RAPPORT TECHNIQUE

TECHNICAL REPORT

CEI
IEC
TR 61508-0

Première édition
First edition
2005-01

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

Partie 0:
La sécurité fonctionnelle et la CEI 61508

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

Part 0:
Functional safety and IEC 61508

Numéro de référence
Reference number
CEI/IEC/TR 61508-0:2005

Numérotation des publications

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

Editions consolidées

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

Informations supplémentaires sur les publications de la CEI

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

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

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

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

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

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

Publication numbering

As from 1 January 1997 all IEC publications are issued with a designation in the 60000 series. For example, IEC 34-1 is now referred to as IEC 60034-1.

Consolidated editions

The IEC is now publishing consolidated versions of its publications. 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.

Further information on IEC publications

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 this publication, including its validity, is available in the IEC Catalogue of publications (see below) in addition to new editions, amendments and corrigenda. 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 also available from the following:

- **IEC Web Site (www.iec.ch)**
- **Catalogue of IEC publications**

  The on-line catalogue on the IEC web site (www.iec.ch/searchpub) enables you to search by a variety of criteria including text searches, technical committees and date of publication. On-line information is also available on recently issued publications, withdrawn and replaced publications, as well as corrigenda.
- **IEC Just Published**

  This summary of recently issued publications (www.iec.ch/online_news/justpub) is also available by email. Please contact the Customer Service Centre (see below) for further information.
- **Customer Service Centre**

  If you have any questions regarding this publication or need further assistance, please contact the Customer Service Centre:

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

.

RAPPORT TECHNIQUE

TECHNICAL REPORT

CEI
IEC
TR 61508-0

Première édition
First edition
2005-01

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

Partie 0: La sécurité fonctionnelle et la CEI 61508

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

Part 0: Functional safety and IEC 61508

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

Commission Electrotechnique Internationale
International Electrotechnical Commission
Международная Электротехническая Комиссия

CODE PRIX
PRICE CODE Q

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

SOMMAIRE

CONTENTS

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

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

Partie 0: La sécurité fonctionnelle et la CEI 61508

AVANT-PROPOS

1) La Commission Electrotechnique Internationale (CEI) 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, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés "Publication(s) de la CEI"). 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 de la CEI intéressés sont représentés dans chaque comité d'études.
3) Les Publications de la CEI se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de la CEI. Tous les efforts raisonnables sont entrepris afin que la CEI s'assure de l'exactitude du contenu technique de ses publications; la CEI ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.
4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de la CEI s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de la CEI dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de la CEI et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
5) La CEI n'a prévu aucune procédure de marquage valant indication d'approbation et n'engage pas sa responsabilité pour les équipements déclarés conformes à une de ses Publications.
6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.
7) Aucune responsabilité ne doit être imputée à la CEI, à ses administrateurs, employés, auxiliaires ou mandataires, y compris ses experts particuliers et les membres de ses comités d'études et des Comités nationaux de la CEI, pour tout préjudice causé en cas de dommages corporels et matériels, ou de tout autre dommage de quelque nature que ce soit, directe ou indirecte, ou pour supporter les coûts (y compris les frais de justice) et les dépenses découlant de la publication ou de l'utilisation de cette Publication de la CEI ou de toute autre Publication de la CEI, ou au crédit qui lui est accordé.
8) L'attention est attirée sur les références normatives citées dans cette publication. L'utilisation de publications référencées est obligatoire pour une application correcte de la présente publication.
9) L'attention est attirée sur le fait que certains des éléments de la présente Publication de la CEI 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 tâche principale des comités d'études de la CEI est l'élaboration des Normes internationales. Toutefois, un comité d'études peut proposer la publication d'un rapport technique lorsqu'il a réuni des données de nature différente de celles qui sont normalement publiées comme Normes internationales, cela pouvant comprendre, par exemple, des informations sur l'état de la technique.

La CEI 61508-0, qui est un rapport technique, 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.

INTERNATIONAL ELECTROTECHNICAL COMMISSION

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

Part 0: Functional safety and IEC 61508

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of 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, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as “IEC Publication(s)”). 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. 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 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 IEC National Committees.
3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
5) IEC provides no marking procedure to indicate its approval and cannot be rendered responsible for any equipment declared to be in conformity with an IEC Publication.
6) All users should ensure that they have the latest edition of this publication.
7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

The main task of IEC technical committees is to prepare International Standards. However, a technical committee may propose the publication of a technical report when it has collected data of a different kind from that which is normally published as an International Standard, for example "state of the art".

IEC 61508-0, which is a technical report, has been prepared by subcommittee 65A: System Aspects, of IEC technical committee 65: Industrial-process measurement and control.

Le texte de ce rapport technique est issu des documents suivants:

Projet d'enquête	Rapport de vote
65A/413/DTR	65A/422/RVC

Le rapport de vote indiqué dans le tableau ci-dessus donne toute information sur le vote ayant abouti à l'approbation de ce rapport technique.

Cette publication a été rédigée selon les Directives ISO/CEI, Partie 2.

Les parties de cette publication, la CEI 61508, présentées sous le titre général *Sécurité fonctionnelle des systèmes électriques/électroniques/ électroniques programmables relatifs à la sécurité* sont données en 4.6.

Le comité a décidé que le contenu de cette publication ne sera pas modifié avant la date de maintenance indiquée sur le site web de la CEI sous «http://webstore.iec.ch» dans les données relatives à la publication recherchée. A cette date, la publication sera

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

The text of this technical report is based on the following documents:

Enquiry draft	Report on voting
65A/413/DTR	65A/422/RVC

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

This publication has been drafted in accordance with the ISO/IEC Directives, Part 2.

The parts of this publication, IEC 61508, under the general title *Functional safety of electrical/ electronic/programmable electronic safety-related systems* are listed in 4.6.

The committee has decided that the contents of this publication will remain unchanged until the maintenance result date indicated on the IEC web site under "http://webstore.iec.ch" in the data related to the specific publication. At this date, the publication will be

- reconfirmed;
- withdrawn;
- replaced by a revised edition, or
- amended.

INTRODUCTION

L'objet de ce rapport technique est d'introduire le concept de sécurité fonctionnelle et de donner une vue d'ensemble de la série de normes CEI 61508.

Il convient de lire ce document dans les cas suivants:

- si vous voulez savoir comment la CEI 61508 s'applique à vous,
- si vous êtes impliqués dans le développement de systèmes électriques, électroniques ou électroniques programmables qui on trait à la sécurité,
- si vous participez à l'élaboration d'autres normes pour lesquelles la sécurité fonctionnelle est un élément pertinent.

L'Article 3 de ce document donne une définition informelle de la sécurité fonctionnelle, décrit les relations entre les fonctions de sécurité, l'intégrité de sécurité et les systèmes relatifs à la sécurité, donne un exemple de comment les exigences de sécurité fonctionnelle sont déduites et liste en partie les points à surmonter pour atteindre la sécurité fonctionnelle dans les systèmes électriques, électroniques et électroniques programmables. L'Article 4 donne des détails sur la CEI 61508, qui procure une approche pour l'atteinte de la sécurité fonctionnelle. L'article décrit les objectifs de la norme, l'approche technique et la structure en différentes parties. Il explique que la CEI 61508 peut être appliquée en l'état à un large éventail d'applications industrielles et qu'elle fournit une base à beaucoup d'autres normes.

INTRODUCTION

The purpose of this Technical Report is to introduce the concept of functional safety and to give an overview of the IEC 61508 series of standards.

You should read it if you are:

- wondering whether IEC 61508 applies to you,
- involved in the development of electrical, electronic or programmable electronic systems which may have safety implications, or
- drafting any other standard where functional safety is a relevant factor.

