IEC 61508-4

Edition 2.0 2010-04

INTERNATIONAL STANDARD

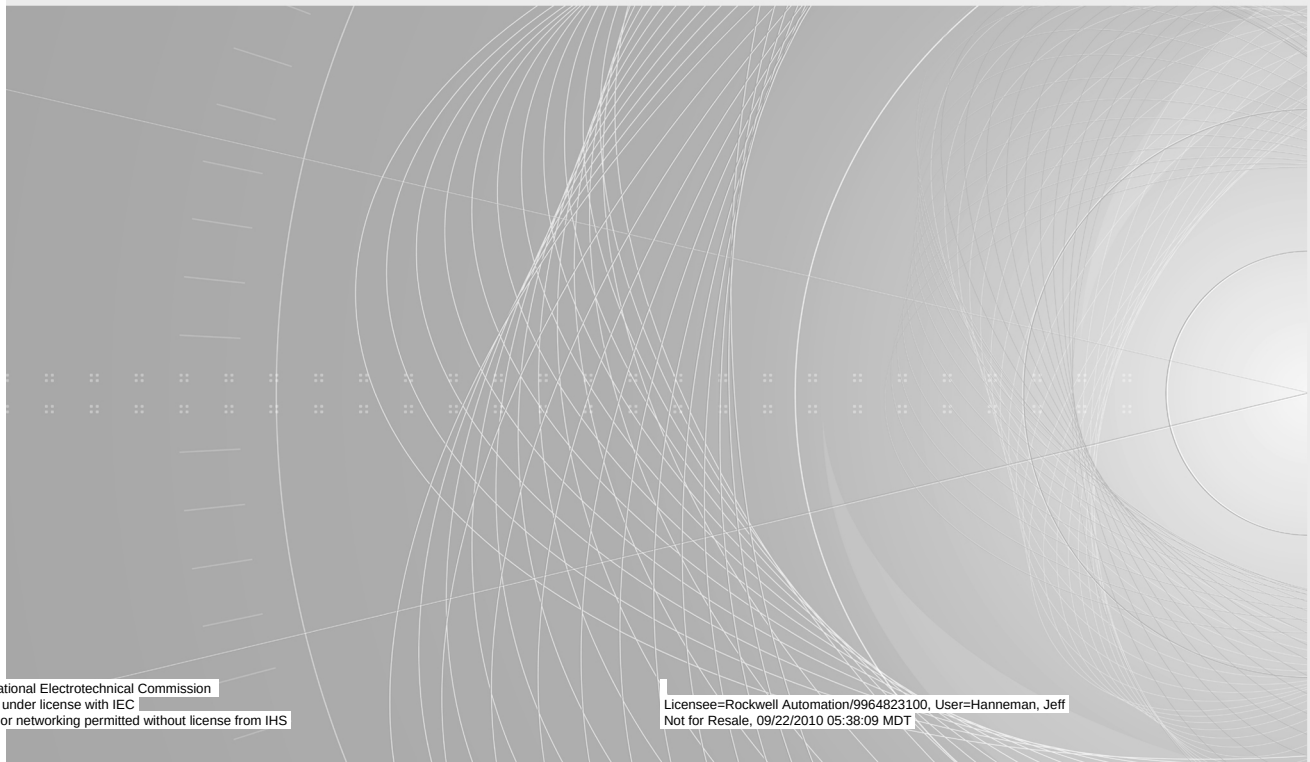
NORME INTERNATIONALE

BASIC SAFETY PUBLICATION

PUBLICATION FONDAMENTALE DE SÉCURITÉ

Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 4: Definitions and abbreviations

Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 4: Définitions et abréviations



IEC 61508-4:2010

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland
Email: inmail@iec.ch
Web: www.iec.ch

About the IEC

The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications

The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigenda or an amendment might have been published.

- Catalogue of IEC publications: www.iec.ch/searchpub
The IEC on-line Catalogue enables you to search by a variety of criteria (reference number, text, technical committee,…). It also gives information on projects, withdrawn and replaced publications.
- IEC Just Published: www.iec.ch/online_news/justpub
Stay up to date on all new IEC publications. Just Published details twice a month all new publications released. Available on-line and also by email.
- Electropedia: www.electropedia.org
The world's leading online dictionary of electronic and electrical terms containing more than 20 000 terms and definitions in English and French, with equivalent terms in additional languages. Also known as the International Electrotechnical Vocabulary online.
- Customer Service Centre: www.iec.ch/webstore/custserv
If you wish to give us your feedback on this publication or need further assistance, please visit the Customer Service Centre FAQ or contact us:
Email: csc@iec.ch
Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00

A propos de la CEI

La Commission Electrotechnique Internationale (CEI) est la première organisation mondiale qui élabore et publie des normes internationales pour tout ce qui a trait à l'électricité, à l'électronique et aux technologies apparentées.

A propos des publications CEI

Le contenu technique des publications de la CEI est constamment revu. Veuillez vous assurer que vous possédez l'édition la plus récente, un corrigendum ou amendement peut avoir été publié.

