécurité logicielle	Rapport (validation de la sécurité logicielle)
Modification du logiciel	Instruction (procédures de modification du logiciel); Demande (modification du logiciel); Rapport (analyse d'impact d'une modification du logiciel); Journal (modification du logiciel)
Concerne toutes les phases	Plan (sécurité logicielle); Plan (vérification du logiciel); Rapport (vérification du logiciel); Plan (évaluation de la sécurité fonctionnelle du logiciel); Rapport (évaluation de la sécurité fonctionnelle du logiciel)

A.3 Structure physique du document

La structure physique de la documentation correspond à la façon dont les différents documents sont assemblés en documents, ensembles de documents, classeurs et groupes de classeurs. La figure A.1 présente des exemples de tels ensembles de classeurs structurés selon les groupes d'utilisateurs. Un même document peut apparaître dans différents ensembles.

Pour un système grand et complexe, il est très probable que les nombreux documents soient divisés en plusieurs classeurs. Pour un petit système, de faible complexité, avec un nombre limité de documents physiques, ils peuvent être tous rassemblés dans un seul classeur avec différentes étiquettes intercalaires pour les différents ensembles de documents (voir figure A.2).

La structure physique fournit un moyen de sélection de la documentation nécessaire pour des activités spécifiques par la personne ou le groupe de personnes réalisant ces activités. Par conséquent, certains documents physiques peuvent apparaître dans plusieurs ensembles de classeurs ou tout autre media (par exemple les disques informatiques).

Table A.3 – Example documentation structure for information related to the software safety lifecycle

Software safety lifecycle phase	Information
Software safety requirements	Specification (software safety requirements, comprising: software safety functions and software safety integrity)
Software validation planning	Plan (software safety validation)
Software design and development	
Software architecture	Description (software architecture design) (see table A.2 for hardware architecture design description); Specification (software architecture integration tests); Specification (programmable electronic and software integration tests); Instruction (development tools and coding manual)
Software system design	Description (software system design); Specification (software system integration tests)
Software module design	Specification (software module design); Specification (software module tests)
Coding	List (source code); Report (software module test); Report (code review)
Software module testing	Report (software module test)
Software integration	Report (software module integration test); Report (software system integration test); Report (software architecture integration test)
Programmable electronic integration	Report (programmable electronic and software integration test)
Software operation and maintenance procedures	Instruction (user); Instruction (operation and maintenance)
Software safety validation	Report (software safety validation)
Software modification	Instruction (software modification procedures); Request (software modification); Report (software modification impact analysis); Log (software modification)
Concerning all phases	Plan (software safety); Plan (software verification); Report (software verification); Plan (software functional safety assessment); Report (software functional safety assessment)

A.3 Physical document structure

The physical structure of the documentation is the way that the different documents are combined into documents, document sets, binders and groups of binders. Figure A.1 shows examples of such sets of binders structured according to user groups. The same document may occur in different sets.

For a large and complex system, the many physical documents are likely to be split into several binders. For a small, low complexity system with a limited number of physical documents, they may be combined into one binder with different tabs for the different sets of documents (see figure A.2).

The physical structure provides a means of selecting the documentation needed for the specific activities by the person or group of persons performing the activities. Consequently, some of the physical documents may occur in several binder sets or other media (for example computer disks).

NOTE – L'information prescrite par les documents du tableau A.1 peut être contenue dans les divers ensembles de documents présentés aux figures A.1 et A.2. Par exemple, au sein du groupe pour l'ingénierie, on pourra trouver des documents comme la description de l'analyse de danger et de risque et/ou la spécification des prescriptions globales de sécurité.

