Publication 61508-4 de la CEI
(Première édition – 1998)

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

Partie 4: Définitions et abréviations

IEC Publication 61508-4
(First edition – 1998)

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

Part 4: Definitions and abbreviations

CORRIGENDUM

Page 6

Au sixième tiret, remplacer le titre de la partie 6 par le titre amendé suivant:

– Partie 6: Lignes directrices pour l'application des parties 2 et 3

Page 7

Sixth dash, replace the title of part 6 by the following amended title:

– Part 6: Guidelines on the application of parts 2 et 3

Page 12

Remplacer le texte de l'article 1.3 existant par le texte amendé suivant:

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

Une des responsabilités incombant à un comité technique est, dans la mesure du possible, d'utiliser les publications 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.

Page 13

Replace the existing text of clause 1.3 by the following amended text:

1.3 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.

Page 18

Tableau 1

Pour MooN dans la deuxième colonne, à la deuxième ligne, remplacer le texte existant par ce qui suit:

(par exemple 1oo2 est une architecture où chacun des deux canaux peut accomplir la fonction de sécurité)

3.1 Termes relatifs à la sécurité

3.1.1

Ajouter la note suivante:

NOTE – Cette définition doit être considérée en cas d'analyse d'un phénomène dangereux et d'un risque (voir CEI 61508-1, 7.4). Si le domaine d'application devait être élargi (i.e. pour inclure les dégâts causés à l'environnement qui ne produisent pas de blessures physiques ou atteintes à la santé) elle devrait être considérée dans la phase de définition globale du domaine d'application (voir CEI 61508-1, 7.3).

3.1.5

Remplacer le texte de la note par le texte amendé suivant:

NOTE – Pour plus d'information sur ce concept, voir annexe A de la CEI 61508-5.

Page 36

Corrections en anglais seulement

Page 19

Table 1

For MooN in the second row, second line, replace the existing text by the following:

(for example 1oo2 is 1 out of 2 architecture, where either of the two channels can perform the safety function)

3.1 Safety terms

3.1.1

Add the following note:

NOTE – This definition will need to be addressed when carrying out a hazard and risk analysis (see IEC 61508-1, 7.4). If the scope is to be widened (e.g to include environmental damage which may not give rise to physical injury or damage to health) then this would need to be addressed in the Overall Scope Definition phase (see IEC 61508-1, 7.3).

3.1.5

The corrections apply to the French text only

Page 37

3.6.4

At the end of note 2, instead of:

IEV 50(191).

read:

IEV 60050(191).

Page 39

Figure 4

In note 1, fifth line, instead of:

(I)

read:

(*I*)

Page 44

3.8.6

Dans la note 1 et dans l'équation, au lieu de:

λ_{total}

lire:

$\lambda_{D\ total}$

3.8.8

Composer les termes suivants en caractères gras:

révélé
déclaré

Page 46

3.8.9

Composer les termes suivants en caractères gras:

non révélé
non déclaré

Page 48

Annexe A

In the last item, instead of:

ANSI/ISA 584...

read:

ANSI/ISA S84...

Page 45

3.8.6

In the first line of definition, instead of:

...failure...

read:

...failures...

In note 1 and in the equation, instead of:

λ_{total}

read:

$\lambda_{D\ total}$

3.8.8

Set the following terms in bold letters:

revealed
overt

Page 47

3.8.9

Set the following terms in bold letters:

unrevealed
covert

Page 49

Annex A

Dans la dernière entrée, au lieu de:

ANSI/ISA 584...

lire:

ANSI/ISA S84...

NORME INTERNATIONALE

INTERNATIONAL STANDARD

CEI
IEC
61508-4

Première édition
First edition
1998-11

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

Partie 4: Définitions et abréviations

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

Part 4: Definitions and abbreviations

Numéro de référence
Reference number
CEI/IEC 61508-4:1998

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: *Symboles 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
61508-4

Première édition
First edition
1998-11

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

Partie 4: Définitions et abréviations

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

Part 4: Definitions and abbreviations

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

IEC Commission Electrotechnique Internationale
International Electrotechnical Commission
Международная Электротехническая Комиссия

CODE PRIX
PRICE CODE U

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

SOMMAIRE

Pages

AVANT-PROPOS 4
INTRODUCTION 8

Articles

1 Domaine d'application 12
2 Références normatives 16
3 Définitions et abréviations 18
3.1 Termes relatifs à la sécurité 18
3.2 Matériel et dispositifs 20
3.3 Systèmes: aspects généraux 24
3.4 Systèmes: aspects relatifs à la sécurité 28
3.5 Fonctions de sécurité et intégrité de sécurité 30
3.6 Anomalie, défaillance et erreur 36
3.7 Activités liées au cycle de vie 40
3.8 Confirmation des mesures de sécurité 42

Annexe A (informative) Bibliographie 48

Index 50

Figures

1 Structure générale de la présente norme 14
2 Système électronique programmable(PES): structure et terminologie 26
3 Système électrique/électronique/électronique programmable(E/E/PES): structure et terminologie 26
4 Modèle de défaillance 38

Tableau

1 Abréviations utilisées dans la présente norme 18

CONTENTS

Page

FOREWORD 5
INTRODUCTION 9

Clause

1 Scope 13
2 Normative references 17
3 Definitions and abbreviations 19
3.1 Safety terms 19
3.2 Equipment and devices 21
3.3 Systems: general aspects 25
3.4 Systems: safety-related aspects 29
3.5 Safety functions and safety integrity 31
3.6 Fault, failure and error 37
3.7 Lifecycle activities 41
3.8 Confirmation of safety measures 43

Annex A (informative) Bibliography 49
Index 51

Figures

1 Overall framework of this standard 15
2 Programmable electronic system (PES): structure and terminology 27
3 Electrical/electronic/programmable electronic system (E/E/PES): structure and terminology 27
4 Failure model 39

Table

1 Abbreviations used in this standard 19

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

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

Partie 4: Définitions et abréviations

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 61508-4 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/265/FDIS	65A/275/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.

L'annexe A est donnée uniquement à titre d'information.

INTERNATIONAL ELECTROTECHNICAL COMMISSION

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

Part 4: Definitions and abbreviations

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 61508-4 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/265/FDIS	65A/275/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.

Annex A is for information only.

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

Cette partie 4 doit être lue conjointement avec toutes les autres parties.

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

This part 4 shall be read in conjunction with all other parts.

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, les actionneurs), mais qu'elle doit considère aussi 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 those 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 recognised 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 International 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 4: Définitions et abréviations

1 Domaine d'application

1.1 La présente partie de la CEI 61508 contient les définitions et explications des termes utilisés dans les parties 1 à 7 de cette norme

1.2 Les définitions sont regroupées sous des titres généraux de telle sorte que les termes qui sont en rapport puissent être compris dans le contexte des autres. Toutefois, il convient de remarquer que ces titres ne sont pas attribués pour ajouter un sens aux définitions et, dans cette perspective, il convient de ne pas prendre en considération les titres de regroupement.

1.3 La CEI 61508-1, la CEI 61508-2, la CEI 61508-3 et la CEI 61508-4 sont des publications fondamentales de sécurité, bien que ce statut ne s'applique pas dans le cas de systèmes E/E/PE de sécurité de faible complexité (voir 3.4.4). En tant que publications fondamentales de sécurité, elles sont destinées à être utilisées par tous les comités d'études pour la mise au point de leurs normes, conformément aux principes décrits dans le Guide CEI 104 et dans le Guide ISO/CEI 51. L'une des responsabilités d'un comité d'études est, chaque fois que cela peut s'appliquer, d'utiliser les publications fondamentales de sécurité pour préparer ses propres publications. La CEI 61508 est également prévue pour une utilisation en tant que norme autonome.

1.4 La figure 1 montre la structure générale des parties 1 à 7 de la CEI 61508 et indique le rôle que CEI 61508-4 joue dans la réalisation de la sécurité fonctionnelle pour les systèmes E/E/PE relatifs à la sécurité.

NOTE – Aux Etats-Unis d'Amérique et au Canada, les normes nationales de sécurité des processus existantes, basées sur la CEI 61508 (par exemple l'ANSI/ISA S84.01-1996, voir référence [8] à l'annexe C) peuvent être appliquées dans le domaine des processus, à la place de la CEI 61508, et cela jusqu'à ce que les normes internationales concernant la mise en œuvre de la CEI 61508 dans le domaine des processus soient publiées.

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

Part 4: Definitions and abbreviations

1 Scope

1.1 This part of IEC 61508 contains the definitions and explanation of terms that are used in parts 1 to 7 of this standard.

1.2 The definitions are grouped under general headings so that related terms can be understood within the context of each other. But it should be noted that these headings are not intended to add meaning to the definitions, and in this sense the headings should be disregarded.

1.3 IEC 61508-1, IEC 61508-2, IEC 61508-3 and IEC 61508-4 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). 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. One of the responsibilities of a technical committee is, wherever applicable, to make use of basic safety publications in the preparation of its own publications. IEC 61508 is also intended for use as a stand-alone standard.

1.4 Figure 1 shows the overall framework for parts 1 to 7 of IEC 61508 and indicates the role that IEC 61508-4 plays in the achievement of functional safety for E/E/PE safety-related systems.

NOTE – In the USA and Canada, until the proposed process sector implementation of IEC 61508 (i.e. IEC 61511) 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) can be applied to the process sector instead of IEC 61508.