- Catalogue des publications de la CEI: www.iec.ch/searchpub/cur_fut-f.htm
Le Catalogue en-ligne de la CEI vous permet d'effectuer des recherches en utilisant différents critères (numéro de référence, texte, comité d'études,…). Il donne aussi des informations sur les projets et les publications retirées ou remplacées.
- Just Published CEI: www.iec.ch/online_news/justpub
Restez informé sur les nouvelles publications de la CEI. Just Published détaille deux fois par mois les nouvelles publications parues. Disponible en-ligne et aussi par email.
- Electropedia: www.electropedia.org
Le premier dictionnaire en ligne au monde de termes électroniques et électriques. Il contient plus de 20 000 termes et définitions en anglais et en français, ainsi que les termes équivalents dans les langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International en ligne.
- Service Clients: www.iec.ch/webstore/custserv/custserv_entry-f.htm
Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions, visitez le FAQ du Service clients ou contactez-nous:
Email: csc@iec.ch
Tél.: +41 22 919 02 11
Fax: +41 22 919 03 00

IEC 61508-4

Edition 2.0 2010-04

INTERNATIONAL STANDARD

NORME INTERNATIONALE

BASIC SAFETY PUBLICATION

PUBLICATION FONDAMENTALE DE SÉCURITÉ

Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 4: Definitions and abbreviations

Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 4: Définitions et abréviations

INTERNATIONAL ELECTROTECHNICAL COMMISSION

COMMISSION ELECTROTECHNIQUE INTERNATIONALE

PRICE CODE
CODE PRIX V

ICS 25.040.40; 29.020

ISBN 978-2-88910-527-4

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

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

Part 4: Definitions and abbreviations

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
6) All users should ensure that they have the latest edition of this publication.
7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

International Standard IEC 61508-4 has been prepared by subcommittee 65A: System aspects, of IEC technical committee 65: Industrial-process measurement, control and automation.

This second edition cancels and replaces the first edition published in 1998. This edition constitutes a technical revision.

This edition has been subject to a thorough review and incorporates many comments received at the various revision stages.

It has the status of a basic safety publication according to IEC Guide 104.

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

FDIS	Report on voting
65A/551/FDIS	65A/575/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.

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

A list of all parts of the IEC 61508 series, published under the general title *Functional safety of electrical / electronic / programmable electronic safety-related systems*, can be found on the IEC website.

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

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

INTRODUCTION

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

This International Standard sets out a generic approach for all safety lifecycle activities for systems comprised of electrical and/or electronic and/or programmable electronic (E/E/PE) elements 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 product and application sector international standards based on the IEC 61508 series.

NOTE 1 Examples of product and application sector international standards based on the IEC 61508 series are given in the Bibliography (see references [1], [2] and [3]).

In most situations, safety is achieved by a number of 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 E/E/PE safety-related systems, it may also provide a framework within which safety-related systems based on other technologies may be considered.

It is recognized that there is a great variety of applications using E/E/PE safety-related systems 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 product and application sector international standards and in revisions of those that already exist.

This International Standard

– considers all relevant overall, E/E/PE system and software safety lifecycle phases (for example, from initial concept, though design, implementation, operation and maintenance to decommissioning) when E/E/PE systems 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 product and application sector international standards, dealing with E/E/PE safety-related systems, to be developed; the development of product and application sector international standards, within the framework of this standard, should lead to a high level of consistency (for example, of underlying principles, terminology etc.) both within application sectors and across application sectors; this will have both safety and economic benefits;
– provides a method for the development of the safety requirements specification necessary to achieve the required functional safety for E/E/PE safety-related systems;
– adopts a risk-based approach by which the safety integrity requirements can be determined;
– introduces 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;

NOTE 2 The standard does not specify the safety integrity level requirements for any safety function, nor does it mandate how the safety integrity level is determined. Instead it provides a risk-based conceptual framework and example techniques.

– sets target failure measures for safety functions carried out by E/E/PE safety-related systems, which are linked to the safety integrity levels;

– sets a lower limit on the target failure measures for a safety function carried out by 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 a dangerous failure on demand of 10^{-5};

  – a high demand or a continuous mode of operation, the lower limit is set at an average frequency of a dangerous failure of 10^{-9} [h^{-1}];

NOTE 3 A single E/E/PE safety-related system does not necessarily mean a single-channel architecture.

NOTE 4 It may be possible to achieve designs of safety-related systems with lower values for the target safety integrity for non-complex systems, but these limits are considered to represent what can be achieved for relatively complex systems (for example programmable electronic safety-related systems) at the present time.

– sets requirements for the avoidance and control of systematic faults, which are based on experience and judgement from practical experience gained in industry. Even though the probability of occurrence of systematic failures cannot in general be quantified the standard does, however, allow a claim to be made, for a specified safety function, that the target failure measure associated with the safety function can be considered to be achieved if all the requirements in the standard have been met;

– introduces systematic capability which applies to an element with respect to its confidence that the systematic safety integrity meets the requirements of the specified safety integrity level;

– adopts a broad range of principles, techniques and measures to achieve functional safety for E/E/PE safety-related systems, but does not explicitly use the concept of fail safe However**,** the concepts of “fail safe” and “inherently safe” principles may be applicable and adoption of such concepts is acceptable providing the requirements of the relevant clauses in the standard are met.

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 the IEC 61508 series of standards.

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

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 3.4.3 of IEC 61508-4). 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. IEC 61508-1, IEC 61508-2, IEC 61508-3 and IEC 61508-4 are also intended for use as stand-alone publications. The horizontal safety function of this international standard does not apply to medical equipment in compliance with the IEC 60601 series.

1.4 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.