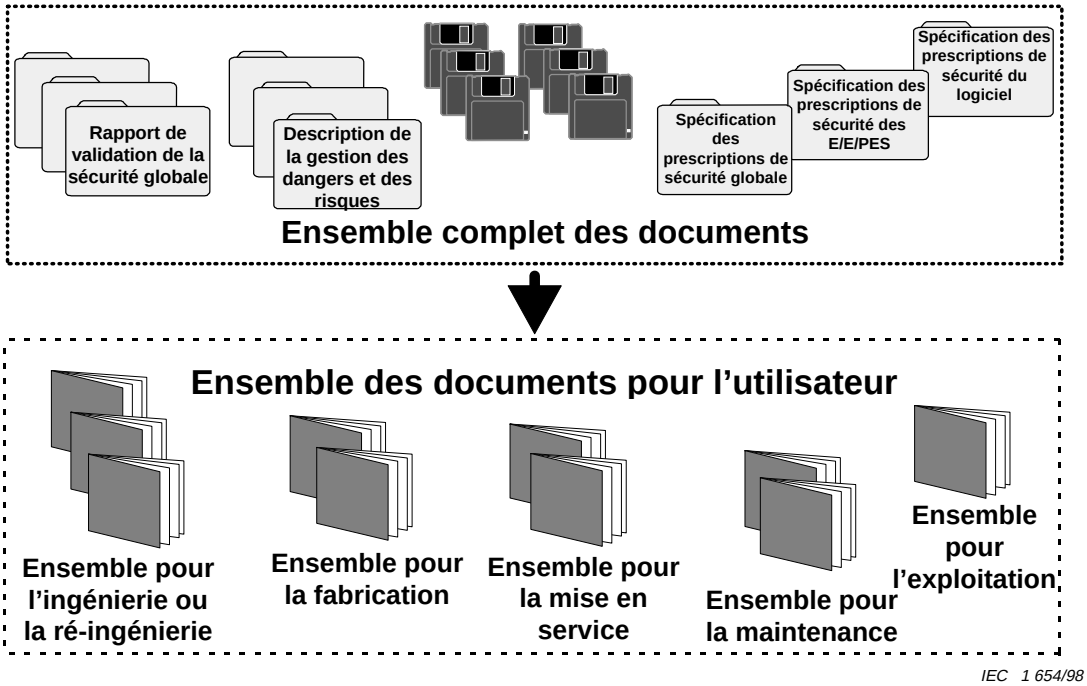


Figure A.1 – Structuration de l'information en ensembles de document pour les groupes d'utilisateurs

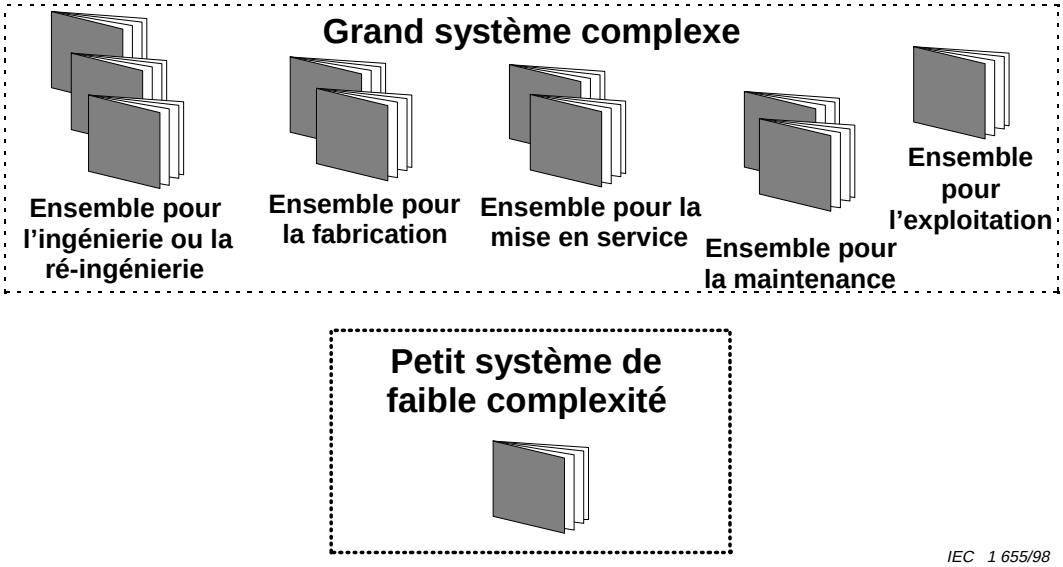


Figure A.2 – Structuration de l'information pour les grands systèmes complexes et les petits systèmes de faible complexité