Clause 3 of this document gives an informal definition of functional safety, describes the relationship between safety functions, safety integrity and safety-related systems, gives an example of how functional safety requirements are derived, and lists some of the challenges in achieving functional safety in electrical, electronic or programmable electronic systems. Clause 4 gives details of IEC 61508, which provides an approach for achieving functional safety. The clause describes the standard's objectives, technical approach and parts framework. It explains that IEC 61508 can be applied as is to a large range of industrial applications and yet also provides a basis for many other standards.

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

Partie 0: La sécurité fonctionnelle et la CEI 61508

1 Domaine d'application

Le présent rapport technique introduit le concept de sécurité fonctionnelle et donne une vue d'ensemble de la série CEI 61508.

2 Références normatives

Les documents de référence suivants sont indispensables pour l'application du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

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

CEI 61508-2:2000, *Sécurité 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*

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

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

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

CEI 61508-6:2000, *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 6: Lignes directrices pour l'application de la CEI 61508-2 et de la CEI 61508-3*

CEI 61508-7:2000, *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 7: Présentation de techniques et mesures*

Guide CEI 104, *Elaboration des publications de sécurité et utilisation des publications fondamentales de sécurité et publications groupées de sécurité*

Guide ISO/CEI 51, *Aspects liés à la sécurité – Principes directeurs pour les inclure dans les normes*

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

Part 0: Functional safety and IEC 61508

1 Scope

This Technical Report introduces the concept of functional safety and gives an overview of the IEC 61508 series.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 61508-1:1998, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General requirements*

IEC 61508-2:2000, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems*

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

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

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

IEC 61508-6:2000, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3*

IEC 61508-7:2000, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 7: Overview of techniques and measures*

IEC Guide 104, *The preparation of safety publications and the use of basic safety publications and group safety publications*

ISO/IEC Guide 51, *Safety aspects – Guidelines for their inclusion in standards*

3 Sécurité fonctionnelle

3.1 Qu'est ce que la sécurité fonctionnelle ?

Commençons avec la définition de la *sécurité*. C'est l'absence de tout risque de blessure physique ou pour la santé des individus, résultant directement ou indirectement de dégradation de propriétés ou de l'environnement.

La *sécurité fonctionnelle* est une partie de la sécurité au sens général, qui dépend d'un système ou d'un équipement répondant correctement aux entrées de ce dernier.

Par exemple, un dispositif de protection contre une surchauffe, utilisant un capteur thermique placé dans l'enroulement d'un moteur électrique pour désactiver le moteur avant qu'il soit en surchauffe est un exemple de dispositif de sécurité fonctionnelle. Mais un isolement spécifique dont le but est de résister à une haute température n'est pas un exemple de sécurité fonctionnelle (même s'il est du ressort de la sécurité et peut protéger contre le même danger).

Ni la sécurité, ni la sécurité fonctionnelle ne peuvent être déterminées sans prendre en considération le système en son entier et l'environnement avec lequel il interagit.

3.2 Fonctions de sécurité et systèmes relatifs à la sécurité

Généralement, les risques significatifs pour un équipement et tous ses systèmes de contrôle-commande associés dans l'environnement auquel il est destiné doivent être identifiés par les personnes qui le spécifient ou qui le développent, à l'aide d'une analyse de risque. L'analyse détermine si la sécurité fonctionnelle est nécessaire pour assurer une protection adéquate contre chaque risque significatif. S'il en est ainsi, la sécurité fonctionnelle doit être prise en compte de façon appropriée dans la conception. La sécurité fonctionnelle est une des méthodes pour traiter les risques, et d'autres moyens, tels que l'obtention de la sécurité naturellement par la conception, sont de première importance pour éliminer ou réduire les risques.

Le terme *relatif à la sécurité* est utilisé pour décrire des systèmes qui sont requis pour effectuer une (ou des) fonction spécifique pour assurer que le risque est maintenu à un niveau acceptable. De telles fonctions sont, par définition, de *sécurité fonctionnelle*. Deux types d'exigences doivent être respectées pour atteindre la sécurité fonctionnelle:

- les exigences de sécurité fonctionnelle (ce que la fonction fait), et
- *les exigences d'intégrité de sécurité* (la probabilité que la fonction de sécurité soit réalisée avec satisfaction).

Les exigences de sécurité fonctionnelle découlent de l'analyse de risque et les exigences d'intégrité de sécurité découlent de l'évaluation des risques. Plus haut est le niveau d'intégrité de sécurité, plus basse est la probabilité de défaillance dangereuse.

Tout système, quelle que soit sa technologie, qui intègre des fonctions de sécurité est un *système de sécurité*. Un système de sécurité peut être séparé de tout autre équipement de contrôle-commande ou bien le système de contrôle-commande de l'équipement peut contenir lui-même des fonctions de sécurité. Dans ce dernier cas, le système de contrôle-commande de l'équipement est un système relatif à la sécurité. Les niveaux d'intégrité de sécurité les plus élevés exigent une grande rigueur de la part de l'ingénierie du système de sécurité.

3 Functional safety

3.1 What is functional safety?

We begin with a definition of *safety*. This is freedom from unacceptable risk of physical injury or of damage to the health of people, either directly, or indirectly as a result of damage to property or to the environment.

Functional safety is part of the overall safety that depends on a system or equipment operating correctly in response to its inputs.

For example, an overtemperature protection device, using a thermal sensor in the windings of an electric motor to de-energise the motor before it can overheat, is an instance of functional safety. But providing specialised insulation to withstand high temperatures is not an instance of functional safety (although it is still an instance of safety and could protect against exactly the same hazard).

Neither safety nor functional safety can be determined without considering the systems as a whole and the environment with which they interact.

3.2 Safety functions and safety-related systems

Generally, the significant hazards for equipment and any associated control system in its intended environment have to be identified by the specifier or developer via a hazard analysis. The analysis determines whether functional safety is necessary to ensure adequate protection against each significant hazard. If so, then it has to be taken into account in an appropriate manner in the design. Functional safety is just one method of dealing with hazards, and other means for their elimination or reduction, such as inherent safety through design, are of primary importance.

The term *safety-related* is used to describe systems that are required to perform a specific function or functions to ensure risks are kept at an accepted level. Such functions are, by definition, *safety functions*. Two types of requirements are necessary to achieve functional safety:

- *safety function requirements* (what the function does) and
- *safety integrity requirements* (the likelihood of a safety function being performed satisfactorily).

The safety function requirements are derived from the hazard analysis and the safety integrity requirements are derived from a risk assessment. The higher the level of safety integrity, the lower the likelihood of dangerous failure.

Any system, implemented in any technology, which carries out safety functions is a *safety-related system*. A safety-related system may be separate from any equipment control system or the equipment control system may itself carry out safety functions. In the latter case, the equipment control system will be a safety-related system. Higher levels of safety integrity necessitate greater rigour in the engineering of the safety-related system.

3.3 Exemple de sécurité fonctionnelle

Considérons une machine avec une lame circulaire qui est protégée par un capot rigide basculant. La lame est accessible pour des nettoyages de routine par remontée du capot. Le capot est verrouillé de telle sorte que lorsqu'il est enlevé, le circuit électrique du moteur est coupé et un frein agit. Ainsi, la lame est arrêtée avant qu'elle puisse blesser un opérateur.

Une analyse de risque et une évaluation de risque sont nécessaires pour assurer que la sécurité est atteinte.

a) L'analyse de risque identifie les risques associés au nettoyage de la lame. Dans le cas de cette machine, il peut être montré qu'il convient que le capot ne puisse être relevé de plus de 5 mm avant l'activation du frein et l'arrêt de la lame. Une autre analyse peut révéler que le temps pour arrêter la lame doit être de 1 s ou moins. Ces analyses décrivent ensemble la *fonction de sécurité*.

b) L'évaluation de risque détermine les exigences de performance pour la fonction de sécurité. L'objectif est d'assurer que l'intégrité de sécurité est suffisante pour que personne ne soit exposé à un risque inacceptable lié à cet évènement dangereux.