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

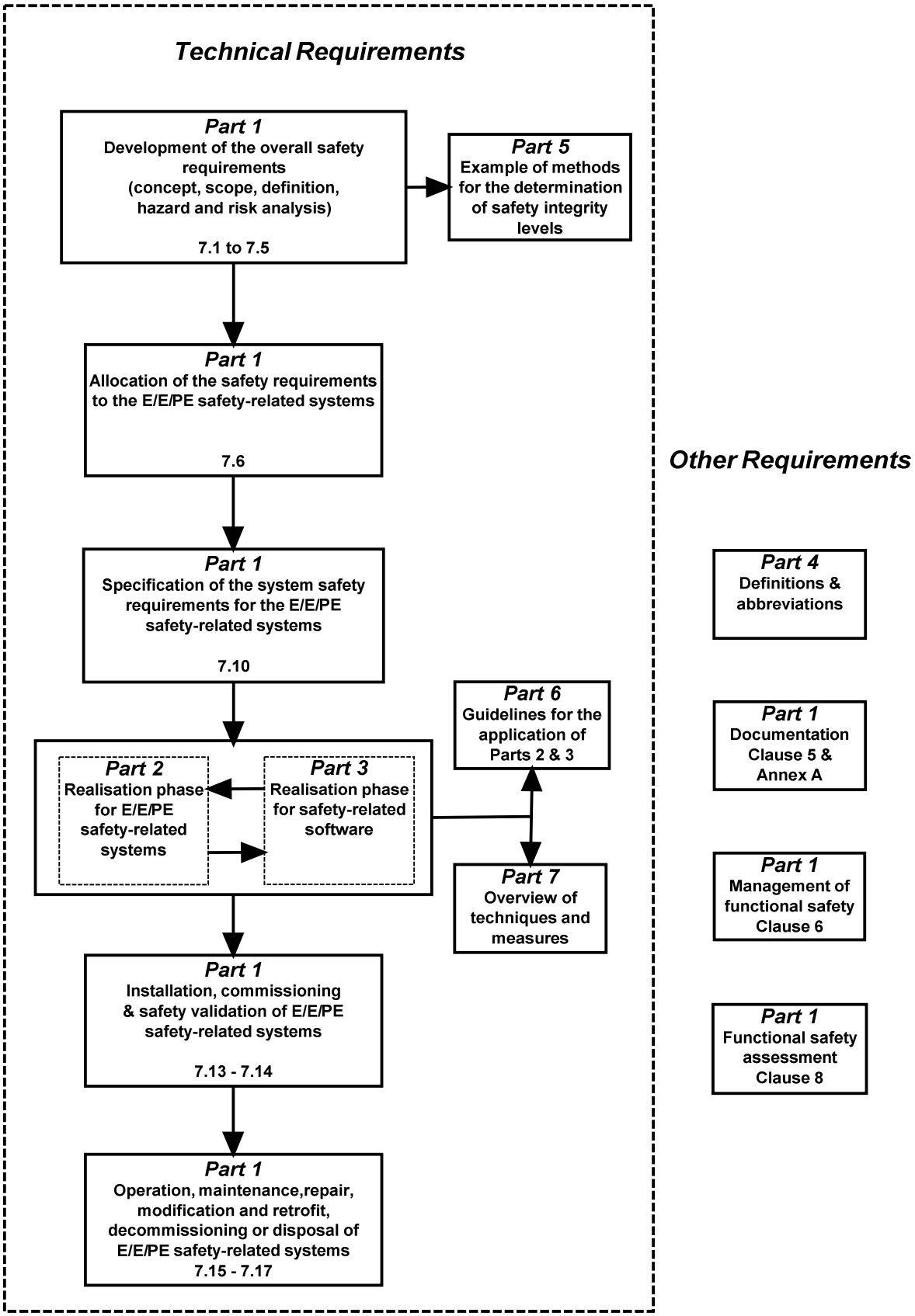


Figure 1 – Overall framework of the IEC 61508 series

2 Normative references

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

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

ISO/IEC Guide 51:1999, *Safety aspects – Guidelines for their inclusion in standards*

3 Definitions and abbreviations

For the purposes of this document, the definitions and the abbreviations given in Table 1 below, as well as the following apply.

Table 1 – Abbreviations used in this standard

Abbreviation	Full expression	Definition and/or explanation of term
ALARP	As Low As Reasonably Practicable	IEC 61508-5, Annex C
ASIC	Application Specific Integrated Circuit	3.2.15
CCF	Common Cause Failure	3.6.10
CPLD	Complex Programmable Logic Device	
DC	Diagnostic Coverage	3.8.6
(E)EPLD	(Electrically) Erasable Programmable Logic Device	
E/E/PE	Electrical/Electronic/Programmable Electronic	3.2.13, example: E/E/PE safety-related system
E/E/PE (system)	Electrical/Electronic/Programmable Electronic System	3.3.2
EEPROM	Electrically Erasable Programmable Read-Only Memory	
EPROM	Erasable Programmable Read-Only Memory	
EUC	Equipment Under Control	3.2.1
FPGA	Field Programmable Gate Array	
GAL	Generic Array Logic	
HFT	Hardware Fault Tolerance	7.4.4 of IEC 61508-2
MooN	M out of N channel architecture (for example 1oo2 is 1 out of 2 architecture, where either of the two channels can perform the safety function)	IEC 61508-6, Annex B
MooND	M out of N channel architecture with Diagnostics	IEC 61508-6, Annex B
MTBF	Mean Time Between Failures	3.6.19, NOTE 3
MTTR	Mean Time To Repair	3.6.21
MRT	Mean Repair Time	3.6.22
PAL	Programmable Array Logic	
PE	Programmable Electronic	3.2.12
PE(system)	Programmable Electronic	3.3.1
PFD	Probability of Dangerous Failure on Demand	3.6.17
PFD_{avg}	Average Probability of dangerous Failure on Demand	3.6.18
PFH	Average frequency of dangerous failure [h^{-1}]	3.6.19
PLA	Programmable Logic Array	

Abbreviation	Full expression	Definition and/or explanation of term
PLC	Programmable Logic Controller	IEC 61508-6, Annex E
PLD	Programmable Logic Device	
PLS	Programmable Logic Sequencer	
PML	Programmable Macro Logic	
RAM	Random Access Memory	
ROM	Read-Only Memory	
SFF	Safe Failure Fraction	3.6.15
SIL	Safety Integrity Level	3.5.8
VHDL	Very High Speed Integrated Circuit Hardware Description Language	IEC 61508-2, Annex F, Note 5

3.1 Safety terms

3.1.1
harm
physical injury or damage to the health of people or damage to property or the environment

[ISO/IEC Guide 51:1999, definition 3.3]

3.1.2
hazard
potential source of harm

[ISO/IEC Guide 51:1999, definition 3.5]

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 people, property or the environment are exposed to one or more hazards

[ISO/IEC Guide 51:1999, definition 3.6, modified]

3.1.4
hazardous event
event that may result in harm

NOTE Whether or not a hazardous event results in harm depends on whether people, property or the environment are exposed to the consequence of the hazardous event and, in the case of harm to people, whether any such exposed people can escape the consequences of the event after it has occurred.