NOTE – The information required by the documents in table A.1 may be contained within the different sets of documents shown in figures A.1 and A.2. For example, within the engineering set, documents such as the hazard and risk analysis description and/or overall safety requirements specification would be contained in it.

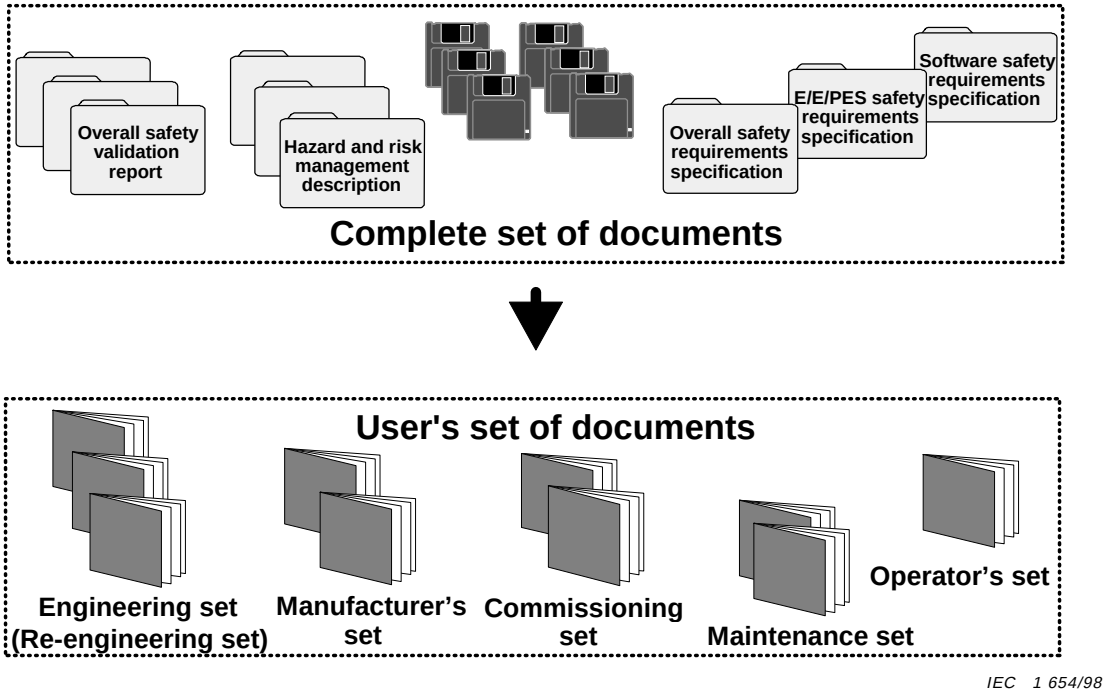


Figure A.1 – Structuring information into document sets for user groups

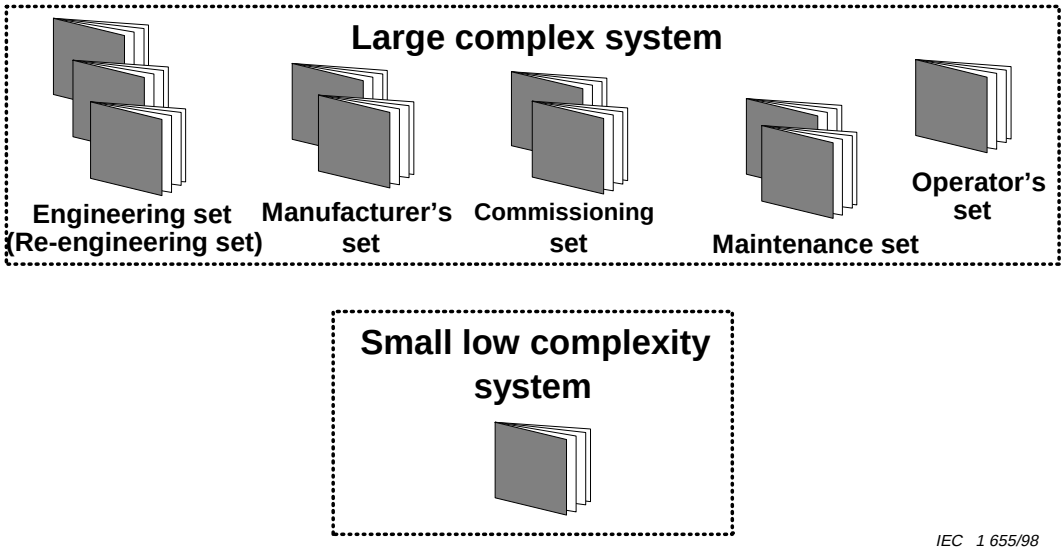


Figure A.2 – Structuring information for large complex systems and small low complexity systems

A.4 Liste des documents

La liste des documents inclura typiquement l'information suivante:

– le numéro des dessins ou documents;
– l'index de révision;
– le code de désignation du document;
– le titre;
– la date de révision;
– le support de données.

Cette liste peut prendre différents aspects, par exemple celui d'une base de données pouvant être triée selon les numéros de dessins, de document ou le code de désignation du document. Le code de désignation du document peut contenir la désignation de référence pour la fonction, la localisation ou le produit décrit dans le document, faisant de ce code un outil de recherche d'information puissant.

A.4 List of documents

The list of documents will typically include the following information:

– drawing or document number;
– revision index;
– document designation code;
– title;
– date of revision;
– data carrier.

This list may appear in different forms, for example in a database capable of being sorted according to drawing, document number or document designation code. The document designation code may contain the reference designation for the function, location or product described in the document, making it a powerful tool in searching for information.