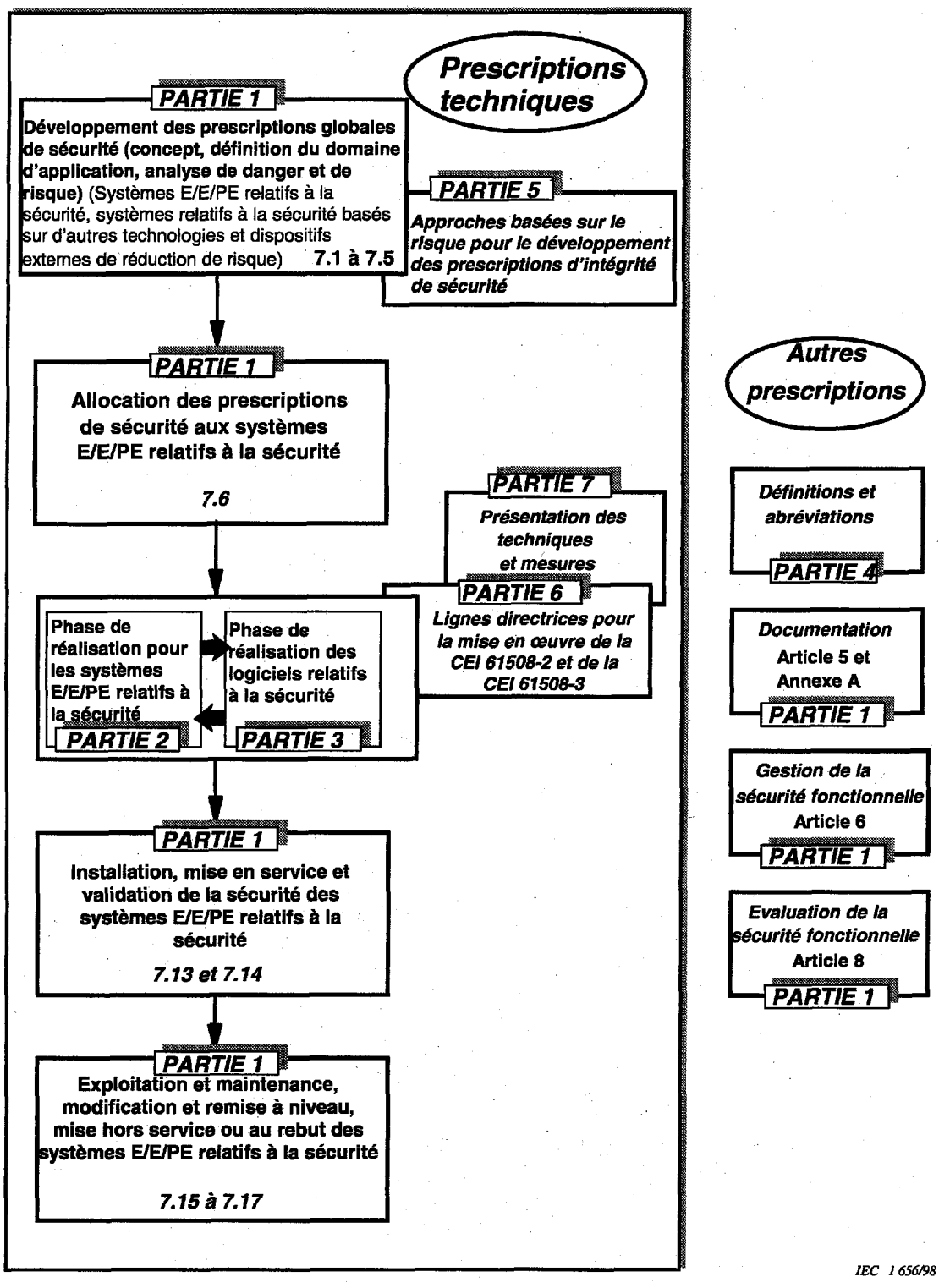


Figure 1 — Structure générale de la présente norme

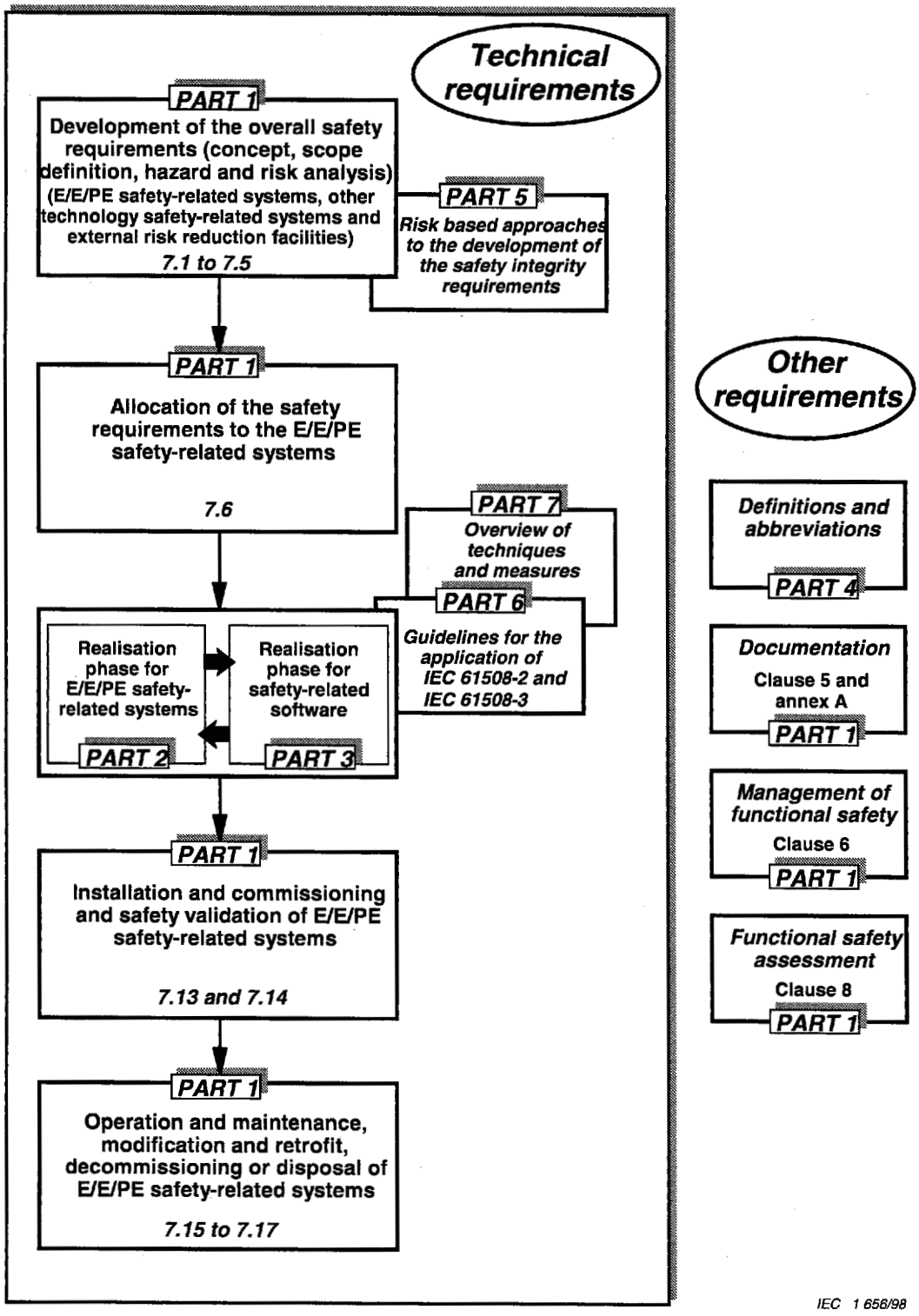


Figure 1 — Overall framework of this standard

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. Au moment de la publication, les éditions indiquées étaient en vigueur. Tout document normatif est sujet à révision et les parties prenantes aux accords fondés sur la présente partie de la CEI 61508 sont invitées à rechercher la possibilité d'appliquer les éditions les plus récentes des documents normatifs indiqués ci-après. Les membres de la CEI et de l'ISO possèdent le registre des Normes internationales en vigueur.

CEI 60050(191):1990, *Vocabulaire Electrotechnique International (VEI) – Chapitre 191: Sûreté de fonctionnement et qualité de service*

CEI 60050(351):1975, *Vocabulaire Electrotechnique International (VEI) – Chapitre 351: Commande et régulation automatiques*

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

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

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

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

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

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

Guide CEI 104:1997, *Elaboration des publications de sécurité et utilisation des publications fondamentales de sécurité et publications groupées de sécurité*

ISO/CEI 2382-14:1998, *Traitement de l'information – Vocabulaire – Partie 14: Fiabilité, maintenabilité et disponibilité*

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

ISO 8402:1994, *Management de la qualité et assurance de la qualité – Vocabulaire*

[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.

IEC 60050(191):1990, *International Electrotechnical Vocabulary (IEV) – Chapter 191: Dependability and quality of service*

IEC 60050(351):1975, *International Electrotechnical Vocabulary (IEV) – Chapter 351: Automatic control*

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

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 61508-5:1998, *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 IEC 61508-2 and IEC 61508-3*[1)]

IEC 61508-7:—, *Functional safety of electrical/electronical/programmable electronic safety-related systems – Part 7: Overview of techniques and measures*[1)]

IEC Guide 104:1997, *The preparation of safety publications and the use of basic safety publications and group safety publications*

ISO/IEC 2382-14:1998, *Data processing – Vocabulary – Part 14: Reliability, maintainability and availability*

ISO/IEC Guide 51:1990, *Safety aspects – Guidelines for their inclusion in standards*

ISO 8402:1994, *Quality management and quality assurance – Vocabulary*

---

1) To be published.

3 Définitions et abréviations

Pour les besoins de la présente Norme internationale, les définitions suivantes s'appliquent, ainsi que les abréviations données dans le tableau 1.

Tableau 1 — Abréviations utilisées dans la présente norme

Abréviation	Expression complète	Définition et/ou explication du terme
MooN	Architecture N canaux parmi M (par exemple 1oo2 est une architecture «1 canal parmi 2»)	Annexe B de la CEI 61508-6
MooND	Architecture N canaux parmi M, avec diagnostic	Annexe B de la CEI 61508-6
ALARP	Aussi faible que raisonnablement possible	Annexe B de la CEI 61508-5
E/E/PE	Electrique/électronique/électronique programmable	3.2.6
E/E/PES	Système électrique/électronique/électronique programmable	3.3.3
EUC	Matériel commandé	3.2.3
PES	Système électronique programmable	3.3.2
PLC	Automate programmable	Annexe E de la CEI 61508-6
SIL	Niveau d'intégrité de sécurité	3.5.6

3.1 Termes relatifs à la sécurité

3.1.1
dommage
blessure physique ou atteinte à la santé affectant des personnes soit directement soit indirectement comme conséquence à un dégât causé aux biens ou à l'environnement

[Guide 51 ISO/CEI:1990 (modifié)]

3.1.2
phénomène dangereux
une source potentielle de danger [Guide 51 ISO/CEI:1990]

NOTE – Ce terme comprend le danger sur des personnes survenant dans un laps de temps très court (feu ou explosion), mais aussi le danger à long terme sur la santé d'une personne (dégagement d'une substance toxique).

3.1.3
situation dangereuse
situation dans laquelle une personne est exposée à un (des) phénomène(s) dangereux

3.1.4
événement dangereux
situation dangereuse qui conduit à un dommage

3.1.5
risque
une combinaison de la probabilité d'un dommage et de sa gravité

[Guide 51 ISO/CEI:1990 (modifié)]

NOTE – Pour plus d'

3.1.6
risque tolérable
risque accepté dans un certain contexte et fondé sur les valeurs actuelles de la société

NOTE – Voir annexe B de la CEI 61508-5.

3 Definitions and abbreviations

For the purposes of this International Standard, the following definitions and the abbreviations given in table 1 apply.

Table 1 — Abbreviations used in this standard

Abbreviation	Full expression	Definition and/or explanation of term
MooN	M out of N channel architecture (for example 1oo2 is 1 out of 2 channel architecture)	Annex B of IEC 61508-6
MooND	M out of N channel architecture with diagnostics	Annex B of IEC 61508-6
ALARP	As low as is reasonably practicable	Annex B of IEC 61508-5
E/E/PE	Electrical/electronic/programmable electronic	3.2.6
E/E/PES	Electrical/electronic/programmable electronic system	3.3.3
EUC	Equipment under control	3.2.3
PES	Programmable electronic system	3.3.2
PLC	Programmable logic controller	Annex E of IEC 61508-6
SIL	Safety integrity level	3.5.6

3.1 Safety terms

3.1.1
harm
physical injury or damage to the health of people either directly or indirectly as a result of damage to property or to the environment
[ISO/IEC Guide 51:1990 (modified)]

3.1.2
hazard
potential source of harm [Guide 51 ISO/IEC:1990]

NOTE – The term includes danger to persons arising within a short time scale (for example, fire and explosion) and also those that have a long-term effect on a person's health (for example, release of a toxic substance).

3.1.3
hazardous situation
circumstance in which a person is exposed to hazard(s)

3.1.4
hazardous event
hazardous situation which results in harm

3.1.5
risk
combination of the probability of occurrence of harm and the severity of that harm
[ISO/IEC Guide 51:1990 (modified)]

NOTE – For more discussion on this concept see annex A of IEC 61508-5.

3.1.6
tolerable risk
risk which is accepted in a given context based on the current values of society

NOTE – See annex B of IEC 61508-5.

3.1.7
risque résiduel
risque restant après que toutes les mesures de prévention ont été prises

3.1.8
sécurité
absence de risque inacceptable

3.1.9
sécurité fonctionnelle
sous-ensemble de la sécurité globale se rapportant à l'EUC et au système de commande de l'EUC qui dépend du fonctionnement correct des systèmes E/E/PE relatifs à la sécurité, des systèmes relatifs à la sécurité basés sur une autre technologie et des dispositifs externes de réduction de risque

3.1.10
état de sécurité
état de l'EUC lorsque la sécurité est réalisée

NOTE – Durant son évolution depuis un état potentiellement dangereux vers un état de sécurité final, l'EUC est susceptible de passer par un certain nombre d'états de sécurité intermédiaires. Dans certaines situations, l'état de sécurité n'est atteint que durant le laps de temps où l'EUC est continuellement commandé. Cette commande continue peut s'étendre sur une période courte ou indéfinie.

3.1.11
mauvais usage raisonnablement prévisible
utilisation d'un produit, d'un procédé ou d'un service dans des conditions ou des fins non prévues par le fournisseur, mais qui peut être induite par le comportement humain habituel en conjonction avec la conception du produit, du procédé ou du service, ou comme résultat de ce comportement

3.2 Matériel et dispositifs

3.2.1
unité fonctionnelle
entité matérielle ou logicielle, ou les deux à la fois, capable de remplir une fonction déterminée

NOTE – Dans le VEI 191-01-01, le terme «entité» est employé à la place d'unité fonctionnelle. Une entité peut, dans certains cas, comprendre du personnel.

[ISO/CEI 2382-14-01-01]

3.2.2
logiciel
création intellectuelle comprenant les programmes, les données, les procédures et règles, ainsi que toute documentation se référant au fonctionnement d'un système de traitement de données

NOTE 1 – Le logiciel est indépendant du support sur lequel il a été enregistré.

NOTE 2 – Cette définition sans la note 1 diffère de l'ISO 2382-1, et la définition complète diffère de l'ISO 9000-3 par l'ajout du mot «données».

3.2.3
équipement commandé (EUC)
équipement, machine, appareil ou installation utilisés pour les activités de fabrication, de traitement, de transport, médicales ou d'autres activités

NOTE – Le système de commande de l'EUC est séparé et distinct de l'EUC.

3.1.7
residual risk
risk remaining after protective measures have been taken

3.1.8
safety
freedom from unacceptable risk

3.1.9
functional safety
part of the overall safety relating to the EUC and the EUC control system which depends on the correct functioning of the E/E/PE safety-related systems, other technology safety-related systems and external risk reduction facilities

3.1.10
safe state
state of the EUC when safety is achieved

NOTE – In going from a potentially hazardous condition to the final safe state, the EUC may have to go through a number of intermediate safe states. For some situations a safe state exists only so long as the EUC is continuously controlled. Such continuous control may be for a short or an indefinite period of time.

3.1.11
reasonably foreseeable misuse
use of a product, process or service under conditions or for purposes not intended by the supplier, but which can happen, induced by the product, process or service in combination with, or as a result of, common human behaviour

3.2 Equipment and devices

3.2.1
functional unit
entity of hardware or software, or both, capable of accomplishing a specified purpose

NOTE – In IEV 191-01-01 the more general term "item" is used in place of functional unit. An item may sometimes include people.

[ISO/IEC 2382-14-01-01]

3.2.2
software
intellectual creation comprising the programs, procedures, data, rules and any associated documentation pertaining to the operation of a data processing system

NOTE 1 – Software is independent of the medium on which it is recorded.

NOTE 2 – This definition without note 1 differs from ISO 2382-1, and the full definition differs from ISO 9000-3, by the addition of the word data.

3.2.3
equipment under control (EUC)
equipment, machinery, apparatus or plant used for manufacturing, process, transportation, medical or other activities

NOTE – The EUC control system is separate and distinct from the EUC.

3.2.4
risque EUC
risque provenant de l'EUC ou de l'interaction de l'EUC avec son système de commande

NOTE 1 – Dans ce contexte, il s'agit du risque associé à l'événement dangereux spécifique pour lequel les systèmes E/E/PE relatifs à la sécurité, les systèmes relatifs à la sécurité basés sur une autre technologie et les dispositifs externes de réduction de risque doivent être utilisés afin de procurer la réduction de risque nécessaire (c'est-à-dire le risque associé à la sécurité fonctionnelle).

NOTE 2 – Le risque EUC est abordé dans la figure A.1 de la CEI 61508-5. L'objectif principal dans la détermination du risque EUC est d'établir un point de référence pour le risque sans prendre en compte les systèmes E/E/PE relatifs à la sécurité, les systèmes relatifs à la sécurité basés sur une autre technologie et les dispositifs externes de réduction de risque.