3.1.5
harmful event
occurrence in which a hazardous situation or hazardous event results in harm

NOTE Adapted from ISO/IEC Guide 51, definition 3.4, to allow for a hazardous event.

3.1.6
risk
combination of the probability of occurrence of harm and the severity of that harm

[ISO/IEC Guide 51:1999, definition 3.2]

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

3.1.7
tolerable risk
risk which is accepted in a given context based on the current values of society

[ISO/IEC Guide 51:1999, definition 3.7]

NOTE See Annex C of IEC 61508-5.

3.1.8
residual risk
risk remaining after protective measures have been taken

[ISO/IEC Guide 51:1999, definition 3.9]

3.1.9
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 harmful event in which E/E/PE safety-related systems and other risk reduction measures 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 and other risk reduction measures.

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

3.1.10
target risk
risk that is intended to be reached for a specific hazard taking into account the EUC risk together with the E/E/PE safety-related systems and the other risk reduction measures

3.1.11
safety
freedom from unacceptable risk

[ISO/IEC Guide 51:1999, definition 3.1]

3.1.12
functional safety
part of the overall safety relating to the EUC and the EUC control system that depends on the correct functioning of the E/E/PE safety-related systems and other risk reduction measures

3.1.13
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.

3.1.14
reasonably foreseeable misuse
use of a product, process or service in a way not intended by the supplier, but which may result from readily predictable human behaviour

[ISO/IEC Guide 51:1999, definition 3.14]

3.2 Equipment and devices

3.2.1
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.

3.2.2
environment
all relevant parameters that can affect the achievement of functional safety in the specific application under consideration and in any safety lifecycle phase

NOTE This would include, for example, physical environment, operating environment, legal environment and maintenance environment.

3.2.3
functional unit
entity of hardware or software, or both, capable of accomplishing a specified purpose
[ISO/IEC 2382-1, 01-01-40]

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

3.2.4
application
task related to the EUC rather than to the E/E/PE system

3.2.5
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/IEC 2382-1 (reference [7] in the Bibliography) by the addition of the word data.

3.2.6
system software
part of the software of a PE system that relates to the functioning of, and services provided by, the programmable device itself, as opposed to the application software that specifies the functions that perform a task related to the safety of the EUC

NOTE Refer to IEC 61508-7 for examples.

3.2.7
application software
application data
configuration data
part of the software of a programmable electronic system that specifies the functions that perform a task related to the EUC rather than the functioning of, and services provided by the programmable device itself

3.2.8
pre-existing software
software element which already exists and is not developed specifically for the current project or safety-related system.

NOTE The software could be a commercially available product, or it could have been developed by some organisation for a previous product or system. Pre-existing software may or may not have been developed in accordance with the requirements of this standard.

3.2.9
data
information represented in a manner suitable for communication, interpretation, or processing by computers

NOTE 1 Data may take the form of static information (for example configuration of a set point or a representation of geographical information) or it may take the form of instructions to specify a sequence of pre-existing functions.

NOTE 2 Refer to IEC 61508-7 for examples.

3.2.10
software on-line support tool
software tool that can directly influence the safety-related system during its run time

3.2.11
software off-line support tool
software tool that supports a phase of the software development lifecycle and that cannot directly influence the safety-related system during its run time. Software off-line tools may be divided into the following classes:

– **T1**
generates no outputs which can directly or indirectly contribute to the executable code (including data) of the safety related system;

NOTE 1 T1 examples include: a text editor or a requirements or design support tool with no automatic code generation capabilities; configuration control tools.

– **T2**
supports the test or verification of the design or executable code, where errors in the tool can fail to reveal defects but cannot directly create errors in the executable software;

NOTE 2 T2 examples include: a test harness generator; a test coverage measurement tool; a static analysis tool.

– **T3**
generates outputs which can directly or indirectly contribute to the executable code of the safety related system.

NOTE 3 T3 examples include: an optimising compiler where the relationship between the source code program and the generated object code is not obvious; a compiler that incorporates an executable run-time package into the executable code.

3.2.12
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).

3.2.13
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 3.2.12.

3.2.14
limited variability language
software programming language, whose notation is textual or graphical or has characteristics of both, 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 (reference [8] in the Bibliography) 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.

3.2.15
application specific integrated circuit
ASIC
integrated circuit designed and manufactured for specific function, where its functionality is defined by the product developer

NOTE The term ASIC as a stand-alone covers all types of the following integrated circuits:

– Full custom ASIC: ASIC where design and production is similar to a standard integrated circuit with the functionality defined by the product developer.

  A standard integrated circuit is manufactured in large quantities and can be used for different applications. Functionality, validation, production and production test are solely in the hand of the semiconductor vendor. Manual manipulations and optimisations at layout level are frequently used to reduce required area. They are not designed for safety-related systems. Frequent changes in production process, process technology and layout are likely for cost and yield optimisation. The number of components manufactured using a certain process or mask revision are not publicly known.