Le préjudice résultant de la défaillance de la fonction de sécurité peut être une amputation de la main de l'opérateur ou juste une ecchymose. Le risque dépend aussi de la fréquence à laquelle le capot doit être remonté, ce qui peut être plusieurs fois par jour ou moins d'une fois par mois. Le niveau d'intégrité de sécurité requis augmente avec la sévérité du préjudice et la fréquence de l'exposition au risque.

L'intégrité de sécurité de la fonction de sécurité dépendra de tout l'équipement qui est nécessaire à la réalisation correcte de la fonction de sécurité, c'est-à-dire le verrou et son circuit électrique associé, le moteur et le système de freinage. La fonction de sécurité et son intégrité de sécurité spécifient les comportements requis pour les systèmes considérés en leur intégralité dans un environnement particulier.

Pour résumer, l'analyse de risque identifie ce qui doit être fait pour éviter les évènements dangereux associés à la lame. L'évaluation de risque donne l'intégrité de sécurité requise pour le système de verrouillage pour que le risque devienne acceptable. Ces deux éléments, "Quelle fonction de sécurité doit être réalisée ?" – les exigences de la fonction de sécurité – et "Quel degré de certitude est nécessaire pour que la fonction de sécurité soit réalisée ?" – les exigences d'intégrité de sécurité – sont les fondements de la sécurité fonctionnelle.

3.4 Défis rencontrés dans l'atteinte de la sécurité fonctionnelle

Les fonctions de sécurité sont de plus en plus réalisées par des systèmes électriques, électroniques ou électroniques programmables. Ces systèmes sont habituellement complexes, ce qui rend impossible en pratique de déterminer complètement chaque mode de défaillance ou de tester tous les comportements possibles. Il est difficile de prédire la performance de la fonction de sécurité, bien que le test demeure essentiel.

Le défi est de concevoir le système de telle sorte que toutes les défaillances dangereuses soient écartées ou maintenues sous contrôle si elles apparaissent.

Des défaillances dangereuses peuvent survenir du fait de:

- spécifications incorrectes du système, matériel ou logiciel;
- omissions d'exigences de sécurité dans les spécifications (par exemple, défaillance dans le développement de fonctions de sécurité pertinentes dans différents modes opératoires);
- mécanismes de défaillance aléatoire de matériel;
- mécanismes de défaillance systématique de matériel;
- erreur logicielle;

3.3 Example of functional safety

Consider a machine with a rotating blade that is protected by a hinged solid cover. The blade is accessed for routine cleaning by lifting the cover. The cover is interlocked so that whenever it is lifted an electrical circuit de-energises the motor and applies a brake. In this way, the blade is stopped before it could injure the operator.

In order to ensure that safety is achieved, both hazard analysis and risk assessment are necessary.

a) The *hazard analysis* identifies the hazards associated with cleaning the blade. For this machine it might show that it should not be possible to lift the hinged cover more than 5 mm without the brake activating and stopping the blade. Further analysis could reveal that the time for the blade to stop shall be 1 s or less. Together, these describe the *safety function*.

b) The *risk assessment* determines the performance requirements of the safety function. The aim is to ensure that the *safety integrity* of the safety function is sufficient to ensure that no one is exposed to an unacceptable risk associated with this hazardous event.

The harm resulting from a failure of the safety function could be amputation of the operator's hand or could be just a bruise. The risk also depends on how frequently the cover has to be lifted, which might be many times during daily operation or might be less than once a month. The level of safety integrity required increases with the severity of injury and the frequency of exposure to the hazard.

The safety integrity of the safety function will depend on all the equipment that is necessary for the safety function to be carried out correctly, i.e. the interlock, the associated electrical circuit and the motor and braking system. Both the safety function and its safety integrity specify the required behaviour for the systems as a whole within a particular environment.

To summarise, the hazard analysis identifies what has to be done to avoid the hazardous event, or events, associated with the blade. The risk assessment gives the safety integrity required of the interlocking system for the risk to be acceptable. These two elements, "What safety function has to be performed?" – the *safety function requirements* – and "What degree of certainty is necessary that the safety function will be carried out?" – the *safety integrity requirements* – are the foundations of functional safety.

3.4 Challenges in achieving functional safety

Safety functions are increasingly being carried out by electrical, electronic or programmable electronic systems. These systems are usually complex, making it impossible in practice to fully determine every failure mode or to test all possible behaviour. It is difficult to predict the safety performance, although testing is still essential.

The challenge is to design the system in such a way as to prevent dangerous failures or to control them when they arise. Dangerous failures may arise from

- incorrect specifications of the system, hardware or software;
- omissions in the safety requirements specification (e.g. failure to develop all relevant safety functions during different modes of operation);
- random hardware failure mechanisms;
- systematic hardware failure mechanisms;
- software errors;
- common cause failures;

- défaillances de cause commune;
- erreur humaine;
- influences environnementales (par exemple phénomènes électromagnétiques, thermiques ou mécaniques);
- perturbations du système d'alimentation en tension (par exemple, pertes, tensions réduites, reconnexion d'alimentation).

La CEI 61508 expose des exigences pour réduire ces défaillances et elle est décrite dans l'article suivant.

4 La CEI 61508 – Sécurité fonctionnelle des systèmes E/E/PE relatifs à la sécurité

4.1 Objectifs

La CEI 61508 a pour but de:

- permettre l'utilisation du potentiel des technologies E/E/PE pour améliorer à la fois la sécurité et son coût;
- permettre aux développements technologiques de participer à la structure globale de la sécurité;
- apporter une assise technique, une approche système, avec suffisamment de souplesse pour le futur;
- apporter une approche fondée sur le risque pour déterminer la performance requise pour le système de sécurité;
- fournir une norme générale qui peut être utilisée directement par l'industrie mais qui peut aussi aider à développer d'autres normes sectorielles (par exemple pour les machines, les usines de productions chimiques, le médical ou le ferroviaire) ou des normes produits (par exemple les systèmes de conduite de puissance);
- apporter aux utilisateurs et aux législateurs un moyen d'accroître leur confiance dans l'utilisation des technologies basées sur l'informatique;
- énoncer des exigences fondées sur des principes communs sous-jacents afin de faciliter:
  - — l'efficacité de la chaîne d'approvisionnement pour les fournisseurs de sous-systèmes et de composants de secteurs différents,
  - — la compréhension des exigences (c'est-à-dire de clarifier ce qui doit être spécifié),
  - — le développement de techniques et de mesures utilisables quels que soient les secteurs, en augmentant les ressources utilisables,
  - — le développement des services d'évaluation de la conformité, si nécessaire.

La CEI 61508 ne couvre pas le domaine des précautions qui peuvent être nécessaires pour que des personnes non qualifiées ne puissent détériorer et/ou affecter la sécurité fonctionnelle réalisée par les systèmes E/E/PE relatifs à la sécurité.

4.2 Systèmes E/E/PE relatifs à la sécurité

La CEI 61508 s'applique à la sécurité fonctionnelle, atteinte par des systèmes de sécurité qui sont principalement basés sur des technologies électriques et/ou électronique et/ou électroniques programmables (E/E/PE), c'est-à-dire les systèmes E/E/PE relatifs à la sécurité. La norme est générique en cela qu'elle s'applique à tous ces systèmes quelle que soit leur application.

- human error;
- environmental influences (e.g. electromagnetic, temperature, mechanical phenomena);
- supply system voltage disturbances (e.g. loss of supply, reduced voltages, re-connection of supply).

IEC 61508 contains requirements to minimise these failures and is described in the next clause.

4 IEC 61508 – Functional safety of E/E/PE safety-related systems

4.1 Objectives

IEC 61508 aims to

- release the potential of E/E/PE technology to improve both safety and economic performance;
- enable technological developments to take place within an overall safety framework;
- provide a technically sound, system based approach, with sufficient flexibility for the future;
- provide a risk-based approach for determining the required performance of safety-related systems;
- provide a generically-based standard that can be used directly by industry but can also help with developing sector standards (e.g. machinery, process chemical plants, medical or rail) or product standards (e.g. power drive systems);
- provide a means for users and regulators to gain confidence when using computer-based technology;
- provide requirements based on common underlying principles to facilitate:
  - — improved efficiencies in the supply chain for suppliers of subsystems and components to various sectors,
  - — improvements in communication and requirements (i.e. to increase clarity of what needs to be specified),
  - — the development of techniques and measures that could be used across all sectors, increasing available resources,
  - — the development of conformity assessment services if required.