Annexe B
(informative)

Compétence des personnes

B.1 Objectif

Cette annexe résume les points à prendre en considération pour s'assurer que les personnes qui ont des responsabilités pour toute activité du cycle de vie de sécurité global du E/E/PES ou du logiciel sont compétentes vis à vis de ces responsabilités.

B.2 Considérations générales

Il est recommandé que toutes les personnes impliquées dans toute activité du cycle de vie de sécurité global du E/E/PES ou du logiciel, y compris les activités de gestion, possèdent la formation appropriée, la connaissance technique, l'expérience et les qualifications relevant des charges spécifiques qu'elles auront à réaliser.

Il est recommandé d'évaluer la formation, l'expérience et les qualifications de toute personne impliquée dans toute activité du cycle de vie de sécurité global du E/E/PES ou du logiciel, y compris toute activité de gestion de la sécurité fonctionnelle, relative à l'application particulière.

Il convient de considérer les facteurs suivants, lors de l'évaluation de la compétence des personnes à réaliser leur travail:

a) connaissances d'ingénierie appropriées au domaine d'application;

b) connaissances d'ingénierie appropriées à la technologie (par exemple ingénierie électrique, électronique, électronique programmable, logiciel);

c) connaissances d'ingénierie de la sécurité appropriées à la technologie;

d) connaissance du cadre légal et réglementaire concernant la sécurité;

e) les conséquences dans le cas d'une défaillance des systèmes de sécurité E/E/PE; il convient d'avoir une spécification et une évaluation de compétence d'autant plus rigoureuse que les conséquences sont plus importantes;