– Core based ASIC: ASIC based on a pre-layout, designed or generated macro cores, supported by additional logic.

  EXAMPLE 1 Examples for pre-layout macros are standard microprocessor cores, peripheral components, communication interfaces, analogue blocks, special function I/O cells.

  EXAMPLE 2 Examples for pre-designed macros known as Intellectual Property (IP) are a variety of similar components as mentioned in Example 1, with the difference that the design data consists of a high level hardware description language (VHDL, Verilog) as described for cell based ASIC.

  EXAMPLE 3 Examples for generated macros include embedded RAM, ROM, EEPROM or FLASH (flash memory). Generated blocks are assumed to be correct by construction, based on design rules. Pre-layout or generated macros are process specific but may be ported to different technologies. In most cases, the macro cores are not identical to the original discrete off-the-shelf components (different process, provided by a third party).

– Cell based ASIC: ASIC based on logic primitives (like AND, OR, Flip-Flop, Latch) taken from a cell library.

  The gate-level netlist containing the logic primitives and the interconnections is usually created from a high level hardware description language (VHDL, Verilog HDL) using synthesis tools. The functional and timing

characteristics of the logic primitives is characterised in the cell library; these parameters are used to drive the synthesis tool and are also used for simulation. In addition, layout tools are used to place the cells and to route the interconnects.

– Gate array: pre-manufactured silicon masters with a fixed number of cells that provide a common starting point for different components.

  The functionality is defined by the interconnection matrix (metal layer) between the pre-manufactured cells. The design process is very similar to that of a cell based ASIC, while the layout step is replaced by a routing step to connect the already existing cells.

– Field programmable gate array (FPGA): standard integrated circuit, using one-time programmable or re-programmable elements to define the connection between functional blocks and to configure the functionality of the individual blocks.

  It is not possible to test one-time programmable FPGAs completely during production due to the nature of the programmable element.

– Programmable logic device (PLD): standard integrated circuit, with low to medium complexity, using one-time programmable or electrical erasable elements (fuses) to define combinatorial logic – typically based on AND or OR product terms – and configurable storage elements.

  PLDs provide predictable timing and guaranteed maximum operating frequency in synchronous design due to their regular structure.

  Type of PLD are for example PAL, GAL, PML, (E)EPLD, PLA, PLS.

– Complex programmable logic device (CPLD): multiple PLD-like blocks on a single chip, connected by a programmable interconnection matrix (crossbar).

  The programmable logic element is re-programmable (EPROM or EEPROM) in most cases.

3.3 Systems – general aspects

3.3.1
programmable electronic system
PE system
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

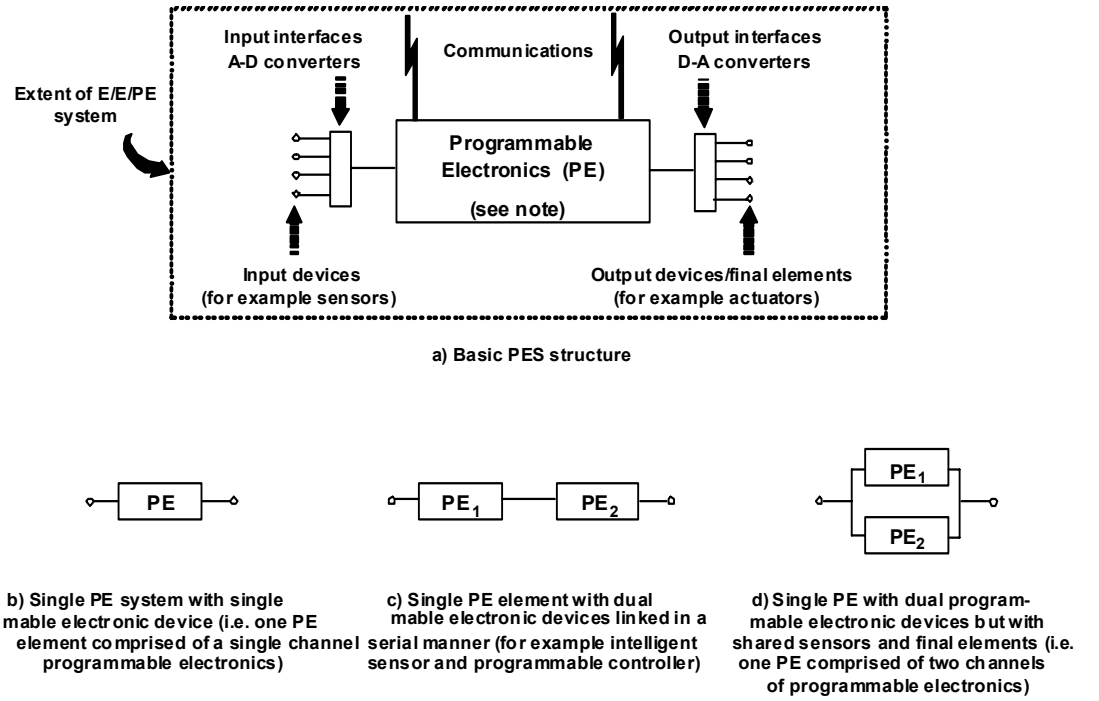
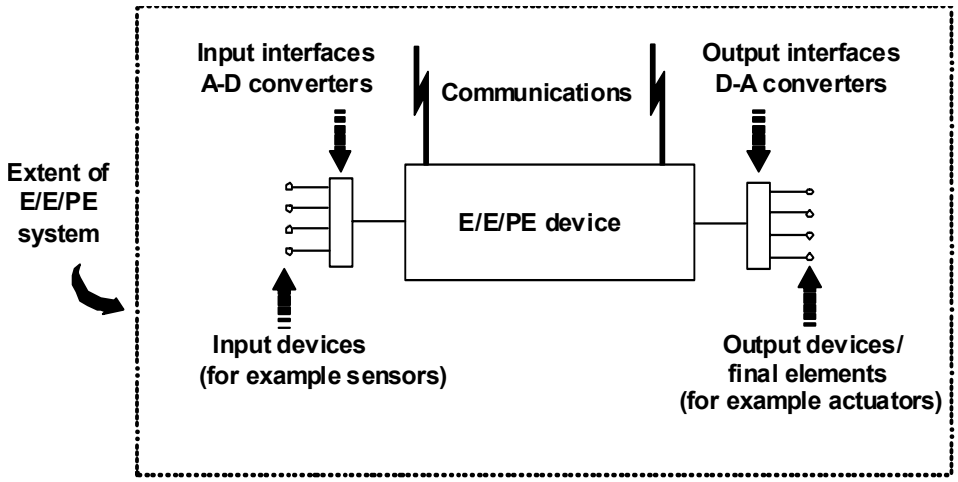