NOTE 3 – L'évaluation de ce risque comprend les problèmes associés aux facteurs humains.

3.2.5
électronique programmable (PE)
technologie basée sur l'informatique, pouvant comprendre du matériel, du logiciel, ainsi que les unités d'entrée et/ou de sortie

NOTE – Ce terme recouvre les appareils micro-électroniques basés sur une ou plusieurs unités centrales de traitement (CPU) associées à des mémoires, etc.

EXEMPLES Tous les dispositifs suivants sont des dispositifs électroniques programmables:
- les microprocesseurs;
- les microcontrôleurs;
- les automates programmables (PC);
- les circuits intégrés spécifiques à une application (ASIC);
- les automates logiques programmables (PLC);
- les autres appareils basés sur la technologie informatique (par exemple capteurs intelligents, les transmetteurs, les actionneurs).

3.2.6
électrique/électronique/électronique programmable (E/E/PE)
technologie basée sur la technologie électrique (E), et/ou électronique (E) et/ou électronique programmable (PE)

NOTE – Ce terme désigne l'ensemble des appareils fonctionnant selon les principes électriques.

EXEMPLE Les dispositifs électriques/électroniques/électroniques programmables comprennent
- les appareils électromécaniques (électriques);
- les appareils électroniques non programmables à circuits intégrés (électroniques);
- les appareils électroniques basés sur la technologie informatique (électroniques programmables); voir 3.2.5.

3.2.7
langage de variabilité limitée
langage de programmation de logiciel, textuel ou graphique, pour les automates programmables destinés aux applications commerciales et industrielles dont l'étendue des possibilités est limitée aux besoins de leur application

EXEMPLE Les langages suivants sont des langages de variabilité limitée, définis à partir de la CEI 61131-3 et d'autres sources, utilisés pour représenter le programme d'application d'un système d'automates programmables:

– langage à contacts: langage graphique consistant en une série de symboles d'entrée (représentant le comportement de dispositifs similaires à des contacts normalement ouverts et des contacts normalement fermés) interconnectés par des lignes (pour indiquer le sens du courant) à des symboles de sortie (représentant un comportement similaire à celui de relais);

– algèbre booléenne: langage de bas niveau basé sur des opérateurs booléens tels que ET, OU et NON avec la possibilité d'ajouter quelques instructions mnémoniques;

– langage en blocs fonctionnels: en plus des opérateurs booléens, il permet l'utilisation de fonctions plus complexes telles que fichiers de transfert de données, bloc de transfert lecture/écriture, registre à décalage et séquenceur d'instructions;

– diagramme fonctionnel en séquence: représentation graphique d'un programme séquentiel consistant en étapes interconnectées, actions et liens orientés comportant des conditions de transition.

3.2.4
EUC risk
risk arising from the EUC or its interaction with the EUC control system

NOTE 1 – The risk in this context is that associated with the specific hazardous event in which E/E/PE safety-related systems, other technology safety-related systems and external risk reduction facilities are to be used to provide the necessary risk reduction, (i.e. the risk associated with functional safety).

NOTE 2 – The EUC risk is indicated in figure A.1 of IEC 61508-5. The main purpose of determining the EUC risk is to establish a reference point for the risk without taking into account E/E/PE safety-related systems, other technology safety-related systems and external risk reduction facilities.

NOTE 3 – Assessment of this risk will include associated human factor issues.

3.2.5
programmable electronic (PE)
based on computer technology which may be comprised of hardware, software, and of input and/or output units

NOTE – This term covers microelectronic devices based on one or more central processing units (CPUs) together with associated memories, etc.

EXAMPLE The following are all programmable electronic devices:

- microprocessors;
- micro-controllers;
- programmable controllers;
- application specific integrated circuits (ASICs);
- programmable logic controllers (PLCs);
- other computer-based devices (for example smart sensors, transmitters, actuators).

3.2.6
electrical/electronic/programmable electronic (E/E/PE)
based on electrical (E) and/or electronic (E) and/or programmable electronic (PE) technology

NOTE – The term is intended to cover any and all devices or systems operating on electrical principles.

EXAMPLE Electrical/electronic/programmable electronic devices include

- electro-mechanical devices (electrical);
- solid-state non-programmable electronic devices (electronic);
- electronic devices based on computer technology (programmable electronic); see 3.2.5.

3.2.7
limited variability language
software programming language, either textual or graphical, for commercial and industrial programmable electronic controllers with a range of capabilities limited to their application

EXAMPLE The following are limited variability languages, from IEC 61131-3 and other sources, which are used to represent the application program for a PLC system:

– ladder diagram: a graphical language consisting of a series of input symbols (representing behaviour similar to devices such as normally open and normally closed contacts) interconnected by lines (to indicate the flow of current) to output symbols (representing behaviour similar to relays);

– Boolean algebra: a low-level language based on Boolean operators such as AND, OR and NOT with the ability to add some mnemonic instructions;

– function block diagram: in addition to Boolean operators, allows the use of more complex functions such as data transfer file, block transfer read/write, shift register and sequencer instructions;

– sequential function chart: a graphical representation of a sequential program consisting of interconnected steps, actions and directed links with transition conditions.

3.3 Systèmes: aspects généraux

3.3.1
système
ensemble d'éléments qui interagissent selon un modèle précis, un élément pouvant être un autre système, appelé sous-système, les sous-systèmes pouvant être eux-mêmes soit un système de commande soit un système commandé composé de matériel, de logiciel en interaction avec l'être humain

NOTE 1 – Une personne peut faire partie d'un système (voir aussi note 5 en 3.4.1).

NOTE 2 – Cette définition est différente de celle du VEI 351-01-01

3.3.2
système électronique programmable (PES)
système de commande, de protection ou de surveillance basé sur un ou plusieurs dispositifs électroniques programmables. Ce terme recouvre tous les éléments du système, tels que l'alimentation, les capteurs, ou autres dispositifs d'entrée, jusqu'aux actionneurs, ou autres dispositifs de sortie, en passant par les autoroutes de données ou autres voies de communication (voir la figure 2)

NOTE – La structure d'un PES est présentée à la figure 2 a). La figure 2 b) illustre la façon dont est représenté le PES dans cette Norme internationale, l'électronique programmable étant une unité distincte des capteurs et actionneurs de l'EUC et de leurs interfaces. Cependant l'électronique programmable peut être présente en divers endroits du PES. La figure 2 c) présente un PES pourvu de deux unités discrètes d'électronique programmable. La figure 2 d) illustre un PES pourvu d'une électronique programmable doublée (c'est-à-dire à deux canaux), mais avec un seul capteur et un seul actionneur.

3.3.3
système électrique/électronique/électronique programmable (E/E/PES)
système de commande, de protection ou de surveillance basé sur un ou plusieurs dispositifs électroniques programmables. Ce terme recouvre tous les éléments du système, tels que l'alimentation, les capteurs, ou autres dispositifs d'entrée, jusqu'aux actionneurs, ou autres dispositifs de sortie, en passant par les autoroutes de données ou autres voies de communication (voir la figure 3)

3.3.4
système de commande de l'EUC
système qui réagit à des signaux d'entrée provenant du processus et/ou d'un opérateur et qui produit des signaux de sortie qui font que l'EUC fonctionne de la façon souhaitée

NOTE – Le système de commande de l'EUC comprend des dispositifs d'entrée et des éléments terminaux.

3.3.5
architecture
configuration spécifique des éléments matériels et logiciels dans un système

3.3.6
module
composant de série ou discret ou ensemble fonctionnel de composants de série ou discrets encapsulés formant un tout

3.3.7
module logiciel
construction consistant en des procédures et/ou déclarations de données pouvant aussi être en interaction avec d'autres constructions de même nature

3.3 Systems: general aspects

3.3.1
system
set of elements which interact according to a design, where an element of a system can be another system, called a subsystem, which may be a controlling system or a controlled system and may include hardware, software and human interaction

NOTE 1 – A person can be part of a system (see also note 5 of 3.4.1).

NOTE 2 – This definition differs from IEV 351-01-01.

3.3.2
programmable electronic system (PES)
system for control, protection or monitoring based on one or more programmable electronic devices, including all elements of the system such as power supplies, sensors and other input devices, data highways and other communication paths, and actuators and other output devices (see figure 2)

NOTE – The structure of a PES is shown in figure 2 a). Figure 2 b) illustrates the way in which a PES is represented in this International Standard, with the programmable electronics shown as a unit distinct from sensors and actuators on the EUC and their interfaces, but the programmable electronics could exist at several places in the PES. Figure 2 c) illustrates a PES with two discrete units of programmable electronics. Figure 2 d) illustrates a PES with dual programmable electronics (i.e. two-channel), but with a single sensor and a single actuator.

3.3.3
electrical/electronic/programmable electronic system (E/E/PES)
system for control, protection or monitoring based on one or more electrical/electronic programmable electronic (E/E/PE) devices, including all elements of the system such as power supplies, sensors and other input devices, data highways and other communication paths, and actuators and other output devices (see figure 3)

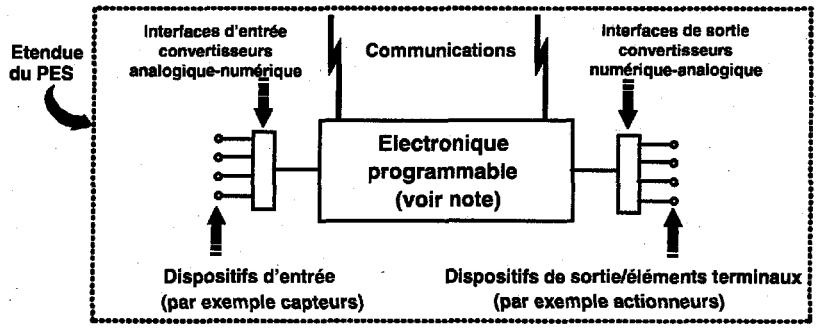
3.3.4
EUC control system
system which responds to input signals from the process and/or from an operator and generates output signals causing the EUC to operate in the desired manner

NOTE – The EUC control system includes input devices and final elements.

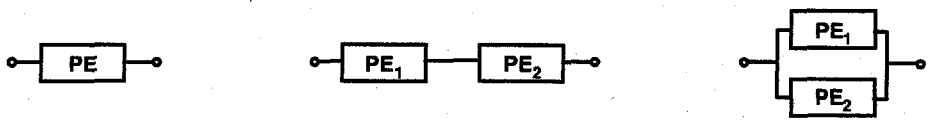
3.3.5
architecture
specific configuration of hardware and software elements in a system

3.3.6
module
routine, discrete component or a functional set of encapsulated routines or discrete components belonging together

3.3.7
software module
construct that consists of procedures and/or data declarations and that can also interact with other such constructs



a) Structure de base d'un PES



b) PES seul avec un seul dispositif électronique programmable (c'est-à-dire un seul PES composé d'une électronique programmable à un seul canal)

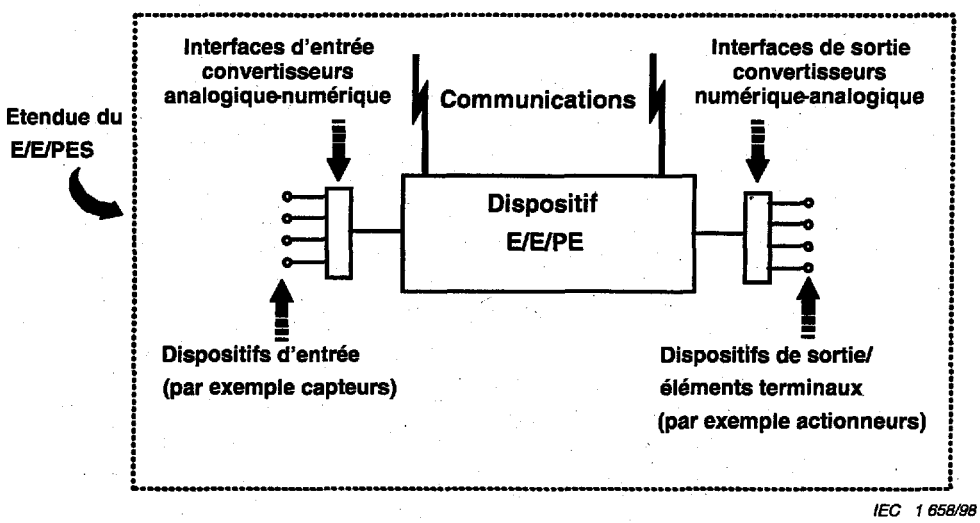
c) PES seul avec deux dispositifs électroniques programmables en série (par exemple capteur intelligent et automate programmable)

d) PES seul avec deux dispositifs électroniques programmables qui se partagent les capteurs et les éléments terminaux (c'est-à-dire un PES composé de deux canaux d'électronique programmable)

IEC 1 657/98

NOTE – L'électronique programmable est présentée de façon centrale, mais elle peut se situer en différents endroits du PES.

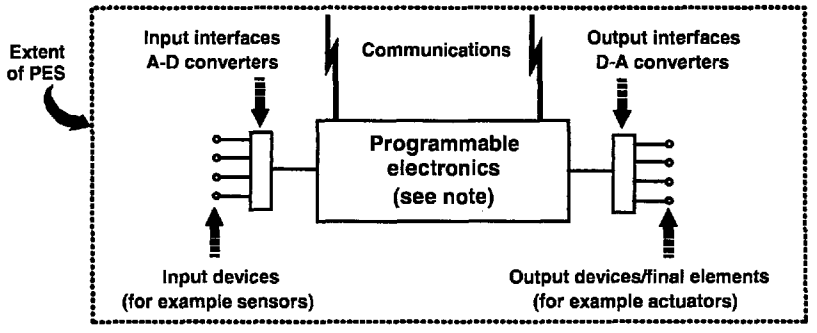
Figure 2 — Système électronique programmable(PES): structure et terminologie



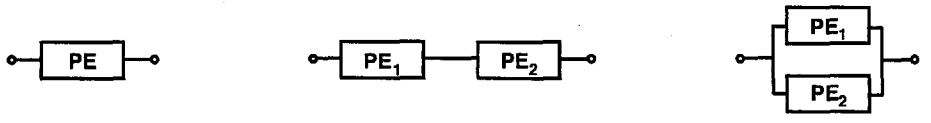
IEC 1 658/98

NOTE – Le dispositif E/E/PE est présenté de façon centrale mais un tel ou de tels dispositifs peuvent se situer en différents endroits du E/E/PES.