f) les niveaux d'intégrité de sécurité des systèmes de sécurité E/E/PE; il convient d'avoir une spécification et une évaluation de compétence d'autant plus rigoureuse que les niveaux d'intégrité de sécurité sont élevés;

g) l'innovation dans la conception, les procédures de conception ou l'application; il convient d'avoir une spécification et une évaluation de compétence d'autant plus rigoureuse que la conception, les procédures de conception ou l'application, sont nouvelles ou innovatrices;

h) l'expérience accumulée et sa pertinence vis à vis des tâches spécifiques devant être réalisées et de la technologie devant être employée; il convient que les compétences acquises par l'expérience et celles exigées pour réaliser les tâches spécifiques soient d'autant plus proches que les niveaux de compétence exigés sont élevés;

i) la pertinence des qualifications vis à vis des tâches spécifiques devant être réalisées.

Il convient de documenter la formation, l'expérience et les qualifications de toute personnes impliquée dans toute activité du cycle de vie de sécurité global du E/E/PES ou du logiciel.

Annex B
(informative)

Competence of persons

B.1 Objective

This annex outlines considerations for ensuring that persons who have responsibilities for any overall, E/E/PES or software safety lifecycle activity are competent to discharge those responsibilities.

B.2 General considerations

All persons involved in any overall, E/E/PES or software safety lifecycle activity, including management activities, should have the appropriate training, technical knowledge, experience and qualifications relevant to the specific duties they have to perform.

The training, experience and qualifications of all persons involved in any overall, E/E/PES or software safety lifecycle activity, including any management of functional safety activities, should be assessed in relation to the particular application.

The following factors should be considered when assessing the competence of persons to carry out their duties:

a) engineering knowledge appropriate to the application area;

b) engineering knowledge appropriate to the technology (for example electrical, electronic, programmable electronic, software engineering);

c) safety engineering knowledge appropriate to the technology;

d) knowledge of the legal and safety regulatory framework;

e) the consequences in the event of failure of the E/E/PE safety-related systems; the greater the consequences, the more rigorous should be the specification and assessment of competence;

f) the safety integrity levels of the E/E/PE safety-related systems; the higher the safety integrity levels, the more rigorous should be the specification and assessment of competence;

g) the novelty of the design, design procedures or application; the newer or more untried the designs, design procedures or application, the more rigorous the specification and assessment of competence should be;

h) previous experience and its relevance to the specific duties to be performed and the technology being employed; the greater the required competence levels, the closer the fit should be between the competencies developed from previous experience and those required for the specific duties to be undertaken;

i) relevance of qualifications to specific duties to be performed.

The training, experience and qualifications of all persons involved in any overall, E/E/PES or software safety lifecycle activity should be documented.

Annexe C
(informative)

Bibliographie

[1] CEI 60300-3-1:1991, *Gestion de la sûreté de fonctionnement – Partie 3: Guide d'application – Section 1: Techniques d'analyse de la sûreté de fonctionnement: Guide méthodologique*

[2] CEI 60300-3-9:1995, *Gestion de la sûreté de fonctionnement – Partie 3: Guide d'application – Section 9: Analyse du risque des systèmes technologiques*

[3] CEI 61355:1997, *Classification et désignation des documents pour installations industrielles, systèmes et matériels*

[4] CEI 61506:1997, *Mesure et commande dans les processus industriels – Documentation des logiciels d'application*

[5] ISO 8613-1:1994, *Traitement de l'information – Architecture des documents ouverts (ODA) et format d'échange: Introduction et principes généraux*

[6] ISO 10007:1995, *Management de la qualité – Lignes directrices pour la gestion de configuration*

[7] ISO/CEI TR 15846, *Technologies de l'information – Procédés de cycle de vie du logiciel – Gestion de configuration pour le logiciel (en anglais seulement)*