Figure 2 – Programmable electronic system

3.3.2
electrical/electronic/programmable electronic system
E/E/PE system
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)



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

Figure 3 – Electrical/electronic/programmable electronic system (E/E/PE system) – structure and terminology

3.3.3
EUC control system
system that 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.

3.3.4
architecture
specific configuration of hardware and software elements in a system

3.3.5
software module
construct that consists of procedures and/or data declarations and that can also interact with other such constructs

3.3.6
channel
element or group of elements that independently implement an element safety function

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

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

3.3.7
diversity
different means of performing a required function

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

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 and other risk reduction measures, 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 other risk reduction measures (see 3.4.2), the necessary risk reduction in order to meet the required tolerable risk (see 3.1.7). See also Annex A of IEC 61508-5.

NOTE 2 Safety-related systems are designed to prevent the EUC from going into a dangerous state by taking appropriate action on detection of a condition which may lead to a hazardous event. 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.

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 harmful event arises);

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

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

NOTE 5 A person can be part of a safety-related system. 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 A safety-related system 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 risk reduction measure
measure to reduce or mitigate risk that is separate and distinct from, and does not use, E/E/PE safety-related systems

EXAMPLE A relief valve is an other risk reduction measure.

3.4.3
low complexity E/E/PE safety-related system
E/E/PE safety-related system (see 3.2.13 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.

3.4.4
subsystem
entity of the top-level architectural design of a safety-related system where a dangerous failure according to 3.6.7 (a) of the subsystem results in dangerous failure of a safety function according to 3.6.7 (a)

3.4.5
element
part of a subsystem comprising a single component or any group of components that performs one or more element safety functions.

[IEC 62061, definition 3.2.6, modified]

NOTE 1 An element may comprise hardware and/or software.

NOTE 2 A typical element is a sensor, programmable controller or final element

3.4.6
redundancy
the existence of more than one means for performing a required function or for representing information.

[based on IEC 62059-11]

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

NOTE 1 Redundancy is used primarily to improve reliability (probability of functioning properly over a given period of time) or availability (probability of functioning at given instant). It may also be used in order to minimize spurious actions through architectures such as 2oo3.

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

NOTE 3 Redundancy may be "hot" or "active" (all redundant item running at the same time), "cold" or "stand-by" (only one of the redundant item working at the same time), "mixed" (one or several items running and one or several items in stand-by at the same time).

3.5 Safety functions and safety integrity

3.5.1
safety function
function to be implemented by an E/E/PE safety-related system or other risk reduction measures, that is intended to achieve or maintain a safe state for the EUC, in respect of a specific hazardous event (see 3.4.1 and 3.4.2)

EXAMPLE Examples of safety functions include:

– functions that are required to be carried out as positive actions to avoid hazardous situations (for example switching off a motor); and

– functions that prevent actions being taken (for example preventing a motor starting).

3.5.2
overall safety function
means of achieving or maintaining a safe state for the EUC, in respect of a specific hazardous event

3.5.3
element safety function
that part of a safety function (see 3.5.1) which is implemented by an element

3.5.4
safety integrity
probability of an E/E/PE safety-related system satisfactorily performing the specified safety functions under all the stated conditions within a stated period of time

NOTE 1 The higher the level of safety integrity, the lower the probability that the safety-related system will fail to carry out the specified safety functions or will fail to adopt a specified state when required.

NOTE 2 There are four levels of safety integrity (see 3.5.8).

NOTE 3 In determining safety integrity, all causes of failures (both random hardware failures and systematic failures) that 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 average frequency of failure in the dangerous mode of failure or the probability of a safety-related protection system failing to operate on demand. However, safety integrity also depends on many factors that cannot be accurately quantified but can only be considered qualitatively.

NOTE 4 Safety integrity comprises hardware safety integrity (see 3.5.7) and systematic safety integrity (see 3.5.6).

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).

3.5.5
software safety integrity
part of the safety integrity of a safety-related system relating to systematic failures in a dangerous mode of failure that are attributable to software

3.5.6
systematic safety integrity
part of the safety integrity of a safety-related system relating to systematic failures in a dangerous mode of failure

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

3.5.7
hardware safety integrity
part of the safety integrity of a safety-related system relating to random hardware failures in a dangerous mode of failure

NOTE 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 average frequency of dangerous failure 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.

3.5.8
safety integrity level
SIL
discrete level (one out of a possible four), corresponding to a range of safety integrity values, where safety integrity level 4 has the highest level of safety integrity and safety integrity level 1 has the lowest

NOTE 1 The target failure measures (see 3.5.17) for the four safety integrity levels are specified in Tables 2 and 3 of IEC 61508-1.