Figure 3 — Système électrique/électronique/électronique programmable(E/E/PES): structure et terminologie



a) Basic PES structure



b) Single PES with single programmable electronic device (i.e. one PES comprised of a single channel of programmable electronics)

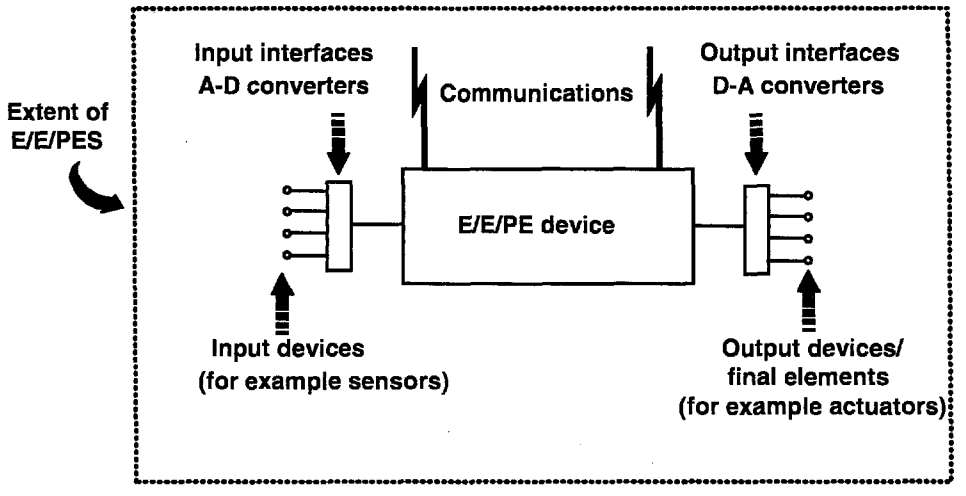
c) Single PES with dual programmable electronic devices linked in a serial manner (for example intelligent sensor and programmable controller)

d) Single PES with dual programmable electronic devices but with shared sensors and final elements (i.e. one PES comprised of two channels of programmable electronics)

IEC 1 657/98

NOTE – The programmable electronics are shown centrally located but could exist at several places in the PES.

Figure 2 — Programmable electronic system (PES): structure and terminology



IEC 1 658/98

NOTE – THE E/E/PE device is shown centrally located but such device(s) could exist at several places in the E/E/PES.

Figure 3 — Electrical/electronic/programmable electronic system (E/E/PES): structure and terminology

3.3.8
canal
élément ou groupe d'éléments exécutant une fonction indépendante

EXEMPLE Une configuration à deux canaux (à canal doublé) comprend deux canaux réalisant indépendamment la même fonction.

NOTE 1 – Les éléments d'un canal peuvent par exemple comporter des modules d'entrée et de sortie, un système logique (voir 3.4.5), des capteurs et des éléments terminaux.

NOTE 2 – Ce terme peut être utilisé pour décrire un système complet ou une partie seulement d'un système (par exemple les capteurs ou les éléments terminaux).

3.3.9
diversité
moyens différents pour réaliser une fonction requise

EXEMPLE La diversité peut être réalisée en utilisant d'autres principes physiques ou d'autres manières de résoudre un même problème.

3.3.10
redondance
existence de plus de moyens que strictement nécessaire pour accomplir une fonction requise dans une unité fonctionnelle ou pour représenter des informations par des données.

EXEMPLE Utilisation d'éléments fonctionnels en double, adjonction de bits de parité

NOTE 1 – La redondance sert essentiellement à améliorer la fiabilité ou la disponibilité.

NOTE 2 – La définition du VEI 191-15-01 est moins complète.

[ISO/CEI 2382-14-01-12]

3.4 Systèmes: aspects relatifs à la sécurité

3.4.1
système relatif à la sécurité
un tel système est un système qui, à la fois

– met en oeuvre les fonctions de sécurité requises pour atteindre un état de sécurité de l'EUC ou pour maintenir un tel état;

– est prévu pour atteindre, par lui même ou grâce à des systèmes E/E/PE relatifs à la sécurité, ou des systèmes relatifs à la sécurité basés sur une autre technologie ou des dispositifs externes de réduction de risque, le niveau d'intégrité de sécurité nécessaire à la mise en oeuvre des fonctions de sécurité requises.

NOTE 1 – Ce terme fait référence aux systèmes spécifiques dits relatifs à la sécurité qui, avec les dispositifs externes de réduction de risque (voir 3.4.3), permettent de réaliser la réduction de risque nécessaire, afin d'atteindre le niveau de sécurité tolérable requis (voir 3.1.6). Voir également annexe A de la CEI 61508-5.

NOTE 2 – Les systèmes relatifs à la sécurité sont conçus pour empêcher l'EUC d'entrer dans un état dangereux en prenant les mesures appropriées dès l'arrivée des commandes. La défaillance d'un système relatif à la sécurité serait alors incluse dans les événements à l'origine du ou des phénomènes dangereux déterminés. Bien qu'il puisse exister d'autres systèmes possédant des fonctions de sécurité, ce sont les systèmes relatifs à la sécurité qui ont été choisis pour atteindre à leur façon le niveau de risque tolérable. Les systèmes relatifs à la sécurité peuvent globalement être divisés en deux classes, les systèmes relatifs à la sécurité de commande et les systèmes relatifs à la sécurité de protection et ils ont deux modes de fonctionnement (voir 3.5.12).

NOTE 3 – Les systèmes relatifs à la sécurité peuvent faire partie intégrante du système de commande de l'EUC ou peuvent être interfacés avec l'EUC par l'intermédiaire de capteurs et/ou d'actionneurs. Cela signifie qu'il est possible d'atteindre le niveau d'intégrité de sécurité requis en mettant en oeuvre les fonctions de sécurité dans le système de commande de l'EUC (et également par l'adjonction éventuelle de systèmes séparés et indépendants) ou que ces fonctions de sécurité peuvent être exécutées par des systèmes séparés et indépendants dédiés à la sécurité.

NOTE 4 – Un système relatif à la sécurité peut

a) être choisi pour prévenir un événement dangereux (c'est-à-dire qu'aucun événement dangereux ne survient tant que les systèmes relatifs à la sécurité exécutent leurs fonctions de sécurité);

b) être choisi pour réduire les effets d'un événement dangereux, réduisant ainsi le risque en réduisant les conséquences de ce risque;

c) être choisi pour réaliser une combinaison de a) et b).

3.3.8
channel
element or group of elements that independently perform(s) a function

EXAMPLE A two-channel (or dual-channel) configuration is one with two channels that independently perform the same function.

NOTE 1 – The elements within a channel could include input/output modules, a logic system (see 3.4.5), sensors and final elements.

NOTE 2 – The term can be used to describe a complete system, or a portion of a system (for example, sensors or final elements).

3.3.9
diversity
different means of performing a required function

EXAMPLE Diversity may be achieved by different physical methods or different design approaches.

3.3.10
redundancy
existence of means, in addition to the means which would be sufficient for a functional unit to perform a required function or for data to represent information

EXAMPLE Duplicated functional components and the addition of parity bits are both instances of redundancy.

NOTE 1 – Redundancy is used primarily to improve reliability or availability.

NOTE 2 – The definition in IEV 191-15-01 is less complete.

[ISO/IEC 2382-14-01-12]

3.4 Systems: safety-related aspects

3.4.1
safety-related system
designated system that both

- implements the required safety functions necessary to achieve or maintain a safe state for the EUC; and
- is intended to achieve, on its own or with other E/E/PE safety-related systems, other technology safety-related systems or external risk reduction facilities, the necessary safety integrity for the required safety functions

NOTE 1 – The term refers to those systems, designated as safety-related systems, that are intended to achieve, together with the external risk reduction facilities (see 3.4.3), the necessary risk reduction in order to meet the required tolerable risk (see 3.1.6). See also annex A of IEC 61508-5.

NOTE 2 – The safety-related systems are designed to prevent the EUC from going into a dangerous state by taking appropriate action on receipt of commands. The failure of a safety-related system would be included in the events leading to the determined hazard or hazards. Although there may be other systems having safety functions, it is the safety-related systems that have been designated to achieve, in their own right, the required tolerable risk. Safety-related systems can broadly be divided into safety-related control systems and safety-related protection systems, and have two modes of operation (see 3.5.12).

NOTE 3 – Safety-related systems may be an integral part of the EUC control system or may interface with the EUC by sensors and/or actuators. That is, the required safety integrity level may be achieved by implementing the safety functions in the EUC control system (and possibly by additional separate and independent systems as well) or the safety functions may be implemented by separate and independent systems dedicated to safety.

NOTE 4 – A safety-related system may

a) be designed to prevent the hazardous event (i.e. if the safety-related systems perform their safety functions then no hazardous event arises);

b) be designed to mitigate the effects of the hazardous event, thereby reducing the risk by reducing the consequences;

c) be designed to achieve a combination of a) and b).

NOTE 5 – Une personne peut faire partie d'un système relatif à la sécurité (voir 3.3.1). Par exemple, une personne peut recevoir des informations d'un dispositif électronique programmable et exécuter une activité de sécurité à partir de cette information, éventuellement par l'intermédiaire d'un dispositif électronique programmable.

NOTE 6 – Ce terme recouvre l'ensemble des matériels, logiciels, ainsi que tous les équipements annexes (par exemple alimentation) nécessaires pour mener à bien la fonction de sécurité spécifiée (les capteurs, les autres dispositifs d'entrée, les éléments terminaux (actionneurs) ainsi que les autres dispositifs de sortie sont par conséquent compris dans le système relatif à la sécurité).

NOTE 7 – Un système relatif à la sécurité peut être basé sur une large gamme de technologies, comprenant les technologies électrique, électronique, électronique programmable, hydraulique et pneumatique.

3.4.2
système relatif à la sécurité basé sur une autre technologie
systèmes relatifs à la sécurité qui sont basés sur une technologie autre qu'électrique/-électronique/ électronique programmable

EXEMPLE Une soupape de sécurité est un système relatif à la sécurité basé sur une autre technologie.

3.4.3
dispositifs externes de réduction de risque
mesures destinées à réduire ou atténuer les risques qui sont séparées et distinctes et n'utilisent pas de système E/E/PE relatif à la sécurité ou un système relatif à la sécurité basé sur une autre technologie

EXEMPLE Un système de drainage, une cloison coupe-feu, une digue sont des dispositifs externes de réduction de risque.

3.4.4
système E/E/PE relatif à la sécurité de faible complexité
système E/E/PE relatif à la sécurité (voir 3.2.6 et 3.4.1) pour lequel

– les modes de défaillance de chaque composant individuel sont bien définis;
– le comportement du système dans des conditions anormales peut être complètement déterminé.

NOTE – Le comportement du système dans des conditions anormales peut être déterminé par des méthodes analytiques et/ou d'essai.

EXEMPLE Un système qui comprend un ou plusieurs interrupteurs de fin de course, faisant fonctionner, éventuellement via des relais électromécaniques interposés, un ou plusieurs contacteurs destinés à couper l'alimentation de moteurs électriques est un système E/E/PE relatif à la sécurité de faible complexité.

3.4.5
système logique
portion d'un système qui réalise les fonctions logiques, à l'exception des capteurs et des éléments terminaux

NOTE – Dans cette norme, les systèmes logiques suivants sont utilisés:
– systèmes logiques électriques pour la technologie électromécanique;
– systèmes logiques électroniques pour la technologie électronique;
– systèmes logiques programmables pour les systèmes électroniques programmables.

3.5 Fonctions de sécurité et intégrité de sécurité

3.5.1
fonction de sécurité
fonction à réaliser par un système E/E/PE relatif à la sécurité, par un système relatif à la sécurité basé sur une autre technologie, ou par un dispositif externe de réduction de risque, prévue pour assurer ou maintenir un état de sécurité de l'EUC par rapport à un événement dangereux spécifique (voir 3.4.1)

3.5.2
intégrité de sécurité
probabilité pour qu'un système relatif à la sécurité exécute de manière satisfaisante les fonctions de sécurité requises dans toutes les conditions spécifiées et dans une période de temps spécifiée

NOTE 1 – Plus le niveau d'intégrité de sécurité des systèmes relatifs à la sécurité est élevé, plus la probabilité d'une défaillance des systèmes relatifs à la sécurité dans l'exécution des fonctions requises est faible.

NOTE 2 – Il y a quatre niveaux d'intégrité de sécurité pour les systèmes (voir 3.5.6).

NOTE 5 – A person can be part of a safety-related system (see 3.3.1). For example, a person could receive information from a programmable electronic device and perform a safety action based on this information, or perform a safety action through a programmable electronic device.

NOTE 6 – The term includes all the hardware, software and supporting services (for example, power supplies) necessary to carry out the specified safety function (sensors, other input devices, final elements (actuators) and other output devices are therefore included in the safety-related system).

NOTE 7 – A safety-related system may be based on a wide range of technologies including electrical, electronic, programmable electronic, hydraulic and pneumatic.