[8] ANSI/ISA S84:1996, *Application of safety instrumented systems for the process industries*

[9] *Procedures for treating common cause failures in safety and reliability studies – Procedural framework and examples*, NUREG/CR-4780, Volume 1, January 1988

[10] *Procedures for treating common cause failures in safety and reliability studies – Analytical background and techniques*, NUREG/CR-4780, Volume 2, January 1989

_____

Annex C
(informative)

Bibliography

[1] IEC 60300-3-1:1991, *Dependability management – Part 3: Application guide – Section 1: Analysis techniques for dependability: Guide on methodology*

[2] IEC 60300-3-9:1995, *Dependability management – Part 3: Application guide – Section 9: Risk analysis of technological systems*

[3] IEC 61355:1997, *Classification and designation of documentations for plants, systems and equipment*

[4] IEC 61506:1997, *Industrial-process measurement and control – Documentation of application software*

[5] ISO 8613-1:1994, *Information technology – Open Document Architecture (ODA) and interchange format: Introduction and general principles*

[6] ISO 10007:1995, *Quality management – Guidelines for configuration management*

[7] ISO/IEC TR 15846, *Information technology – Software life cycle processes – Configuration management for software*

[8] ANSI/ISA S84:1996, *Application of safety Instrumented Systems for the Process Industries*

[9] *Procedures for treating common cause failures in safety and reliability studies – Procedural framework and examples*, NUREG/CR-4780, Volume 1, January 1988

[10] *Procedures for treating common cause failures in safety and reliability studies – Analytical background and techniques*, NUREG/CR-4780, Volume 2, January 1989

_____

Standards Survey

The IEC would like to offer you the best quality standards possible. To make sure that we continue to meet your needs, your feedback is essential. Would you please take a minute to answer the questions overleaf and fax them to us at +41 22 919 03 00 or mail them to the address below. Thank you!

Customer Service Centre (CSC)

International Electrotechnical Commission
3, rue de Varembé
1211 Genève 20
Switzerland

or

Fax to: **IEC**/CSC at +41 22 919 03 00

Thank you for your contribution to the standards-making process.

A Prioritaire

Nicht frankieren
Ne pas affranchir

Non affrancare
No stamp required

RÉPONSE PAYÉE

SUISSE

Customer Service Centre (CSC)
International Electrotechnical Commission
3, rue de Varembé
1211 GENEVA 20
Switzerland

Q1 Please report on **ONE STANDARD** and **ONE STANDARD ONLY**. Enter the exact number of the standard: *(e.g. 60601-1-1)*

.....

Q2 Please tell us in what capacity(ies) you bought the standard *(tick all that apply).* I am the/a:

purchasing agent ❑
librarian ❑
researcher ❑
design engineer ❑
safety engineer ❑
testing engineer ❑
marketing specialist ❑
other.....

Q3 I work for/in/as a: *(tick all that apply)*

manufacturing ❑
consultant ❑
government ❑
test/certification facility ❑
public utility ❑
education ❑
military ❑
other.....

Q4 This standard will be used for: *(tick all that apply)*

general reference ❑
product research ❑
product design/development ❑
specifications ❑
tenders ❑
quality assessment ❑
certification ❑
technical documentation ❑
thesis ❑
manufacturing ❑
other.....

Q5 This standard meets my needs: *(tick one)*

not at all ❑
nearly ❑
fairly well ❑
exactly ❑

Q6 If you ticked NOT AT ALL in Question 5 the reason is: *(tick all that apply)*

standard is out of date ❑
standard is incomplete ❑
standard is too academic ❑
standard is too superficial ❑
title is misleading ❑
I made the wrong choice ❑
other .....

Q7 Please assess the standard in the following categories, using the numbers:
(1) unacceptable,
(2) below average,
(3) average,
(4) above average,
(5) exceptional,
(6) not applicable

timeliness.....
quality of writing.....
technical contents.....
logic of arrangement of contents .....
tables, charts, graphs, figures.....
other .....