NOTE 2 Safety integrity levels are used for specifying the safety integrity requirements of the safety functions to be allocated to the E/E/PE safety-related systems.

NOTE 3 A safety integrity level (SIL) is not a property of a system, subsystem, element or component. The correct interpretation of the phrase "SIL n safety-related system" (where n is 1, 2, 3 or 4) is that the system is potentially capable of supporting safety functions with a safety integrity level up to n.

3.5.9
systematic capability
measure (expressed on a scale of SC 1 to SC 4) of the confidence that the systematic safety integrity of an element meets the requirements of the specified SIL, in respect of the specified element safety function, when the element is applied in accordance with the instructions specified in the compliant item safety manual for the element

NOTE 1 Systematic capability is determined with reference to the requirements for the avoidance and control of systematic faults (see IEC 61508-2 and IEC 61508-3).

NOTE 2 What is a relevant systematic failure mechanism will depend on the nature of the element. For example, for an element comprising solely software, only software failure mechanisms will need to be considered. For an element comprising hardware and software, it will be necessary to consider both systematic hardware and software failure mechanisms.

NOTE 3 A Systematic capability of SC N for an element, in respect of the specified element safety function, means that the systematic safety integrity of SIL N has been met when the element is applied in accordance with the instructions specified in the compliant item safety manual for the element.

3.5.10
software safety integrity level
systematic capability of a software element that forms part of a subsystem of a safety-related system

NOTE SIL characterises the overall safety function, but not any of the distinct subsystems or elements that support that safety function. In common with any element, software therefore has no SIL in its own right. However, it is convenient to talk about "SIL N software" meaning "software in which confidence is justified (expressed on a scale of 1 to 4) that the (software) element safety function will not fail due to relevant systematic failure mechanisms when the (software) element is applied in accordance with the instructions specified in the compliant item safety manual for the element".

3.5.11
E/E/PE system safety requirements specification
specification containing the requirements for the safety functions and their associated safety integrity levels

3.5.12
E/E/PE system 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 E/E/PE system safety requirements specification (see 7.10 and 7.10.2.6 of IEC 61508-1) 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.

3.5.13
E/E/PE system 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 E/E/PE system safety requirements specification (see 7.10 and 7.10.2.7 of IEC 61508-1)

3.5.14
E/E/PE system design requirements specification
specification containing the design requirements for the E/E/PE safety-related system in terms of the subsystems and elements

3.5.15
safety-related software
software that is used to implement safety functions in a safety-related system

3.5.16
mode of operation
way in which a safety function operates, which may be either

– **low demand mode:** where the safety function is only performed on demand, in order to transfer the EUC into a specified safe state, and where the frequency of demands is no greater than one per year; or

NOTE The E/E/PE safety-related system that performs the safety function normally has no influence on the EUC or EUC control system until a demand arises. However, if the E/E/PE safety-related system fails in such a way that it is unable to carry out the safety function then it may cause the EUC to move to a safe state (see 7.4.6 of IEC 61508-2).

– **high demand mode:** where the safety function is only performed on demand, in order to transfer the EUC into a specified safe state, and where the frequency of demands is greater than one per year; or

– **continuous mode:** where the safety function retains the EUC in a safe state as part of normal operation

3.5.17
target failure measure
target probability of dangerous mode failures to be achieved in respect of the safety integrity requirements, specified in terms of either

– the average probability of a dangerous failure of the safety function on demand, (for a low demand mode of operation);

– the average frequency of a dangerous failure [h^{-1}] (for a high demand mode of operation or a continuous mode of operation)

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

3.5.18
necessary risk reduction
risk reduction to be achieved by the E/E/PE safety-related systems and/or other risk reduction measures in order to ensure that the tolerable risk is not exceeded

3.6 Fault, failure and error (see Figure 4)

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

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

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.

3.6.2
fault avoidance
use of techniques and procedures that 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

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

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.

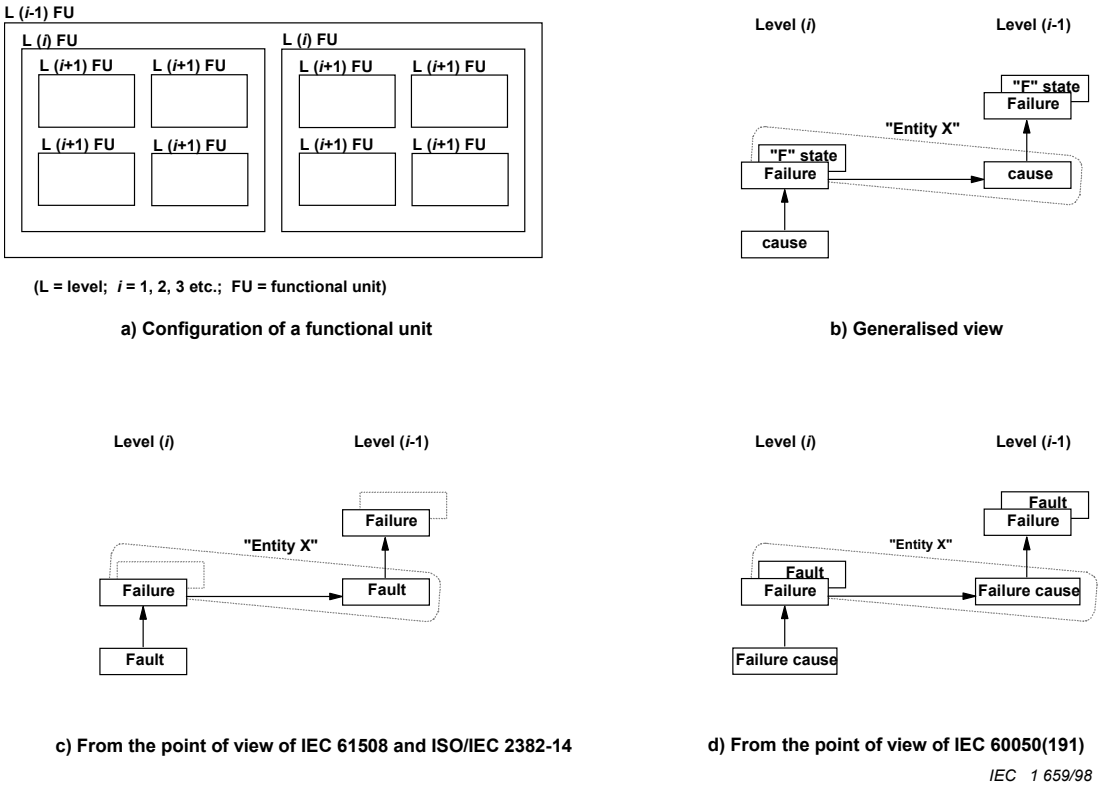
3.6.4
failure
termination of the ability of a functional unit to provide a required function or operation of a functional unit in any way other than as required