IEC 61508 does not cover the precautions that may be necessary to prevent unauthorized persons damaging, and/or otherwise adversely affecting, the functional safety achieved by E/E/PE safety-related systems.

4.2 E/E/PE safety-related systems

IEC 61508 is concerned with functional safety, achieved by safety-related systems that are primarily implemented in electrical and/or electronic and/or programmable electronic (E/E/PE) technologies, i.e. E/E/PE safety related systems. The standard is generic in that it applies to these systems irrespective of their application.

Certaines exigences de la norme relèvent des activités de développement pour lesquelles les choix technologiques ne sont pas encore décidés. Ceci inclut le développement des exigences de la sécurité dans son ensemble (concept, définition du domaine, analyse de risque et évaluation de risque). S'il y a l'éventualité d'utilisation de technologies E/E/PE, il convient que la norme soit appliquée de telle sorte que les exigences de sécurité fonctionnelle pour tout système E/E/PE relatif à la sécurité soient déterminées méthodologiquement et basées sur le risque.

D'autre exigences de la norme ne sont pas seulement spécifiques aux technologies E/E/PE; elle s'appliquent à la documentation, à la gestion de la sécurité fonctionnelle, à l'évaluation de la sécurité fonctionnelle et aux compétences. Toutes les exigences qui ne sont pas spécifiques à la technologie peuvent être utiles pour d'autres systèmes de sécurité même si ces systèmes de sont pas du domaine d'application de la norme.

Les exemples ci-dessous sont des systèmes E/E/PE relatifs à la sécurité:

- systèmes d'arrêt d'urgence dans les usines chimiques à risque;
- indicateur de charge de sécurité d'une grue;
- système de signalisation ferroviaire;
- systèmes de verrouillage et d'arrêt d'urgence de machinerie;
- moteur à vitesse variable utilisé pour réduire la vitesse au titre de moyen de protection;
- systèmes de verrouillage et de contrôle de l'exposition pour un appareil médical de radiothérapie;
- positionnement dynamique (contrôle des mouvements d'un bateau à proximité d'une installation offshore);
- commande de vol électrique d'un avion;
- indicateurs lumineux d'une automobile, freinage anti-blocage, et système de gestion du moteur;
- surveillance à distance, opérations de programmation d'un procédé d'usine par réseau;
- un outil d'aide à la décision dont des résultats erronés affectent la sécurité.

Un système E/E/PE relatif à la sécurité couvre toutes les parties du système qui sont nécessaires pour réaliser la fonction de sécurité (c'est-à-dire du capteur à l'actionneur en passant par la logique de contrôle-commande et les systèmes de communication, en incluant toutes les actions critiques de l'intervention humaine).

Puisque la définition du système E/E/PE relatif à la sécurité découle de la définition de la sécurité, elle concerne aussi l'absence de risques inacceptables de blessure physique et de dommage pour la santé des individus. Le préjudice peut survenir indirectement comme résultat d'un dommage porté à la propriété ou à l'environnement. Cependant, certains systèmes peuvent être initialement conçus contre les défaillances au prix d'une forte implication économique. La CEI 61508 peut être utilisée pour développer tout système E/E/PE ayant des fonctions critiques, telles que la protection d'équipements ou de produits.

4.3 Approche technique

La CEI 61508:

- utilise une approche basée sur le risque pour déterminer les exigences d'intégrité de sécurité des systèmes E/E/PE relatifs à la sécurité, et inclut des exemples montrant comment cela peut être réalisé;
- utilise un modèle de cycle de vie de la sécurité globale comme architecture technique pour les activités nécessaires pour assurer que la sécurité fonctionnelle est atteinte par les systèmes E/E/PE relatifs à la sécurité;

Some requirements of the standard relate to development activities where the implementation technology may not yet have been fully decided. This includes development of the overall safety requirements (concept, scope definition, hazard analysis and risk assessment). If there is a possibility that E/E/PE technologies might be used, the standard should be applied so that the functional safety requirements for any E/E/PE safety-related systems are determined in a methodical, risk-based manner.

Other requirements of the standard are not solely specific to E/E/PE technology, including documentation, management of functional safety, functional safety assessment and competence. All requirements that are not technology-specific might usefully be applied to other safety-related systems although these systems are not within the scope of the standard.

The following are examples of E/E/PE safety-related systems:

- emergency shut-down system in a hazardous chemical process plant;
- crane safe load indicator;
- railway signalling system;
- guard interlocking and emergency stopping systems for machinery;
- variable speed motor drive used to restrict speed as a means of protection;
- system for interlocking and controlling the exposure dose of a medical radiotherapy machine;
- dynamic positioning (control of a ship's movement when in proximity to an offshore installation);
- fly-by-wire operation of aircraft flight control surfaces;
- automobile indicator lights, anti-lock braking and engine-management systems;
- remote monitoring, operation or programming of a network-enabled process plant;
- an information-based decision support tool where erroneous results affect safety.

An E/E/PE safety-related system covers all parts of the system that are necessary to carry out the safety function (i.e. from sensor, through control logic and communication systems, to final actuator, including any critical actions of a human operator).
Since the definition of E/E/PE safety-related system is derived from the definition of safety, it also concerns freedom from unacceptable risk of both physical injury and damage to the health of people. The harm can arise indirectly as a result of damage to property or the environment. However, some systems will be designed primarily to protect against failures with serious economic implications. IEC 61508 can be used to develop any E/E/PE system that has critical functions, such as the protection of equipment or products.

4.3 Technical approach

IEC 61508

- uses a risk based approach to determine the safety integrity requirements of E/E/PE safety-related systems, and includes a number of examples of how this can be done;
- uses an overall safety lifecycle model as the technical framework for the activities necessary for ensuring functional safety is achieved by the E/E/PE safety-related systems;

- couvre les activités de sécurité tout au long du cycle de vie, dès le concept initial jusqu'au démantèlement en passant par l'analyse de risque et l'évaluation du risque, le développement des exigences de sécurité fonctionnelle, la spécification, la conception et la réalisation, le fonctionnement et la maintenance et les modifications;
- embrasse les aspects systèmes (incluant tous les sous-systèmes intervenant dans les fonctions de sécurité, matériel et logiciel) et les mécanismes de défaillance (défaillances systématiques et matériels aléatoires);
- contient les exigences pour la prévention des défaillances (évitant l'introduction de pannes) et les exigences pour maîtriser les défaillances (assurer la sécurité même si des pannes sont présentes);
- spécifie les techniques et les mesures qui sont nécessaires pour atteindre l'intégrité de sécurité requise.

4.4 Niveaux d'intégrité de sécurité

La CEI 61508 spécifie 4 niveaux de performance de sécurité pour une fonction de sécurité. Ils sont appelés niveaux d'intégrité de sécurité. Le niveau 1 d'intégrité de sécurité (SIL 1) est le niveau le plus bas et le niveau d'intégrité 4 (SIL 4) est le plus élevé. La norme détaille les exigences pour atteindre chaque niveau d'intégrité de sécurité. Ces exigences sont plus rigoureuses pour les niveaux élevés d'intégrité de sécurité de telle sorte que la probabilité de défaillance dangereuse soit la plus basse.

Un système E/E/PE relatif à la sécurité réalisera le plus souvent plus d'une fonction de sécurité. Si les exigences d'intégrité de sécurité pour ces fonctions de sécurité sont différentes, et à moins qu'il y ait une indépendance suffisante entre elles, les exigences applicables au niveau d'intégrité le plus élevé sont applicables à tout le système E/E/PE relatif à la sécurité.