3.4.2
other technology safety-related system
safety-related system based on a technology other than electrical/electronic/programmable electronic

EXAMPLE A relief valve is another technology safety-related system.

3.4.3
external risk reduction facility
measure to reduce or mitigate the risks which are separate and distinct from, and do not use, E/E/PE safety-related systems or other technology safety-related systems

EXAMPLE A drain system, a fire wall and a bund are all external risk reduction facilities.

3.4.4
low complexity E/E/PE safety-related system
E/E/PE safety-related system (see 3.2.6 and 3.4.1), in which

- the failure modes of each individual component are well defined;
- the behaviour of the system under fault conditions can be completely determined.

NOTE – Behaviour of the system under fault conditions may be determined by analytical and/or test methods.

EXAMPLE A system comprising one or more limit switches, operating, possibly via interposing electro-mechanical relays, one or more contactors to de-energise an electric motor is a low-complexity E/E/PE safety-related system.

3.4.5
logic system
portion of a system that performs the function logic but excludes the sensors and final elements

NOTE – In this standard the following logic systems are used:
- electrical logic systems for electro-mechanical technology;
- electronic logic systems for electronic technology;
- programmable electronic logic systems for programmable electronic systems.

3.5 Safety functions and safety integrity

3.5.1
safety function
function to be implemented by an E/E/PE safety-related system, other technology safety-related system or external risk reduction facilities, which is intended to achieve or maintain a safe state for the EUC, in respect of a specific hazardous event (see 3.4.1)

3.5.2
safety integrity
probability of a safety-related system satisfactorily performing the required safety functions under all the stated conditions within a stated period of time

NOTE 1 – The higher the level of safety integrity of the safety-related systems, the lower the probability that the safety-related systems will fail to carry out the required safety functions.

NOTE 2 – There are four levels of safety integrity for systems (see 3.5.6).

NOTE 3 – Il convient que l'évaluation de l'intégrité de sécurité prenne en compte toutes les causes de défaillance (à la fois les défaillances aléatoires du matériel et les défaillances systématiques) conduisant à un état de non-sécurité, par exemple les défaillances de matériel, les défaillances induites du logiciel et les défaillances dues aux perturbations électriques. Certaines de ces défaillances, en particulier les défaillances accidentelles du matériel, peuvent être quantifiées à l'aide de mesures telles que celle du taux de défaillance en mode de défaillance dangereux, ou de la probabilité de défaillance de fonctionnement à la demande d'un système de protection de sécurité. Cependant, la sécurité intégrale d'un système dépend également de plusieurs facteurs qui ne peuvent être précisément quantifiés, mais simplement considérés d'un point de vue qualitatif.

NOTE 4 – L'intégrité de sécurité comprend l'intégrité de sécurité du matériel (voir 3.5.5) ainsi que l'intégrité de sécurité systématique (voir paragraphe 3.5.4).

NOTE 5 – Cette définition est centrée sur la fiabilité des systèmes relatifs à la sécurité dans l'exécution de leurs fonctions de sécurité (voir VEI 191-12-01).

3.5.3
intégrité de sécurité du logiciel
mesure indiquant la probabilité pour qu'un logiciel dans un système électronique programmable exécute ses fonctions de sécurité dans toutes les conditions spécifiées et dans une période de temps spécifiée

3.5.4
intégrité de sécurité systématique
partie de l'intégrité de sécurité des systèmes relatifs à la sécurité qui se rapporte aux défaillances systématiques (voir note 3 en 3.5.2) dans un mode de défaillance dangereux

NOTE 1 – L'intégrité de sécurité systématique ne peut normalement être quantifiée (à la différence de l'intégrité de sécurité du matériel qui, la plupart du temps, peut l'être).

NOTE 2 – Voir 3.5.2, 3.5.5 et 3.6.6.

3.5.5
intégrité de sécurité du matériel
partie de l'intégrité de sécurité des systèmes relatifs à la sécurité liée aux défaillances aléatoires du matériel en mode de défaillance dangereux

NOTE 1 – Ce terme fait référence aux défaillances en mode dangereux, c'est-à-dire aux défaillances survenant dans un système relatif à la sécurité et susceptibles de nuire à son intégrité de sécurité. Les deux paramètres à prendre en compte en l'occurrence sont le taux global de défaillance et la probabilité de défaillance du fonctionnement à la demande. Le premier de ces deux paramètres de fiabilité est utilisé chaque fois qu'il est nécessaire de maintenir un contrôle continu afin de garantir la sécurité; le second paramètre, quant à lui, est utilisé dans le contexte des systèmes de protection de sécurité.

NOTE 2 – Voir 3.5.2, 3.5.4 et 3.6.5.

3.5.6
niveau d'intégrité de sécurité (SIL)
niveau discret (parmi quatre possibles) permettant de spécifier les prescriptions concernant l'intégrité de sécurité des fonctions de sécurité à allouer aux systèmes E/E/PE relatifs à la sécurité. Le niveau 4 d'intégrité de sécurité possède le plus haut degré d'intégrité; le niveau 1 possède le plus bas.

NOTE – Les mesures cibles des défaillances (voir 3.5.13) pour les quatre niveaux d'intégrité de sécurité sont indiquées dans les tableaux 2 et 3 de la CEI 61508-1.

3.5.7
niveau d'intégrité de sécurité du logiciel
niveau discret (parmi quatre possibles) permettant de spécifier l'intégrité de sécurité d'un logiciel dans un système relatif à la sécurité

NOTE – Voir 3.5.3 et 3.5.6.

3.5.8
spécification des prescriptions concernant la sécurité
spécification contenant toutes les prescriptions liées aux fonctions de sécurité qui doivent être exécutés par les systèmes relatifs à la sécurité

NOTE – Cette spécification se divise en deux parties:
- spécification des prescriptions concernant les fonctions de sécurité (voir 3.5.9);
- spécification des prescriptions concernant l'intégrité de sécurité (voir 3.5.10).

NOTE 3 – In determining safety integrity, all causes of failures (both random hardware failures and systematic failures) which lead to an unsafe state should be included, for example hardware failures, software induced failures and failures due to electrical interference. Some of these types of failure, in particular random hardware failures, may be quantified using such measures as the failure rate in the dangerous mode of failure or the probability of a safety-related protection system failing to operate on demand. However, the safety integrity of a system also depends on many factors which cannot be accurately quantified but can only be considered qualitatively.

NOTE 4 – Safety integrity comprises hardware safety integrity (see 3.5.5) and systematic safety integrity (see 3.5.4).

NOTE 5 – This definition focuses on the reliability of the safety-related systems to perform the safety functions (see IEV 191-12-01 for a definition of reliability).

3.5.3
software safety integrity
measure that signifies the likelihood of software in a programmable electronic system achieving its safety functions under all stated conditions within a stated period of time

3.5.4
systematic safety integrity
part of the safety integrity of safety-related systems relating to systematic failures (see note 3 of 3.5.2) in a dangerous mode of failure

NOTE 1 – Systematic safety integrity cannot usually be quantified (as distinct from hardware safety integrity which usually can).

NOTE 2 – See 3.5.2, 3.5.5 and 3.6.6.

3.5.5
hardware safety integrity
part of the safety integrity of the safety-related systems relating to random hardware failures in a dangerous mode of failure

NOTE 1 – The term relates to failures in a dangerous mode, that is, those failures of a safety-related system that would impair its safety integrity. The two parameters that are relevant in this context are the overall dangerous failure rate and the probability of failure to operate on demand. The former reliability parameter is used when it is necessary to maintain continuous control in order to maintain safety, the latter reliability parameter is used in the context of safety-related protection systems.

NOTE 2 – See 3.5.2, 3.5.4 and 3.6.5.

3.5.6
safety integrity level (SIL)
discrete level (one out of a possible four) for specifying the safety integrity requirements of the safety functions to be allocated to the E/E/PE safety-related systems, where safety integrity level 4 has the highest level of safety integrity and safety integrity level 1 has the lowest

NOTE – The target failure measures (see 3.5.13) for the four safety integrity levels are specified in tables 2 and 3 of IEC 61508-1.

3.5.7
software safety integrity level
discrete level (one out of a possible four) for specifying the safety integrity of software in a safety-related system

NOTE – See 3.5.3 and 3.5.6.

3.5.8
safety requirements specification
specification containing all the requirements of the safety functions that have to be performed by the safety-related systems

NOTE – This specification is divided into the
- safety functions requirements specification (see 3.5.9);
- safety integrity requirements specification (see 3.5.10).

3.5.9
spécification des prescriptions concernant les fonctions de sécurité
spécification qui contient les prescriptions nécessaires aux fonctions de sécurité qui doivent être exécutées par les systèmes relatifs à la sécurité

NOTE 1 – Cette spécification constitue une partie (partie concernant les fonctions de sécurité) de la spécification des prescriptions de sécurité (voir 3.5.8). Elle contient le détail précis des fonctions de sécurité réalisées par les systèmes relatifs à la sécurité.

NOTE 2 – Les spécifications peuvent comporter des documents sous forme de texte, d'organigrammes, de matrices, de diagrammes logiques, etc., pourvu que ces documents rendent plus claires les fonctions de sécurité.

3.5.10
spécification des prescriptions concernant l'intégrité de sécurité
spécification qui contient les prescriptions d'intégrité de sécurité des fonctions de sécurité devant être exécutées par les systèmes relatifs à la sécurité

NOTE – Cette spécification constitue une partie (partie concernant l'intégrité de sécurité) de la spécification des prescriptions de sécurité (voir 3.5.8).

3.5.11
logiciel de sécurité
logiciel utilisé pour exécuter des fonctions de sécurité dans un système relatif à la sécurité

3.5.12
mode de fonctionnement
utilisation prévue d'un système relatif à la sécurité, en rapport avec la fréquence des demandes, pouvant être

- **mode demande faible:** lorsque la fréquence des demandes de fonctionnement sur un système relatif à la sécurité est plus grande que une par an et au plus égale à deux fois la fréquence des tests périodiques;
- **mode demande élevée ou mode continu:** lorsque la fréquence des demandes de fonctionnement sur un système relatif à la sécurité est plus grande que une par an ou supérieure à la fréquence des tests périodiques

NOTE 1 – Les modes demande élevée ou continue couvrent les systèmes relatifs à la sécurité qui réalisent une commande continue pour maintenir la sécurité fonctionnelle.

NOTE 2 – Les mesures cibles de défaillances pour les systèmes relatifs à la sécurité fonctionnant en mode demande faible et en mode demande élevée ou en mode continu sont présentées en 3.5.13.

3.5.13
mesure cible des défaillances
probabilité prévisionnelle d'un mode de défaillance dangereux, à réaliser en fonction des prescriptions d'intégrité de sécurité, spécifiée en termes de

- probabilité moyenne de défaillance lors de l'exécution sur demande de la fonction spécifique (en mode demande faible);
- probabilité d'une défaillance dangereuse par année (en mode demande élevée ou en mode continu)

NOTE – Les valeurs numériques des mesures de défaillance cibles sont présentées aux tableaux 2 et 3 de la CEI 61508-1.

3.5.14
réduction de risque nécessaire
réduction de risque à réaliser par le système relatif à la sécurité E/E/PE, un système relatif à la sécurité basé sur une autre technologie et par les dispositifs externes de réduction de risque afin d'assurer que le risque tolérable n'est pas dépassé

3.5.9
safety functions requirements specification
specification containing the requirements for the safety functions that have to be performed by the safety-related systems

NOTE 1 – This specification is one part (the safety functions part) of the safety requirements specification (see 3.5.8) and contains the precise details of the safety functions that have to be performed by the safety-related systems.

NOTE 2 – Specifications may be documented in text, flow diagrams, matrices, logic diagrams, etc., providing that the safety functions are clearly conveyed.

3.5.10
safety integrity requirements specification
specification containing the safety integrity requirements of the safety functions that have to be performed by the safety-related systems

NOTE – This specification is one part (the safety integrity part) of the safety requirements specification (see 3.5.8).

3.5.11
safety-related software
software that is used to implement safety functions in a safety-related system

3.5.12
mode of operation
way in which a safety-related system is intended to be used, with respect to the frequency of demands made upon it, which may be either

- **low demand mode:** where the frequency of demands for operation made on a safety-related system is no greater than one per year and no greater than twice the proof-test frequency;
- **high demand or continuous mode:** where the frequency of demands for operation made on a safety-related system is greater than one per year or greater than twice the proof-check frequency

NOTE 1 – High demand or continuous mode covers those safety-related systems which implement continuous control to maintain functional safety.

NOTE 2 – The target failure measures for safety-related systems operating in low demand mode and high demand or continuous mode are defined in 3.5.13.

3.5.13
target failure measure
intended probability of dangerous mode failures to be achieved in respect of the safety integrity requirements, specified in terms of either

- the average probability of failure to perform the design function on demand (for a low demand mode of operation);
- the probability of a dangerous failure per hour (for a high demand or continuous mode of operation)

NOTE – The numerical values for the target failure measures are given in tables 2 and 3 of IEC 61508-1.

3.5.14
necessary risk reduction
risk reduction to be achieved by the E/E/PE safety-related systems, other technology safety-related systems and external risk reduction facilities in order to ensure that the tolerable risk is not exceeded

3.6 Anomalie, défaillance et erreur

3.6.1
anomalie
condition anormale qui peut entraîner une réduction de capacité ou la perte de capacité d'une unité fonctionnelle à accomplir une fonction requise

NOTE – Le VEI 191-05-01 définit «fault» (en français «panne») comme un état d'inaptitude à accomplir une fonction requise, en excluant l'inaptitude due à la maintenance préventive, à d'autres actions programmées ou à un manque de ressources extérieures. Le terme « fault » a donc deux sens différents rendus par deux termes français différents. Voir la figure 4 pour une illustration de ces deux points de vue.