Q8 I read/use the: *(tick one)*

French text only ❑
English text only ❑
both English and French texts ❑

Q9 Please share any comment on any aspect of the IEC that you would like us to know:

.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

Enquête sur les normes

La CEI ambitionne de vous offrir les meilleures normes possibles. Pour nous assurer que nous continuons à répondre à votre attente, nous avons besoin de quelques renseignements de votre part. Nous vous demandons simplement de consacrer un instant pour répondre au questionnaire ci-après et de nous le retourner par fax au +41 22 919 03 00 ou par courrier à l'adresse ci-dessous. Merci !

Centre du Service Clientèle (CSC)

Commission Electrotechnique Internationale
3, rue de Varembé
1211 Genève 20
Suisse

ou

Télécopie: **CEI**/CSC +41 22 919 03 00

Nous vous remercions de la contribution que vous voudrez bien apporter ainsi à la Normalisation Internationale.

Nicht frankieren
Ne pas affranchir

Non affrancare
No stamp required

A Prioritaire

RÉPONSE PAYÉE

SUISSE

Centre du Service Clientèle (CSC)
Commission Electrotechnique Internationale
3, rue de Varembé
1211 GENÈVE 20
Suisse

Q1 Veuillez ne mentionner qu'**UNE SEULE NORME** et indiquer son numéro exact: (*ex. 60601-1-1)*

.....

Q2 En tant qu'acheteur de cette norme, quelle est votre fonction?
(cochez tout ce qui convient)
Je suis le/un:

agent d'un service d'achat ❑
bibliothécaire ❑
chercheur ❑
ingénieur concepteur ❑
ingénieur sécurité ❑
ingénieur d'essais ❑
spécialiste en marketing ❑
autre(s).....

Q3 Je travaille:
(cochez tout ce qui convient)

dans l'industrie ❑
comme consultant ❑
pour un gouvernement ❑
pour un organisme d'essais/ certification ❑
dans un service public ❑
dans l'enseignement ❑
comme militaire ❑
autre(s).....

Q4 Cette norme sera utilisée pour/comme
(cochez tout ce qui convient)

ouvrage de référence ❑
une recherche de produit ❑
une étude/développement de produit ❑
des spécifications ❑
des soumissions ❑
une évaluation de la qualité ❑
une certification ❑
une documentation technique ❑
une thèse ❑
la fabrication ❑
autre(s).....

Q5 Cette norme répond-elle à vos besoins:
(une seule réponse)

pas du tout ❑
à peu près ❑
assez bien ❑
parfaitement ❑

Q6 Si vous avez répondu PAS DU TOUT à Q5, c'est pour la/les raison(s) suivantes:
(cochez tout ce qui convient)

la norme a besoin d'être révisée ❑
la norme est incomplète ❑
la norme est trop théorique ❑
la norme est trop superficielle ❑
le titre est équivoque ❑
je n'ai pas fait le bon choix ❑
autre(s) .....

Q7 Veuillez évaluer chacun des critères ci-dessous en utilisant les chiffres
(1) inacceptable,
(2) au-dessous de la moyenne,
(3) moyen,
(4) au-dessus de la moyenne,
(5) exceptionnel,
(6) sans objet

publication en temps opportun .....
qualité de la rédaction.....
contenu technique .....
disposition logique du contenu .....
tableaux, diagrammes, graphiques, figures.....
autre(s) .....

Q8 Je lis/utilise: *(une seule réponse)*

uniquement le texte français ❑
uniquement le texte anglais ❑
les textes anglais et français ❑

Q9 Veuillez nous faire part de vos observations éventuelles sur la CEI:

.....
.....
.....
.....
.....
.....

ISBN 2-8318-4575-0

ICS 13.110; 25.040; 29.020; 35.240.50

Typeset and printed by the IEC Central Office
GENEVA, SWITZERLAND