Si un seul système E/E/PE est capable de répondre à toutes les fonctions de sécurité requises, et si le niveau d'intégrité de sécurité est inférieur au niveau SIL 1, la CEI 61508 ne s'applique pas.

4.5 Exemple de sécurité fonctionnelle revisitée

Les exigences de sécurité fonctionnelle et les exigences d'intégrité de sécurité constituent la spécification des exigences de sécurité fonctionnelle. Ces exigences doivent être complètement déterminées avant d'entreprendre la conception du système E/E/PE relatif à la sécurité.

Dans l'exemple décrit dans l'Article 3, les exigences de sécurité fonctionnelle pour l'événement dangereux particulier peuvent être énoncées comme suit.

> Quand le couvercle basculant est soulevé de 5 mm ou plus, le moteur doit être désactivé et le frein doit être activé de telle sorte que la lame soit arrêtée dans la seconde. Le niveau d'intégrité de sécurité de cette fonction de sécurité doit être SIL2.

La spécification des exigences de la fonction de sécurité concerne le comportement du système E/E/PE relatif à la sécurité en son entier, dans un environnement particulier. Dans cet exemple le système E/E/PE relatif à la sécurité inclut un commutateur de verrouillage, le circuit électrique, des contacts, le moteur et le frein.

- covers all safety lifecycle activities from initial concept, through hazard analysis and risk assessment, development of the safety requirements, specification, design and implementation, operation and maintenance, and modification, to final decommissioning and/or disposal;
- encompasses system aspects (comprising all the subsystems carrying out the safety functions, including hardware and software) and failure mechanisms (random hardware and systematic);
- contains both requirements for preventing failures (avoiding the introduction of faults) and requirements for controlling failures (ensuring safety even when faults are present);
- specifies the techniques and measures that are necessary to achieve the required safety integrity.

4.4 Safety integrity levels

IEC 61508 specifies 4 levels of safety performance for a safety function. These are called safety integrity levels. Safety integrity level 1 (SIL1) is the lowest level of safety integrity and safety integrity level 4 (SIL4) is the highest level. The standard details the requirements necessary to achieve each safety integrity level. These requirements are more rigorous at higher levels of safety integrity in order to achieve the required lower likelihood of dangerous failure.

An E/E/PE safety-related system will usually implement more than one safety function. If the safety integrity requirements for these safety functions differ, unless there is sufficient independence of implementation between them, the requirements applicable to the highest relevant safety integrity level shall apply to the entire E/E/PE safety-related system.

If a single E/E/PE system is capable of providing all the required safety functions, and the required safety integrity is less than that specified for SIL1, then IEC 61508 does not apply.

4.5 Example of functional safety revisited

The safety function requirements and the safety integrity requirements constitute the functional safety requirements specification. These requirements must be fully determined before designing the E/E/PE safety-related system.

In the example described in Clause 3, the functional safety requirements for the specific hazardous event could be stated as follows.

> When the hinged cover is lifted by 5 mm or more, the motor shall be de-energised and the brake activated so that the blade is stopped within 1 s. The safety integrity level of this safety function shall be SIL2.

The functional safety requirements specification concerns behaviour of the safety-related system as a whole, within a particular environment. In this example, the E/E/PE safety-related system includes the guard interlock switch, the electrical circuit, contactors, the motor and the brake.

4.6 Structure de la CEI 61508

La CEI 61508 comprend les parties suivantes, présentées sous le titre général *Sécurité fonctionnelle des systèmes électriques/ électroniques/électroniques programmables relatifs à la sécurité*:

Partie 0: La sécurité fonctionnelle et la CEI 61508

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 de détermination des niveaux d'intégrité de sécurité

Partie 6: Lignes directrices pour l'application de la CEI 61508-2 et de la CEI 61508-3

Partie 7: Présentation de techniques et mesures

Une carte des exigences est donnée en Figure 1.

4.6 Parts framework of IEC 61508

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

Part 0: Functional safety and IEC 61508

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 measures and techniques

A requirements map is shown in Figure 1.