[ISO/CEI 2382-14-01-10]

3.6.2
évitement des anomalies
utilisation de techniques et procédures destinées à éviter l'apparition d'anomalies durant chacune des phases du cycle de vie de sécurité du système relatif à la sécurité

3.6.3
tolérance aux anomalies
aptitude d'une unité fonctionnelle à continuer d'accomplir une fonction requise en présence d'anomalies ou d'erreurs

NOTE – La définition du terme «tolérant aux pannes» dans le VEI 191-15-05 ne prend en compte que les pannes de sous entités. Voir la note du terme «anomalie» en 3.6.1.

[ISO/CEI 2382-14-04-06]

3.6.4
défaillance
cessation de l'aptitude d'une unité fonctionnelle à accomplir une fonction requise

NOTE 1 – La définition du VEI 191-04-01 est la même avec des notes en plus.

[ISO/CEI 2382-14-01-11]

NOTE 2 – Voir la figure 4 pour la relation entre anomalies (pannes) et défaillances, tant dans la CEI 61508 que dans le VEI 60050(191).

NOTE 3 – L'accomplissement d'une fonction requise exclut nécessairement certains comportements, et certaines fonctions peuvent être spécifiées en termes de comportements à éviter. L'occurrence d'un comportement à éviter est une défaillance.

NOTE 4 – Les défaillances sont soit aléatoires (dans le matériel) soit systématiques (dans le logiciel ou le matériel), voir 3.6.5 et 3.6.6.

3.6.5
défaillances aléatoires du matériel
défaillances survenant de manière aléatoire et résultant de divers mécanismes de dégradation au sein du matériel

NOTE 1 – Il existe plusieurs mécanismes de dégradation se produisant à des fréquences différentes dans divers composants et puisque les tolérances de fabrication ont pour conséquence une défaillance des composants causée par ces mécanismes après des durées de fonctionnement inégales, les défaillances survenant dans un équipement comprenant plusieurs composants surviennent à des fréquences prévisibles, mais à des instants imprévisibles (car aléatoires).

NOTE 2 – L'une des différences majeures entre les défaillances aléatoires du matériel et les défaillances systématiques (voir 3.6.6) est que les taux de défaillance du système (ou toute autre mesure appropriée), générés par les défaillances aléatoires du matériel, peuvent être prédits avec une précision raisonnablement fiable, alors que les défaillances systématiques, de par leur nature même, ne peuvent être prédites avec précision. C'est-à-dire que les taux de défaillance du système issus des défaillances aléatoires de la machine peuvent être quantifiés de manière assez fiable, mais que les taux issus des défaillances systématiques ne peuvent être quantifiés avec précision.

3.6 Fault, failure and error

3.6.1
fault
abnormal condition that may cause a reduction in, or loss of, the capability of a functional unit to perform a required function

NOTE – IEV 191-05-01 defines "fault" as a state characterised by the inability to perform a required function, excluding the inability during preventative maintenance or other planned actions, or due to lack of external resources. See figure 4 for an illustration of these two points of view.

[ISO/IEC 2382-14-01-10]

3.6.2
fault avoidance
use of techniques and procedures which aim to avoid the introduction of faults during any phase of the safety lifecycle of the safety-related system

3.6.3
fault tolerance
ability of a functional unit to continue to perform a required function in the presence of faults or errors

NOTE – The definition in IEV 191-15-05 refers only to sub-item faults. See the note for the term fault in 3.6.1.

[ISO/IEC 2382-14-04-06]

3.6.4
failure
termination of the ability of a functional unit to perform a required function

NOTE 1 – The definition in IEV 191-04-01 is the same, with additional notes.

[ISO/IEC 2382-14-01-11]

NOTE 2 – See figure 4 for the relationship between faults and failures, both in IEC 61508 and IEV 50(191).

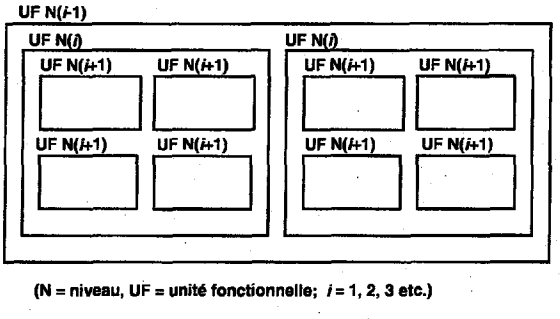
NOTE 3 – Performance of required functions necessarily excludes certain behaviour, and some functions may be specified in terms of behaviour to be avoided. The occurrence of such behaviour is a failure.

NOTE 4 – Failures are either random (in hardware) or systematic (in hardware or software), see 3.6.5 and 3.6.6.

3.6.5
random hardware failure
failure, occurring at a random time, which results from one or more of the possible degradation mechanisms in the hardware

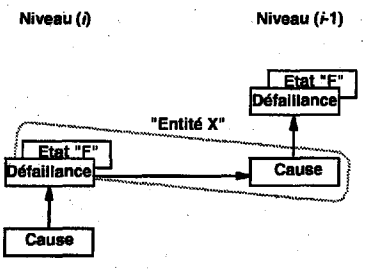
NOTE 1 – There are many degradation mechanisms occurring at different rates in different components and, since manufacturing tolerances cause components to fail due to these mechanisms after different times in operation, failures of equipment comprising many components occur at predictable rates but at unpredictable (i.e. random) times.

NOTE 2 – A major distinguishing feature between random hardware failures and systematic failures (see 3.6.6), is that system failure rates (or other appropriate measures), arising from random hardware failures, can be predicted with reasonable accuracy but systematic failures, by their very nature, cannot be accurately predicted. That is, system failure rates arising from random hardware failures can be quantified with reasonable accuracy but those arising from systematic failures cannot be accurately statistically quantified because the events leading to them cannot easily be predicted.

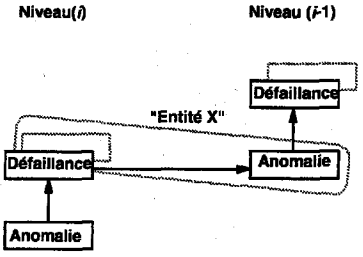


(N = niveau, UF = unité fonctionnelle; *i* = 1, 2, 3 etc.)

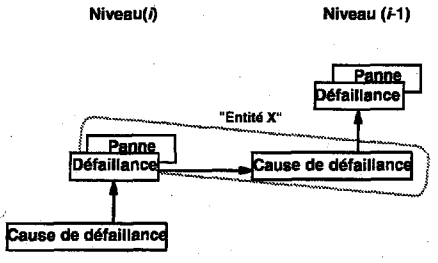
a) Configuration d'une unité fonctionnelle



b) Point de vue général



c) Point de vue de la CEI 61508 et de l'ISO/CEI 2382-14



d) Point de vue de la CEI 60050(191)

IEC 1 659/98

NOTE 1 – Comme le montre a), une unité fonctionnelle peut être considérée comme organisée hiérarchiquement en niveaux, dont chacun constitue à son tour une unité fonctionnelle. A l'intérieur de l'unité fonctionnelle de niveau *i*, une «cause» peut se manifester sous forme d'une erreur (un écart par rapport à la valeur ou à l'état correct) et, si elle n'est pas corrigée ou contournée, elle peut entraîner une défaillance de cette unité fonctionnelle, après laquelle l'unité se trouve dans un état «F» où elle n'est plus apte à accomplir une fonction requise, comme le montre b). Cet état «F» de l'unité fonctionnelle de niveau *i* peut à sont tour se manifester comme une erreur dans l'unité fonctionnelle de niveau (*i*-1) et, s'il n'est pas corrigé ou contourné, peut être la cause d'une défaillance de cette unité fonctionnelle niveau (*i*-1).

NOTE 2 – Dans cette chaîne de causes et d'effets, la même chose («entité X») peut être considérée comme un état (état «F») de l'unité fonctionnelle de niveau *i*, dans lequel cette unité se troue après défaillance, et comme la cause d'une défaillance de l'unité fonctionnelle de niveau (*i*-1). Cette «entité X» combine la notion de «fault» (en français «anomalie») dans l'ISO/CEI 2382-14, qui insiste sur l'aspect cause comme l'illustre c), et celle de «fault»(en français «panne être considérée comme un état (état «F») de l'unité fonctionnelle de niveau i, dans lequel cette unité se troue après défaillance, et comme la cause d'une défaillance de l'unité fonctionnelle de niveau (*i*-1). Cette «entité X» combine la notion de «fault» (en français «anomalie») dans l'ISO/CEI 2382-14, qui insiste sur l'aspect cause comme l'illustre c), et celle de «fault»(en français «panne) dans la CEI 60050(191), qui insiste sur l'aspect état comme l'illustre d). L'état «F» est appelé «panne» dans la CEI 60050(191), alors qu'il n'est pas défini dans la CEI 61508 et dans l'ISO/CEI 2382-14.

NOTE 3 – Dans certains cas, une défaillance peut être causée par un événement externe, tel que la foudre ou une perturbation électrostatique, plutôt que par une anomalie interne. De même, une anomalie (dans l'ISO/CEI 2382-14) ou une panne (dans la CEI 60050(191)) peut exister sans défaillance préalable, due par exemple à une conception inappropriée.

Figure 4 — Modèle de défaillance

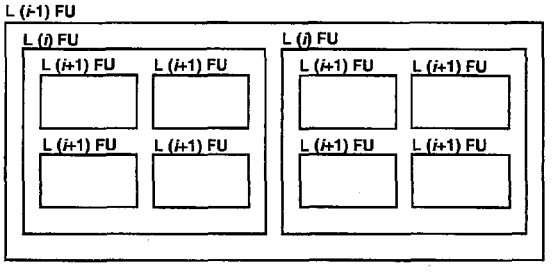
3.6.6
défaillance systématique

défaillance reliée de façon déterministe à une certaine cause, ne pouvant être éliminée que par une modification de la conception ou du processus de fabrication, des procédures d'exploitation, de la documentation ou d'autres facteurs appropriés

NOTE 1 – La maintenance corrective sans modification n'élimine pas, habituellement, la cause de la défaillance.

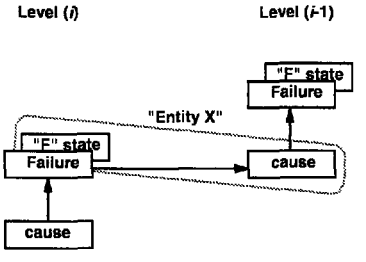
NOTE 2 – Une défaillance systématique peut être induite en simulant la cause de la défaillance.

[VEI 191-04-19, modifié]

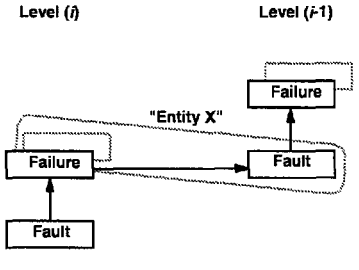


(L = level; i = 1, 2, 3 etc.; FU = functional unit)

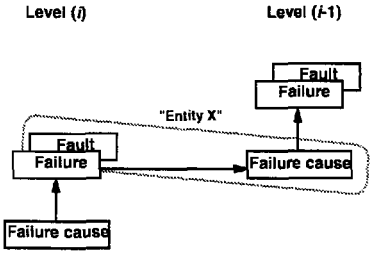
a) Configuration of a functional unit



b) Generalised view



c) From the point of view of IEC 61508 and ISO/IEC 2382-14



d) From the point of view of IEC 60050(191)

IEC 1 659/98

NOTE 1 – As shown in a), a functional unit can be viewed as a hierarchical composition of multiple levels, each of which can in turn be called a functional unit. In level (i), a "cause" may manifest itself as an error (a deviation from the correct value or state) within this level (i) functional unit, and, if not corrected or circumvented, may cause a failure of this functional unit, as a result of which it falls into an "F" state where it is no longer able to perform a required function (see b)). This "F" state of the level (I) functional unit may in turn manifest itself as an error in the level (i-1) functional unit and, if not corrected or circumvented, may cause a failure of this level (i-1) functional unit.

NOTE 2 – In this cause and effect chain, the same thing ("Entity X") can be viewed as a state ("F" state) of the level (i) functional unit into which it has fallen as a result of its failure, and also as the cause of the failure of the level (i-1) functional unit. This "Entity X" combines the concept of "fault" in IEC 61508 and ISO/IEC 2382-14, which emphasizes its cause aspect as illustrated in c), and that of "fault" in IEC 60050(191), which emphasizes its state aspect as illustrated in d). The "F" state is called fault in IEC 60050(191), whereas it is not defined in IEC 61508 and ISO/IEC 2382-14.

NOTE 3 – In some cases, a failure or an error may be caused by an external event such as lightning or electrostatic noise, rather than by an internal fault. Likewise, a fault (in both vocabularies) may exist without a prior failure. An example of such a fault is a design fault.

Figure 4 – Failure model

3.6.6
systematic failure

failure related in a deterministic way to a certain cause, which can only be eliminated by a modification of the design or of the manufacturing process, operational procedures, documentation or other relevant factors

NOTE 1 – Corrective maintenance without modification will usually not eliminate the failure cause.

NOTE 2 – A systematic failure can be induced by simulating the failure cause.

[IEV 191-04-19]

NOTE 3 – Citons comme exemples de causes de défaillances systématiques les erreurs humaines telles que:
- les erreurs de spécification des prescriptions de sécurité;
- les erreurs de conception, fabrication, installation, exploitation du matériel;
- les erreurs de conception, mise en oeuvre, etc. du logiciel.

NOTE 4 – Dans la présente norme, les défaillances d'un système relatif à la sécurité sont classées en défaillances aléatoires du matériel ou en défaillances systématiques (voir 3.6.4 et 3.6.5).