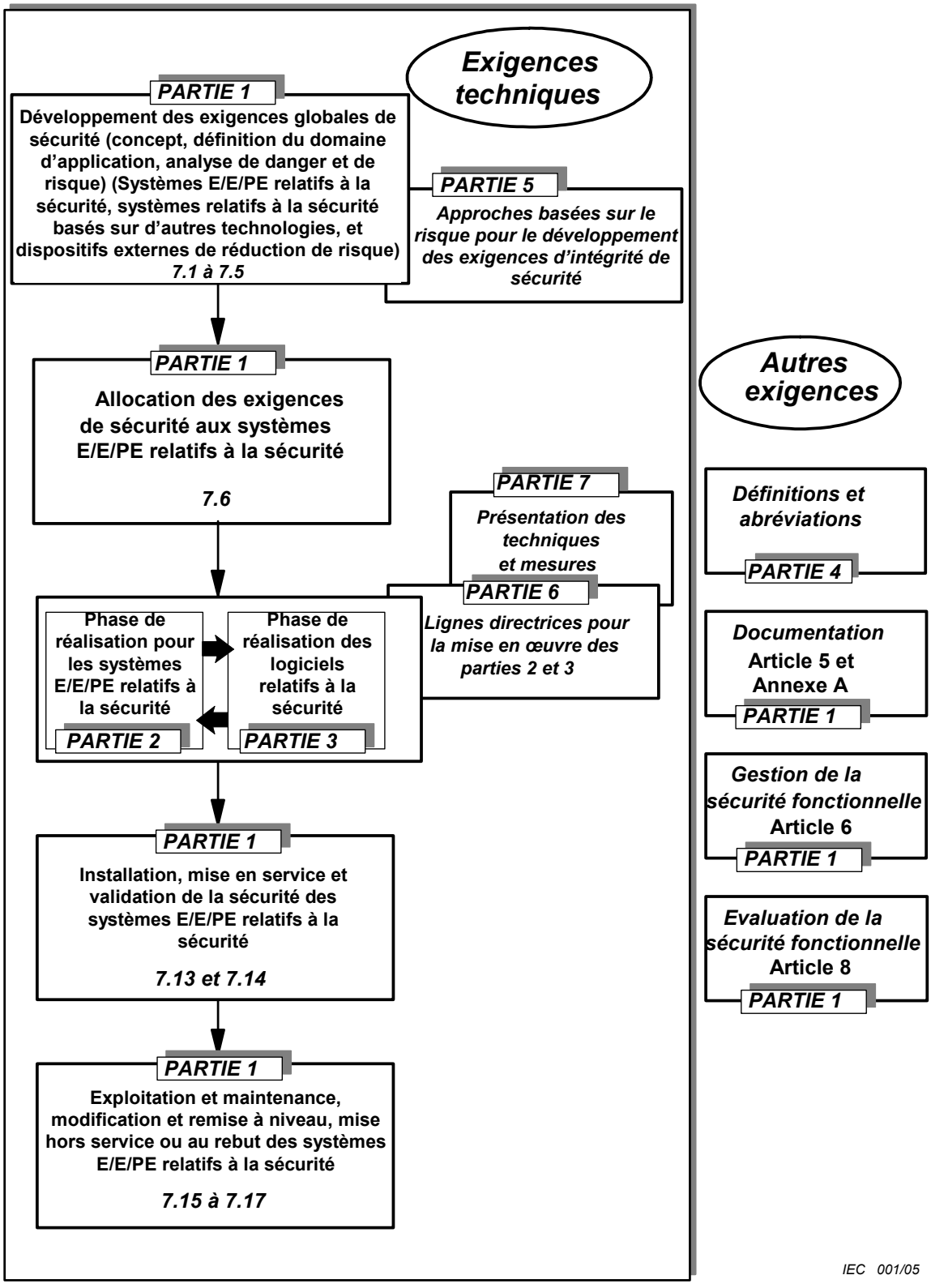

Figure 1 – Carte des exigences pour les parties 1 à 7 de la CEI 61508

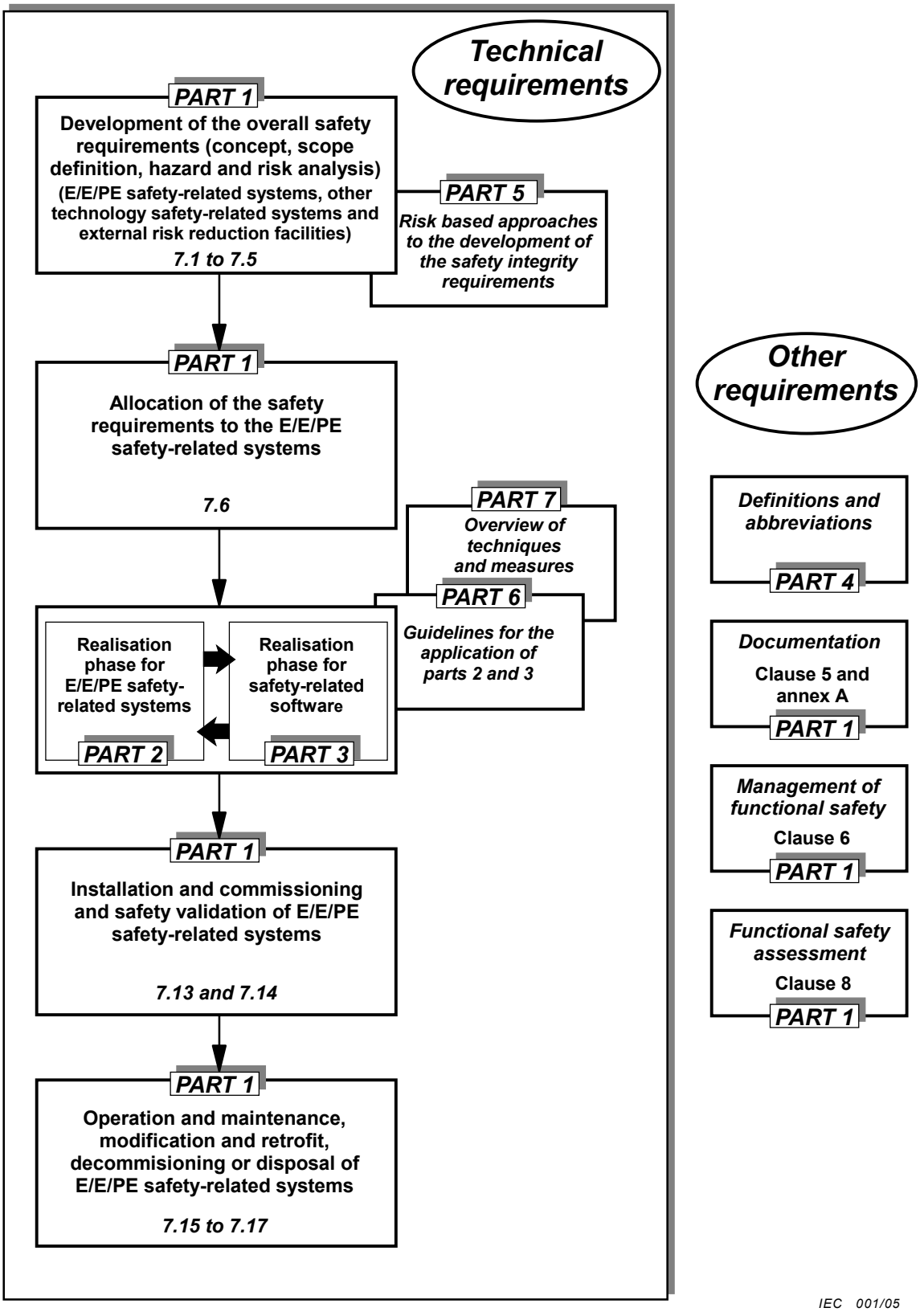

Figure 1 – Requirements map for parts 1 to 7 of IEC 61508

4.7 La CEI 61508, base pour d'autres normes

Les rédacteurs de normes ont besoin de traiter de la sécurité fonctionnelle dans leurs normes de sécurité si l'analyse de risque menée par le comité d'études en établit la nécessité pour la protection adéquate contre des risques significatifs ou des évènements dangereux.

Les parties 1 à 4 de la CEI 61508 sont des publications CEI fondamentales de sécurité. L'une des responsabilités des comités d'études de la CEI est, quand c'est possible, d'utiliser ces parties de la CEI 61508 dans la préparations de leurs propres normes sectorielles ou normes produits qui traitent des systèmes E/E/PE relatifs à la sécurité dans leur domaine d'application. Pour plus de détails, voir le Guide 104 de la CEI et le Guide ISO/CEI 51.

La CEI 61508 est la base pour les normes sectorielles publiées (par exemple pour le secteur des procédés). Elle est aussi couramment utilisée pour le développement d'autres normes sectorielles ou normes produits. Elle a donc une incidence sur le développement des systèmes E/E/PE relatifs à la sécurité et des produits quel que soit leur secteur.

Les normes sectorielles spécifiques basées sur la CEI 61508:

- sont destinées aux concepteurs de systèmes, aux intégrateurs de systèmes et aux utilisateurs;
- prennent en compte les pratiques spécifiques au secteur, qui peuvent autoriser des exigences moins complexes;
- utilisent la terminologie propre au secteur pour gagner en clarté;
- peuvent spécifier des contraintes particulières appropriées au secteur;
- le plus souvent donnent le lien avec les exigences de la CEI 61508 pour des conceptions détaillées de sous-systèmes;
- peuvent permettre à l'utilisateur final d'atteindre la sécurité fonctionnelle sans avoir à considérer la CEI 61508 elle-même.

Le statut de publication fondamentale de sécurité de la CEI 61508 décrit ci-dessus ne s'applique pas aux systèmes E/E/PE relatifs à la sécurité et de faible complexité (voir 4.2 de la CEI 61508-1). Il y a des systèmes E/E/PE relatifs à la sécurité dont les modes de défaillances des composants sont bien définis et le comportement de ces systèmes dans des conditions de panne peut être complètement déterminé: par exemple, un système comprenant un ou plusieurs commutateurs activant un ou plusieurs contacts pour désactiver un moteur électrique, éventuellement avec des relais électromécaniques.

4.8 La CEI 61508 comme norme autonome

Toutes les parties de la CEI 61508 peuvent être directement utilisées par l'industrie comme des publications autonomes. Ceci inclut l'utilisation de la norme:

- comme un ensemble d'exigences générales pour les systèmes E/E/PE relatifs à la sécurité pour lesquels l'application de normes sectorielles ou de normes produit est inexistante ou inappropriée;
- par des fournisseurs de composants ou de sous-systèmes E/E/PE pour une utilisation dans tous les secteurs (par exemple, des matériels et des logiciels pour des détecteurs, des petits actionneurs, des contrôleurs programmables, la communication de données);
- par les constructeurs de système pour respecter les spécifications des utilisateurs de systèmes E/E/PE relatifs à la sécurité;
- par les utilisateurs pour spécifier des exigences en termes de sécurité fonctionnelle ainsi que les exigences de performance de ces fonctions de sécurité;

4.7 IEC 61508 as a basis for other standards

Standards writers need to address functional safety in their safety standard if the hazard analysis carried out by a Technical Committee identifies that this is necessary to adequately protect against a significant hazard or hazardous event.

Parts 1, 2, 3 and 4 of IEC 61508 are *IEC basic safety publications*. One of the responsibilities of IEC Technical Committees is, wherever practicable, to make use of these parts of IEC 61508 in the preparation of their own sector or product standards that have E/E/PE safety-related systems within their scope. For more details see *IEC Guide 104* and *ISO/IEC Guide 51*.

IEC 61508 is the basis for published sector standards (e.g. process sector). It is also currently being used as a basis for developing other sector standards and product standards. It is therefore influencing the development of E/E/PE safety-related systems and products across all sectors.

Sector specific standards based on IEC 61508:

- are aimed at system designers, system integrators and users;
- take account of specific sector practice, which can allow less complex requirements;
- use sector terminology to increase clarity;
- may specify particular constraints appropriate for the sector;
- usually rely on the requirements of IEC 61508 for detailed design of subsystems;
- may allow end users to achieve functional safety without having to consider IEC 61508 themselves.

The basic safety publication status of IEC 61508 described above does not apply for low complexity E/E/PE safety-related systems (see 4.2 of IEC 61508-1). These are E/E/PE safety-related systems in which the failure modes of each individual component are well-defined and the behaviour of the system under fault conditions can be completely determined. An example is a system comprising one or more limit switches, operating one or more contactors to de-energize an electric motor, possibly via interposing electromechanical relays.

4.8 IEC 61508 as a stand-alone standard

All parts of IEC 61508 can be used directly by industry as “stand-alone” publications. This includes use of the standard:

- as a set of general requirements for E/E/PE safety-related systems where no application sector or product standards exist or where they are not appropriate;
- by suppliers of E/E/PE components and subsystems for use in all sectors (e.g. hardware and software of sensors, smart actuators, programmable controllers, data communication);
- by system builders to meet user specifications for E/E/PE safety-related systems;
- by users to specify requirements in terms of the safety functions to be performed together with the performance requirements of those safety functions;

- pour faciliter le maintien de l'intégrité fonctionnelle "telle qu'à la conception" de systèmes E/E/PE relatifs à la sécurité;
- pour apporter un cadre technique à l'évaluation de la conformité et aux services de certification;
- comme base pour mener les évaluations des activités du cycle de vie de la sécurité.

4.9 Autres informations

D'autres informations sur la CEI 61508 et sur la sécurité fonctionnelle, incluant un nombre important de questions fréquentes (voir Annexe A) sont disponibles dans la zone "sécurité fonctionnelle" du site CEI (http://www.iec.ch/functionalsafety).

Si vous disposez d'un exemplaire de la norme et que vous n'êtes pas familiarisé avec son contenu, il peut être utile de lire tout d'abord les articles suivants:

- L'Annexe A de la CEI 61508-5, qui introduit les concepts de risque et de sécurité fonctionnelle.
- La Figure 2 et le Tableau 1 de la CEI 61508-1, qui illustrent l'ensemble du cycle de vie de la sécurité et listent les objectifs de chaque phase du cycle de vie. Les objectifs du cycle de vie et des phases fournissent une clé pour comprendre les exigences de l'Article 7 de la CEI 61508-1.
- Les Articles 6 et 8 de la CEI 61805-1, qui exposent les exigences relatives à la gestion de la sécurité fonctionnelle et à l'évaluation de la sécurité fonctionnelle.
- L'Annexe A de la CEI 61508-6 qui donne en 8 pages, une vue générale des exigences incluses dans la CEI 61508-2 et la CEI 61508-3.
- La Figure 2 et le Tableau 1 de la CEI 61580-2 et la Figure 3 et le Tableau 1 de la CEI 61508-3, qui fournissent une clé pour comprendre respectivement les exigences de l'Article 7 de la CEI 61508-2 et de la CEI 61508-3.

Il convient que toute exigence particulière de la CEI 61508 soit considérée dans le contexte de sa phase du cycle de vie (si applicable) et des objectifs établis pour les exigences de la phase, article ou paragraphe. Les objectifs sont toujours donnés immédiatement avant les exigences.

- to facilitate the maintenance of the "as designed" safety integrity of E/E/PE safety-related systems;
- to provide the technical framework for conformity assessment and certification services;
- as a basis for carrying out assessments of safety lifecycle activities.

4.9 Further information

Further information on IEC 61508 and functional safety, including an extensive set of frequently asked questions (see Annex A), can be found in the “functional safety” zone of the IEC web site (http://www.iec.ch/functionalsafety).

If you have a copy of the standard but are not familiar with its contents, you may find it helpful to read the following sections first:

- Annex A of IEC 61508-5, which introduces risk concepts and safety integrity.
- Figure 2 and Table 1 of IEC 61508-1, which illustrate the overall safety lifecycle and list the objectives of each lifecycle phase. The lifecycle and phase objectives provide a key to understanding the requirements of Clause 7 of IEC 61508-1.
- Clauses 6 and 8 of IEC 61508-1, which contain requirements relating to management of functional safety and functional safety assessment.
- Annex A of IEC 61508-6, which gives an eight-page overview of the requirements in IEC 61508-2 and IEC 61508-3.
- Figure 2 and Table 1 of IEC 61508-2 and Figure 3 and Table 1 of IEC 61508-3, which provide a key to understanding the requirements of Clause 7 of IEC 61508-2 and IEC 61508-3 respectively.

Any particular requirement of IEC 61508 should be considered in the context of its lifecycle phase (where applicable) and the stated objectives for the requirements of that phase, clause or subclause. The objectives are always stated immediately before the requirements.

Annexe A
(informative)

Liste de questions fréquemment posées, tirée de la zone « sécurité fonctionnelle » du site de la CEI

Le Tableau A.1 liste des questions fréquemment posées et auxquelles une réponse est apportée dans la zone «sécurité fonctionnelle» du site CEI (http://www.iec.ch/functionalsafety). D'autres questions peuvent avoir été ajoutées depuis la publication de cette liste.

Tableau A.1 – Liste des questions fréquemment posées

Section	Questions fréquemment posées
Domaine d'application	La CEI 61508 est-elle pertinente pour mon cas?
	Quels sont les systèmes couverts par la CEI 61508?
	Donnez-moi quelques exemples pratiques
	Comment s'applique la CEI 61508 aux technologies E/E/PE constituant une petite partie du système relatif à la sécurité?
	Comment s'applique la CEI 61508 aux systèmes dont la fonction est d'éviter les préjudices à l'environnement ou de lourdes pertes financières?
	En quoi consiste la CEI 61508?
	Puis-je obtenir gratuitement la norme, par exemple à partir de l'Internet?
	Maintenant que j'ai acquis un exemplaire de la norme, comment dois-je m'y prendre pour la lire?
Position dans la structure normative internationale	Comment sera publiée la norme au plan international?
	Quelle est le statut international de la CEI 61508 ?
	Comment s'articule la CEI 61508 avec l'application des normes sectorielles ?
	Qu'est-ce qu'une publication fondamentales de sécurité ?
	Quelles sont les normes sectorielles ou de sous-systèmes basées sur la CEI 61508 ?
	Comment convertir ou relier les niveaux d'intégrité de sécurité 1 à 4 de la CEI 61508 aux catégories de l'EN 954-1?
	Puis-je utiliser la CEI 61508 comme une norme autonome?
	Est-ce que la CEI 61508 sera révisée?
	Puis-je soumettre un commentaire pour le processus de révision ?
Aspects régionaux et interprétation technique	Comment puis-je trouver une information sur la CEI 61508, spécifique à mon pays ?
	Est-ce que la CEI 61508 est aussi une norme européenne ?
	Est-ce que la CEI 61508 est d'application obligatoire du fait d'une Directive Européenne?
	Comment puis-je demander une interprétation technique pour un paragraphe particulier de la norme?
	Comment puis-je contacter mon comité national ?

Annex A
(informative)

List of frequently asked questions from IEC “functional safety” zone

Table A.1 lists, frequently asked questions that are answered in the “functional safety” zone of the IEC web site (http://www.iec.ch/functionalsafety). Other questions may have been added since this list was published.