3.6.7
défaillance dangereuse
défaillance qui a la potentialité de mettre le système relatif à la sécurité dans un état dangereux ou dans l'impossibilité d'exécuter sa fonction

NOTE – Le fait que cette potentialité se réalise ou non peut dépendre de l'architecture du canal du système; pour les systèmes ayant plusieurs canaux pour accroître la sécurité, il est moins probable qu'une défaillance dangereuse du matériel conduise à un état dangereux de l'ensemble ou à un état dans lequel la fonction ne peut plus être exécutée.

3.6.8
défaillance en sécurité
défaillance qui n'a pas la potentialité de mettre le système relatif à la sécurité dans un état dangereux ou dans l'impossibilité d'exécuter sa fonction

NOTE – Le fait que cette potentialité se réalise ou non peut dépendre de l'architecture du canal du système; pour les systèmes ayant plusieurs canaux pour accroître la sécurité, il est moins probable qu'une défaillance en sécurité du matériel se traduise par un arrêt erroné.

3.6.9
défaillance dépendante
défaillance dont la probabilité ne peut être exprimée en tant que simple produit des probabilités non conditionnelles de chacun des événements individuels qui l'ont provoquée

NOTE – Deux événements A et B sont dépendants si, et seulement si, $P(z)$ étant la probabilité de l'événement z:

$$P(\text{A et B}) > P(\text{A}) \times P(\text{B})$$

3.6.10
défaillance de cause commune
défaillance résultant d'un ou plusieurs événements qui, provoquant des défaillances simultanées de deux ou plusieurs canaux séparés dans un système multicanal, conduit à la défaillance du système

3.6.11
erreur
écart ou discordance entre une valeur ou une condition calculée, observée ou mesurée, et la valeur ou la condition vraie, prescrite ou théoriquement correcte

NOTE – Adapté du VEI 191-05-24 en excluant les notes.

3.6.12
erreur humaine
action humaine ou absence d'intervention, qui peut produire un résultat non recherché.
[ISO/CEI 2382-14-01-09]

NOTE – Adapté du VEI 191-05-25 par l'ajout de « ou absence d'intervention ».

3.7 Activités liées au cycle de vie

3.7.1
cycle de vie de sécurité
activités nécessaires à la mise en oeuvre des systèmes relatifs à la sécurité, se déroulant au cours d'une période allant de la phase de conception d'un projet jusqu'au moment où aucun des systèmes E/E/PE relatifs à la sécurité, un système relatif à la sécurité basé sur une autre technologie et les dispositifs externes de réduction de risque ne sont plus disponibles à l'utilisation

NOTE 1 – Le terme «cycle de vie de sécurité fonctionnelle» est extrêmement plus précis, mais l'adjectif «fonctionnelle» n'est pas, dans ce cas, considéré nécessairement dans le contexte de la présente norme.

NOTE 2 – Les modèles de cycle de vie de sécurité utilisés dans cette norme sont spécifiés aux figures 2, 3 et 4 de la CEI 61508-1.

NOTE 3 – Examples of causes of systematic failures include human error in
- the safety requirements specification;
- the design, manufacture, installation, operation of the hardware;
- the design, implementation, etc. of the software.

NOTE 4 – In this standard, failures in a safety-related system are categorized as random hardware failures or systematic failures (see 3.6.4 and 3.6.5).

3.6.7
dangerous failure
failure which has the potential to put the safety-related system in a hazardous or fail-to-function state

NOTE – Whether or not the potential is realised may depend on the channel architecture of the system; in systems with multiple channels to improve safety, a dangerous hardware failure is less likely to lead to the overall dangerous or fail-to-function state.

3.6.8
safe failure
failure which does not have the potential to put the safety-related system in a hazardous or fail-to-function state

NOTE – Whether or not the potential is realised may depend on the channel architecture of the system; in systems with multiple channels to improve safety, a safe hardware failure is less likely to result in an erroneous shut-down.

3.6.9
dependent failure
failure whose probability cannot be expressed as the simple product of the unconditional probabilities of the individual events which caused it

NOTE – Two events A and B are dependent, where $P(z)$ is the probability of event z, only if:

$$P(\text{A and B}) > P(\text{A}) \times P(\text{B})$$

3.6.10
common cause failure
failure, which is the result of one or more events, causing coincident failures of two or more separate channels in a multiple channel system, leading to system failure

3.6.11
error
discrepancy between a computed, observed or measured value or condition and the true, specified or theoretically correct value or condition

NOTE – Adapted from IEV 191-05-24 by excluding the notes.

3.6.12
human error
mistake
human action or inaction that can produce an unintended result

[ISO/IEC 2382-14-01-09]

NOTE – Adapted from IEV 191-05-25 by the addition of "or inaction".

3.7 Lifecycle activities

3.7.1
safety lifecycle
necessary activities involved in the implementation of safety-related systems, occurring during a period of time that starts at the concept phase of a project and finishes when all of the E/E/PE safety-related systems, other technology safety-related systems and external risk reduction facilities are no longer available for use

NOTE 1 – The term "functional safety lifecycle" is strictly more accurate, but the adjective "functional" is not considered necessary in this case within the context of this standard.

NOTE 2 – The safety lifecycle models used in this standard are specified in figures 2, 3 and 4 of IEC 61508-1.

3.7.2
cycle de vie du logiciel
activités se déroulant au cours d'une période allant de la phase pendant laquelle le logiciel est conçu jusqu'au moment où le logiciel n'est définitivement plus utilisé

NOTE 1 – Le cycle de vie du logiciel inclut, typiquement, une phase de spécification, une phase de développement, une phase d'essai, une phase d'intégration, une phase d'installation et une phase de modification.
NOTE 2 – La maintenance du logiciel n'est pas possible. Le logiciel est plutôt modifiable.

3.7.3
gestion de configuration
discipline d'identification des composants d'un système évolutif ayant pour objectif de maîtriser les modifications de ces composants et de maintenir la continuité et la traçabilité tout au long du cycle de vie

NOTE – Pour les détails de la gestion de configuration du logiciel, voir C.5.24 de la CEI 61508-7.

3.7.4
analyse d'impact
activité de détermination de l'effet qu'une modification à une fonction ou à un composant d'un système a sur les autres fonctions ou les autres composants de ce système tout comme sur d'autres systèmes

NOTE – Dans le contexte du logiciel, voir C.5.23 de la CEI 61508-7.

3.8 Confirmation des mesures de sécurité

3.8.1
vérification
confirmation, par examen et apport de preuves tangibles, que les exigences spécifiées ont été satisfaites

NOTE 1 – Adapté de l'ISO 8402 en excluant les notes.
NOTE 2 – Dans le contexte de la présente norme, la «vérification» est l'activité qui consiste, pour chaque phase du cycle de vie de sécurité correspondant (général, E/E/PES et logiciel), à démontrer par analyse et/ou essai que, pour les entrées spécifiques, les éléments livrables remplissent en tout point les objectifs et prescriptions fixés pour la phase spécifique.

EXEMPLE Citons comme exemples d'activités de vérification:
– les revues relatives aux sorties d'une phase (documents concernant toutes les phases du cycle de vie de sécurité) destinées à assurer la conformité avec les objectifs et prescriptions de la phase, et prenant en compte les entrées spécifiques à cette phase;
– les revues de conception;
– les tests réalisés sur les produits mis au point afin de s'assurer que leur fonctionnement est conforme à leur spécification;
– les tests d'intégration réalisés lors de l'assemblage élément par élément de différentes parties d'un système, à partir d'essais d'environnement, afin de s'assurer que toutes les parties fonctionnent les unes avec les autres conformément aux spécifications.

3.8.2
validation
confirmation, par examen et apport de preuves tangibles que les exigences particulières pour un usage spécifique prévu sont satisfaites

NOTE 1 – Adapté de l'ISO 8402 en excluant les notes.
NOTE 2 – Dans la présente norme, il y a trois phases de validation:
– validation de sécurité générale (voir figure 2 de la CEI 61508-1);
– validation E/E/PES (voir figure 3 de la CEI 61508-1);
– validation du logiciel (voir figure 4 de la CEI 61508-1).
NOTE 3 – Dans la présente norme, la "validation" est l'activité qui consiste à démontrer que le système relatif à la sécurité, avant ou après installation correspond en tout point aux prescriptions contenues dans la spécification de sécurité de ce système sécurité. Ainsi, par exemple, la validation du logiciel consiste en la confirmation, par examen et apport de preuves tangibles, que le logiciel répond à la spécification des prescriptions de sécurité du logiciel.

3.7.2
software lifecycle
activities occurring during a period of time that starts when software is conceived and ends when the software is permanently disused

NOTE 1 A software lifecycle typically includes a requirements phase, development phase, test phase, integration phase, installation phase and a modification phase.

NOTE 2 – Software is not capable of being maintained; rather, it is modified.

3.7.3
configuration management
discipline of identifying the components of an evolving system for the purposes of controlling changes to those components and maintaining continuity and traceability throughout the lifecycle

NOTE – For details on software configuration management see C.5.24 of IEC 61508-7.

3.7.4
impact analysis
activity of determining the effect that a change to a function or component in a system will have to other functions or components in that system as well as to other systems

NOTE – In the context of software, see C.5.23 of IEC 61508-7.

3.8 Confirmation of safety measures

3.8.1
verification
confirmation by examination and provision of objective evidence that the requirements have been fulfilled

NOTE 1 – Adapted from ISO 8402 by excluding the notes.

NOTE 2 – In the context of this standard, verification is the activity of demonstrating for each phase of the relevant safety lifecycle (overall, E/E/PES and software), by analysis and/or tests, that, for the specific inputs, the deliverables meet in all respects the objectives and requirements set for the specific phase.

EXAMPLE Verification activities include

– reviews on outputs (documents from all phases of the safety lifecycle) to ensure compliance with the objectives and requirements of the phase, taking into account the specific inputs to that phase;

– design reviews;

– tests performed on the designed products to ensure that they perform according to their specification;

– integration tests performed where different parts of a system are put together in a step-by-step manner and by the performance of environmental tests to ensure that all the parts work together in the specified manner.

3.8.2
validation
confirmation by examination and provision of objective evidence that the particular requirements for a specific intended use are fulfilled

NOTE 1 – Adapted from ISO 8402 by excluding the notes.

NOTE 2 – In this standard there are three validation phases:

– overall safety validation (see figure 2 of IEC 61508-1);

– E/E/PES validation (see figure 3 of IEC 61508-1);

– software validation (see figure 4 of IEC 61508-1).

NOTE 3 – Validation is the activity of demonstrating that the safety-related system under consideration, before or after installation, meets in all respects the safety requirements specification for that safety-related system. Therefore, for example, software validation means confirming by examination and provision of objective evidence that the software satisfies the software safety requirements specification.

3.8.3
évaluation de la sécurité fonctionnelle
recherche destinée à obtenir la certitude, à partir des preuves recueillies, de l'état de sécurité fonctionnelle atteint par un ou plusieurs systèmes relatifs à la sécurité E/E/PE, une ou plusieurs autres technologies de système relatif à la sécurité ou un ou plusieurs dispositifs externes de réduction de risque

3.8.4
audit de la sécurité fonctionnelle
examen systématique et indépendant destiné à déterminer si les procédures spécifiques aux prescriptions sur la sécurité fonctionnelle sont conformes aux procédures prévues, sont effectivement mises en oeuvre et permettent d'atteindre les objectifs spécifiés

NOTE – Un audit de la sécurité fonctionnelle peut être mené dans le cadre d'une évaluation de la sécurité fonctionnelle.

3.8.5
test périodique
test périodique destiné à détecter les défaillances d'un système relatif à la sécurité de telle sorte que, lorsque nécessaire, le système puisse être rétabli dans une condition "comme neuf" ou dans une condition aussi proche que possible de celle-ci

NOTE – L'efficacité d'un test périodique dépend de jusqu'à quel point le système est rétabli dans une condition «comme neuf». Pour que le test soit complètement efficace, il est nécessaire de détecter 100 % des défaillances dangereuses. Bien qu'en pratique il ne soit pas facile d'atteindre 100 % pour tout système autre qu'un système E/E/PE relatif à la sécurité de faible complexité, il convient de garder cet objectif. Au minimum, toutes les fonctions de sécurité qui sont exécutées sont contrôlées conformément aux spécifications des prescriptions de sécurité de l'E/E/PES. Si des canaux séparés sont utilisés, ces tests sont réalisés séparément pour chacun des canaux.

3.8.6
couverture du diagnostic
fraction exprimant la décroissance de la probabilité de défaillance dangereuse du matériel résultant du fonctionnement des tests de diagnostic automatique

NOTE 1 – Cette définition peut également être représentée selon l'équation suivante dans laquelle *DC* est la couverture du diagnostic, λ_{DD} est la probabilité de détection d'une défaillance dangereuse et λ_{total} est la probabilité de toutes les défaillances dangereuses:

$$DC = \frac{\sum \lambda_{DD}}{\sum \lambda_{total}}$$

NOTE 2 – La couverture du diagnostic peut se rapporter à tout ou partie du système relatif à la sécurité. Elle peut, par exemple, être disponible pour les capteurs et/ou le système logique et/ou les éléments terminaux.

NOTE 3 – Le terme couverture de diagnostic en sécurité, ou couverture de diagnostic incluant les défaillances en sécurité, est utilisé pour décrire respectivement la décroissance de la probabilité de défaillance en sécurité du matériel ou bien d'une défaillance en sécurité et/ou dangereuse du matériel, résultant du fonctionnement des tests de diagnostic automatique.

3.8.7
intervalle entre tests de diagnostic
intervalle de temps entre les tests en ligne qui permettent de détecter les anomalies d'un système relatif à la sécurité, la couverture du diagnostic étant spécifiée

3.8.8
détecté
révélé
déclaré
se rapporte au matériel et signifie détecté par les tests de diagnostic, les tests périodiques, une intervention de l'opérateur (par exemple une inspection physique et des tests manuels), ou lors de l'exploitation normale

EXEMPLE Ces adjectifs sont utilisés dans les cas d'anomalie détectée et de défaillance détectée.