Table A.1 – List of frequently asked questions

Section	Frequently asked questions
Scope	Is IEC 61508 relevant to me?
	What systems does IEC 61508 cover?
	Give me some practical examples
	How does IEC 61058 apply where E/E/PE technology makes up only a small part of the safety-related system?
	How does IEC 61508 apply to systems whose function is to avoid damage to the environment or severe financial loss?
	What does IEC 61508 consist of?
	Can I get hold of the standard for free, for example by downloading from the Internet?
	Now I’ve obtained a copy of the standard, how do I go about reading it?
Position in international standards framework	How will the standard be published internationally?
	What is the international status of IEC 61508?
	How does IEC 61508 fit together with application sector standards?
	What is a basic safety publication?
	What application sector or subsystem standards based on IEC 61508 are there?
	How do safety integrity levels 1 to 4 in IEC 61508 convert or relate to the categories described in EN 954-1?
	Can I use IEC 61508 as a stand-alone standard?
	Will IEC 61508 be revised?
	Can I submit a comment for the revision process?
Regional issues and technical interpretation	How can I find information on IEC 61508 specific to my country?
	Is IEC 61508 also a European Standard?
	Is application of IEC 61508 compulsory under any IEC Directive?
	How can I request a technical interpretation for a particular subclause of the standard?
	How can I contact my national committee?

Tableau A.1 *(suite)*

Section	Questions fréquemment posées
Conformité à la norme	Quelles exigences dois-je satisfaire pour pouvoir revendiquer la conformité à la norme ?
	Comment la CEI 61508 s'applique-t-elle aux systèmes E/E/PE relatifs à la sécurité et de faible complexité ?
	Comment évoluent les exigences de la CEI 61508 en fonction du niveau d'intégrité de sécurité de la fonction de sécurité allouée au système E/E/PE relatif à la sécurité ?
	Pour être conforme à la norme, est-il nécessaire de sélectionner les techniques et les mesures parmi celles recommandées en Annexes A et B de la CEI 61508-2 et de la CEI 61508-3 ?
	J'ai une responsabilité contractuelle pour certaines (mais pas toutes) phases de développement pour un système E/E/PE relatif à la sécurité. De quelle information ai-je besoin dans la documentation des autres parties pour être conforme à la CEI 61508 ?
	Les fournisseurs indiquent que leurs produits sont conformes à la CEI 61508 pour un niveau d'intégrité de sécurité spécifique. Cela signifie-t-il que l'utilisation de tels produits est suffisante pour que je sois conforme à la CEI 61508 ?
	Je suis fournisseur de sous-systèmes tels que des capteurs et des actionneurs qui sont destinés à une utilisation dans des systèmes E/E/PE relatifs à la sécurité. Que signifie la CEI 61508 dans mon cas ?
	Pour être conforme à la CEI 61508, dois-je utiliser des composants certifiés par une tierce-partie ?
	Y a-t-il une corrélation entre le niveau d'indépendance requis pour l'évaluation de la sécurité fonctionnelle et la nécessité d'une certification par une tierce-partie ?
	Comment dois-je aborder le besoin de prendre en considération l'impact des activités humaines sur le fonctionnement d'un système E/E/PE relatif à la sécurité ?
	Est-ce qu'un système E/E/PE relatif à la sécurité peut contenir un matériel et/ou un logiciel qui n'est pas produit en accord avec laCEI 61508, et rester conforme à cette norme ?
	Est-ce que les systèmes de contrôle-commande qui font appel à un système relatif à la sécurité doivent être désignés eux-mêmes comme étant des systèmes relatifs à la sécurité ?
	Comment les limites d'immunité électromagnétiques dépendent-elles du niveau d'intégrité de sécurité ?
Concepts clé	Qu'est-ce que la sécurité fonctionnelle?
	Qu'est-ce qu'un système relatif à la sécurité, dans le contexte de la CEI 61508 ?
	Que signifie E/E/PE ?
	Qu'est-ce qu'un système relatif à la sécurité et de faible complexité ?
	Qu'est-ce qu'un niveau d'intégrité de sécurité (SIL)?
	Que signifie l'intégrité de sécurité d'un logiciel dans le contexte d'une intégrité de sécurité définie comme une probabilité de défaillance ?
	Qu'entend-t-on par un système, un sous-système ou un composant SIL ?
	Qu'est-ce que l'évaluation de la sécurité fonctionnelle ?
	Qu'est-ce qu'un mode opératoire?
	Quelle est la différence entre un mode opératoire de faible demande et un mode opératoire de forte demande ou de demande permanente?
	Donnez-moi un exemple d'architecture pour différents modes opératoires.
	Le mode opératoire affecte-t-il la manière dont le niveau d'intégrité de sécurité est déterminé ?
	Qu'est-ce qu'un équipement sous contrôle (EUC)?
Danger et analyse de risque	La CEI 61508 est-elle la seule norme concernée par la sécurité assurée par l'amélioration de la fiabilité ?
	Est-ce que la CEI 61508 couvre l'élimination du risque à sa source ?
	Est-ce que la CEI 61508 exige qu'une analyse de risque quantitative soit menée pour déterminer les niveaux d'intégrité de sécurité ?
	Quels sont les facteurs à prendre en compte pour planifier une méthode graphique de risque pour déterminer les niveaux d'intégrité de sécurité ?
	Comment dois-je prendre en compte les risques introduits par le système E/E/PE relatif à la sécurité ?

_____

Table A.1 (*continued*)

Section	Frequently asked questions
Complying with the standard	Which requirements do I need to satisfy in order to claim compliance with the standard?
	How does IEC 61508 apply to low complexity E/E/PE safety-related systems?
	How do the requirements of IEC 61508 change with respect to the safety integrity level of the safety functions allocated to the E/E/PE safety-related system?
	Is it necessary to choose techniques and measures from those recommended in annexes A and B of IEC 61508-2 and IEC 61508-3 in order to comply with the standard?
	I have contractual responsibility for some (but not all) of the development phases for an E/E/PE safety-related system. What information do I need in documentation from other parties to enable me to comply with IEC 61508?
	Suppliers are quoting that their products conform to IEC 61508 for a specific safety integrity level. Does this mean that using these products is sufficient for me to comply with IEC 61508?
	I supply subsystems, such as sensors or actuators, that are intended for use in an E/E/PE safety-related system. What does IEC 61508 mean for me?
	Do I have to use third party certified components in order to comply with IEC 61508?
	Is there any correlation between the level of independence required for functional safety assessment and the need for third party certification?
	In what ways do I need to consider the impact of human activities on the operation of an E/E/PE safety-related system?
	Can an E/E/PE safety-related system contain hardware and/or software that was not produced according to IEC 61508, and still comply with the standard?
	Do control systems that place demands on a safety-related system have to be themselves designated as safety-related systems?
	How do electromagnetic immunity limits depend on the safety integrity level?
Key concepts	What is functional safety?
	What is a safety-related system in the context of IEC 61508?
	What does E/E/PE mean?
	What is a low complexity E/E/PE safety-related system?
	What is a safety integrity level (SIL)?
	What does software safety integrity mean in the context of safety integrity being defined as probability of failure?
	What is meant by a SIL system, subsystem or component?
	What is functional safety assessment?
	What is a mode of operation?
	What is the difference between low demand mode of operation and high demand or continuous mode of operation?
	Give me example architectures for the different modes of operation.
	Does the mode of operation affect how the safety integrity level is determined?
	What is the equipment under control (EUC)?
Hazard and risk analysis	Is IEC 61508 only concerned about ensuring safety by improving reliability?
	Does IEC 61508 cover the elimination of hazards at source?
	Does IEC 61508 require a quantitative risk analysis to be carried out in order to determine safety integrity levels?
	What factors should I take into account when planning to use a risk graph method for determining safety integrity levels?
	How do I take account of hazards that are introduced by the E/E/PE safety-related system?

_____

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.

Nicht frankieren
Ne pas affranchir

Non affrancare
No stamp required

A Prioritaire

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 2-8318-7816-0

ICS 13.110; 25.040; 29.020; 35.240.50

Typeset and printed by the IEC Central Office
GENEVA, SWITZERLAND