3.8.3
functional safety assessment
investigation, based on evidence, to judge the functional safety achieved by one or more E/E/PE safety-related systems, other technology safety-related systems or external risk reduction facilities

3.8.4
functional safety audit
systematic and independent examination to determine whether the procedures specific to the functional safety requirements to comply with the planned arrangements are implemented effectively and are suitable to achieve the specified objectives

NOTE – A functional safety audit may be carried out as part of a functional safety assessment.

3.8.5
proof test
periodic test performed to detect failures in a safety-related system so that, if necessary, the system can be restored to an "as new" condition or as close as practical to this condition

NOTE – The effectiveness of the proof test will be dependent upon how close to the "as new" condition the system is restored. For the proof test to be fully effective, it will be necessary to detect 100 % of all dangerous failures. Although in practice 100 % is not easily achieved for other than low-complexity E/E/PE safety-related systems, this should be the target. As a minimum, all the safety functions which are executed are checked according to the E/E/PES safety requirements specification. If separate channels are used, these tests are done for each channel separately.

3.8.6
diagnostic coverage
fractional decrease in the probability of dangerous hardware failure resulting from the operation of the automatic diagnostic tests

NOTE 1 – The definition may also be represented in terms of the following equation, where *DC* is the diagnostic coverage, λ_{DD} is the probability of detected dangerous failures and λ_{total} is the probability of total dangerous failures:

$$DC = \frac{\sum \lambda_{DD}}{\sum \lambda_{total}}$$

NOTE 2 – Diagnostic coverage may exist for the whole or parts of a safety-related system. For example diagnostic coverage may exist for sensors and/or logic system and/or final elements.

NOTE 3 – The term safe diagnostic coverage, or diagnostic coverage including safe failures, is used to describe respectively the fractional decrease in the probability of safe hardware failure, or of both safe and dangerous hardware failures, resulting from the operation of the automatic diagnostic tests.

3.8.7
diagnostic test interval
interval between on-line tests to detect faults in a safety-related system that have a specified diagnostic coverage

3.8.8
detected
revealed
overt
in relation to hardware, detected by the diagnostic tests, proof tests, operator intervention (for example physical inspection and manual tests), or through normal operation

EXAMPLE These adjectives are used in detected fault and detected failure.

3.8.9
non détecté
non révélé
non déclaré
se rapporte au matériel et signifie non détecté par les tests de diagnostic, les tests périodiques, une intervention de l'opérateur (par exemple une inspection physique et des tests manuels), ou lors de l'exploitation normale

EXEMPLE Ces adjectifs sont utilisés dans les cas d'anomalie non détectée et de défaillance non détectée.

3.8.10
personne indépendante
personne distinctement séparée de celles responsables des activités qui se déroulent lors des phases du cycle de vie de sécurité des E/E/PES ou du logiciel, chargée de l'évaluation de la sécurité fonctionnelle ou de la validation et qui n'a pas de responsabilité directe dans ces activités

3.8.11
département indépendant
département distinctement séparé de ceux responsables des activités qui se déroulent lors des phases du cycle de vie de sécurité des E/E/PES ou du logiciel, chargé de l'évaluation de la sécurité fonctionnelle ou de la validation

3.8.12
organisation indépendante
organisation distinctement séparée, par sa direction et ses autres ressources, de celles responsables des activités qui se déroulent lors des phases du cycle de vie de sécurité des E/E/PES ou du logiciel, chargée de l'évaluation de la sécurité fonctionnelle ou de la validation

3.8.13
animation
exploitation simulée du logiciel du système (ou de toute partie importante du système), destinée à mettre en évidence les aspects significatifs du comportement du système, appliquée à une spécification d'exigences dans une forme appropriée ou à une représentation appropriée de haut niveau de la conception du système

NOTE – L'animation peut donner une confiance supplémentaire en ce que le système remplit les exigences réelles car elle améliore la prise de conscience humaine du comportement spécifié.

3.8.14
test dynamique
exécution du logiciel et/ou fonctionnement du matériel de manière maîtrisée et systématique, de façon à démontrer l'existence du comportement requis et l'absence de comportement non désiré

NOTE – Le test dynamique diffère de l'analyse statique, qui n'exige pas l'exécution du logiciel.

3.8.15
simulateur de test
moyen capable de simuler (jusqu'à un certain degré d'utilité) l'environnement du logiciel ou du matériel en exploitation pendant le développement, en appliquant des cas de test au logiciel et en enregistrant les réponses

NOTE – Le simulateur de test peut aussi comprendre des générateurs de cas de test et des moyens de vérification des résultats de test (soit automatiques par comparaison à des valeurs réputées correctes, soit par analyse manuelle).

3.8.9
undetected
unrevealed
covert
in relation to hardware, undetected by the diagnostic tests, proof tests, operator intervention (for example physical inspection and manual tests), or through normal operation

EXAMPLE These adjectives are used in undetected fault and undetected failure.

3.8.10
independent person
person who is separate and distinct from the activities which take place during the specific phase of the overall, E/E/PES or software safety lifecycle that is subject to the functional safety assessment or validation, and does not have direct responsibility for those activities

3.8.11
independent department
department which is separate and distinct from the departments responsible for the activities which take place during the specific phase of the overall, E/E/PES or software safety lifecycle that is subject to the functional safety assessment or validation

3.8.12
independent organisation
organisation which is separate and distinct, by management and other resources, from the organisations responsible for the activities which take place during the specific phase of the overall, E/E/PES or software safety lifecycle that is subject to the functional safety assessment or validation

3.8.13
animation
simulated operation of the software system (or of some significant portion of the system) to display significant aspects of the behaviour of the system, for instance applied to a requirements specification in an appropriate format or an appropriate high-level representation of the system design

NOTE – Animation can give extra confidence that the system meets the real requirements because it improves human recognition of the specified behaviour.

3.8.14
dynamic testing
executing software and/or operating hardware in a controlled and systematic way, so as to demonstrate the presence of the required behaviour and the absence of unwanted behaviour

NOTE – Dynamic testing contrasts with static analysis, which does not require the software to be executed.

3.8.15
test harness
facility that is capable of simulating (to some useful degree) the operating environment of software or hardware under development, by applying test cases to the software and recording the response

NOTE – The test harness may also include test case generators and facilities to verify the test results (either automatically against values that are accepted as correct or by manual analysis).

Annexe A
(informative)

Bibliographie

CEI 61131-3:1993, *Automates programmables – Partie 3: Langages de programmation*

CEI 61151:1992, *Instrumentation nucléaire – Amplificateurs et préamplificateurs utilisés avec des détecteurs de rayonnements ionisants – Méthodes d'essai*

ISO/CEI 2382-1:1993, *Technologies de l'information – Vocabulaire – Partie 1: Termes fondamentaux*

ISO 9000-3:1991, *Normes pour la gestion de la qualité et l'assurance de la qualité – Partie 3: Lignes directrices pour l'application de l'ISO 9001 au développement, à la mise à disposition et à la maintenance du logiciel*

ANSI/ISA 584:1996, *Application of Safety Instrumented Systems for the Process Industries*

Annex A
(informative)

Bibliography

IEC 61131-3:1993, *Programmable controllers – Part 3: Programming languages*

IEC 61151:1992, *Nuclear instrumentation – Amplifiers and preamplifiers used with detectors of ionizing radiation – Test procedures*

ISO/IEC 2382-1:1993, *Information technology – Vocabulary – Part 1: Fundamental terms*

ISO 9000-3:1991, *Quality management and quality assurance standards – Part 3: Guidelines for the application of ISO 9001 to the development, supply and maintenance of software*

ANSI/ISA 584:1996, *Application of Safety Instrumented Systems for the Process Industries*

INDEX

analyse d'impact 3.7.4
animation 3.8.13
anomalie 3.6.1
architecture 3.3.5
audit de la sécurité fonctionnelle 3.8.4
canal 3.3.8
couverture du diagnostic 3.8.6
cycle de vie de sécurité 3.7.1
cycle de vie du logiciel 3.7.2
déclaré 3.8.8
défaillance 3.6.4
défaillance dangereuse 3.6.7
défaillance de cause commune 3.6.10
défaillance dépendante 3.6.9
défaillance en sécurité 3.6.8
défaillances aléatoires du matériel 3.6.5
défaillance systématique 3.6.6
département indépendant 3.8.11
détecté 3.8.8
dispositifs externes de réduction de risque 3.4.3
diversité 3.3.9
dommage 3.1.1
électrique/électronique/électronique programmable (E/E/PE) 3.2.6
électronique programmable (PE) 3.2.5
équipement commandé (EUC) 3.2.3
erreur humaine 3.6.12
erreur 3.6.11
état de sécurité 3.1.10
évaluation de la sécurité fonctionnelle 3.8.3
événement dangereux 3.1.4
évitement des anomalies 3.6.2
fonction de sécurité 3.5.1
gestion de configuration 3.7.3
intégrité de sécurité 3.5.2
intégrité de sécurité du logiciel 3.5.3
intégrité de sécurité du matériel 3.5.5
intégrité de sécurité systématique 3.5.4
intervalle entre tests de diagnostic 3.8.7
langage de variabilité limitée 3.2.7
logiciel 3.2.2
logiciel de sécurité 3.5.11
mauvais usage raisonnablement prévisible 3.1.11
mesure cible des défaillances 3.5.13
mode de fonctionnement 3.5.12
module 3.3.6
module logiciel 3.3.7

INDEX

animation 3.8.13
architecture 3.3.5
channel 3.3.8
common cause failure 3.6.10
configuration management 3.7.3
covert 3.8.9
dangerous failure 3.6.7
dependent failure 3.6.9
detected 3.8.8
diagnostic coverage 3.8.6
diagnostic test interval 3.8.7
diversity 3.3.9
dynamic testing 3.8.14
electrical/electronic/programmable electronic (E/E/PE) 3.2.6
electrical/electronic/programmable electronic system (E/E/PES) 3.3.3
equipment under control (EUC) 3.2.3
error 3.6.11
EUC control system 3.3.4
EUC risk 3.2.4
external risk reduction facility 3.4.3
failure 3.6.4
fault 3.6.1
fault avoidance 3.6.2
fault tolerance 3.6.3
functional safety 3.1.9
functional safety assessment 3.8.3
functional safety audit 3.8.4
functional unit 3.2.1
hardware safety integrity 3.5.5
harm 3.1.1
hazard 3.1.2
hazardous event 3.1.4
hazardous situation 3.1.3
human error 3.6.12
impact analysis 3.7.4
independent department 3.8.11
independent organisation 3.8.12
independent person 3.8.10
limited variability 3.2.7
logic system 3.4.5
low-complexity E/E/PE safety-related system 3.4.4
mistake 3.6.12
mode of operation 3.5.12
module 3.3.6

niveau d'intégrité de sécurité (SIL) 3.5.6
niveau d'intégrité de sécurité du logiciel 3.5.7
non déclaré 3.8.9
non détecté 3.8.9
non révélé 3.8.9
organisation indépendante 3.8.12
personne indépendante 3.8.10
phénomène dangereux 3.1.2
redondance 3.3.10
réduction de risque nécessaire 3.5.14
révélé 3.8.8
risque 3.1.5
risque EUC 3.2.4
risque tolérable 3.1.6
risque résiduel 3.1.7
sécurité fonctionnelle 3.1.9
sécurité 3.1.8
simulateur de test 3.8.15
situation dangereuse 3.1.3
spécification des prescriptions concernant l'intégrité de sécurité 3.5.10
spécification des prescriptions concernant la sécurité 3.5.8
spécification des prescriptions concernant les fonctions de sécurité 3.5.9
système 3.3.1
système de commande de l'EUC 3.3.4
système E/E/PE relatif à la sécurité de faible complexité 3.4.4
système électrique/électronique/électronique programmable (E/E/PES) 3.3.3
système électronique programmable (PES) 3.3.2
système logique 3.4.5
système relatif à la sécurité 3.4.1
système relatif à la sécurité basé sur une autre technologie 3.4.2
test dynamique 3.8.14
test périodique 3.8.5
tolérance aux anomalies 3.6.3
unité fonctionnelle 3.2.1
validation 3.8.2
vérification 3.8.1

necessary risk reduction 3.5.14
other technology safety-related system 3.4.2
overt 3.8.8
programmable electronic 3.2.5
programmable electronic system (PES) 3.3.2
proof test 3.8.5
random hardware failure 3.6.5
reasonably foreseeable misuse 3.1.11
redundancy 3.3.10
revealed 3.8.8
risk 3.1.5
safe failure 3.6.8
safe state 3.1.10
safety 3.1.8
safety function 3.5.1
safety functions requirements specification 3.5.9
safety integrity 3.5.2
safety integrity level (SIL) 3.5.6
safety integrity requirements specification 3.5.10
safety lifecycle 3.7.1
safety-related software 3.5.11
safety-related system 3.4.1
safety requirements specification 3.5.8
software 3.2.2
software lifecycle 3.7.2
software module 3.3.7
software safety integrity 3.5.3
software safety integrity level 3.5.7
system 3.3.1
systematic failure 3.6.6
systematic safety integrity 3.5.4
target failure measure 3.5.13
test harness 3.8.15
tolerable risk 3.1.6
undetected 3.8.9
unrevealed 3.8.9
validation 3.8.2
verification 3.8.1

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.

A Prioritaire

Nicht frankieren
Ne pas affranchir

Non affrancare
No stamp required

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 2-8318-4584-X

ICS 25.040.40; 29.020

Typeset and printed by the IEC Central Office
GENEVA, SWITZERLAND