NOTE 1 This is based on IEV 191-04-01 with changes to include systematic failures due to, for example, deficiencies in specification or software.

NOTE 2 See Figure 4 for the relationship between faults and failures, both in the IEC 61508 series and IEC 60050-191.

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.



(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 the IEC 61508 series 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

3.6.5
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.

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

[IEV 191-04-19]

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.

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 (see 3.6.5) or systematic failures.

3.6.7
dangerous failure
failure of an element and/or subsystem and/or system that plays a part in implementing the safety function that:

a) prevents a safety function from operating when required (demand mode) or causes a safety function to fail (continuous mode) such that the EUC is put into a hazardous or potentially hazardous state; or

b) decreases the probability that the safety function operates correctly when required

3.6.8
safe failure
failure of an element and/or subsystem and/or system that plays a part in implementing the safety function that:

a) results in the spurious operation of the safety function to put the EUC (or part thereof) into a safe state or maintain a safe state; or

b) increases the probability of the spurious operation of the safety function to put the EUC (or part thereof) into a safe state or maintain a safe state

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

NOTE Two events A and B are dependent, only if: $P(\text{A and B}) > P(\text{A}) \times P(\text{B})$.

3.6.10
common cause failure
failure, that is the result of one or more events, causing concurrent 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

[IEV 191-05-24, modified]

3.6.12
soft-error
erroneous changes to data content but no changes to the physical circuit itself

NOTE 1 When a soft error has occurred and the data is rewritten, the circuit will be restored to its original state.

NOTE 2 Soft errors can occur in memory, digital logic, analogue circuits, and on transmission lines, etc and are dominant in semiconductor memory, including registers and latches. Data may be obtained, for example, from manufactures.

NOTE 3 Soft errors are transient and should not be confused with software programming errors.

3.6.13
no part failure
failure of a component that plays no part in implementing the safety function

NOTE The no part failure is not used for SFF calculations

3.6.14
no effect failure
failure of an element that plays a part in implementing the safety function but has no direct effect on the safety function

NOTE 1 The no effect failure has by definition no effect on the safety function so it cannot contribute to the failure rate of the safety function.

NOTE 2 The no effect failure is not used for SFF calculations.

3.6.15
safe failure fraction
SFF
property of a safety related element that is defined by the ratio of the average failure rates of safe plus dangerous detected failures and safe plus dangerous failures. This ratio is represented by the following equation:

$SFF = (\Sigma\lambda_{S\ avg} + \Sigma\lambda_{Dd\ avg})/(\Sigma\lambda_{S\ avg} + \Sigma\lambda_{Dd\ avg} + \Sigma\lambda_{Du\ avg})$

when the failure rates are based on constant failure rates the equation can be simplified to:

$SFF = (\Sigma\lambda_{S} + \Sigma\lambda_{Dd})/(\Sigma\lambda_{S} + \Sigma\lambda_{Dd} + \Sigma\lambda_{Du})$

3.6.16
failure rate
reliability parameter ($\lambda(t)$) of an entity (single components or systems) such that $\lambda(t).dt$ is the probability of failure of this entity within [t, t+dt] provided that it has not failed during [0, t]

NOTE 1 Mathematically, $\lambda(t)$ is the conditional probability of failure per unit of time over [t, t+dt]. It is in strong relationship with the reliability function (i.e. probability of no failure from 0 to t) by the general formula $R(t) = \exp(-\int_0^t \lambda(\tau)d\tau$. Reversely it is defined from the reliability function by $\lambda(t) = -\frac{dR(t)}{dt}\frac{1}{R(t)}$.

NOTE 2 Failure rates and their uncertainties can be estimated from field feedback by using conventional statistics. During the "useful life" (i.e. after burn-in and before wear-out), the failure rate of a simple item is more or less constant, $\lambda(t) \equiv \lambda$.

NOTE 3 The average of $\lambda(t)$ over a given period [0, T], $\lambda_{avg}(T) = (\int_0^T \lambda(\tau)d\tau)/T$, is not a failure rate because it cannot be used for calculating $R(t)$ as shown in Note 1. However it may be interpreted as the *average frequency* of failure over this period (i.e. the PFH, see Annex B of IEC 61508-6).

NOTE 4 The failure rate of a series of items is the sum of the failure rates of each item.

NOTE 5 The failure rate of redundant systems is generally non constant. Nevertheless when all failures are quickly revealed, independent and quickly repaired, $\lambda(t)$ converges quickly to an asymptotic value λ_{as} which is the *equivalent failure rate* of the systems. It should not be confused with the average failure rate described in Note 3 which doesn't necessarily converge to an asymptotic value.

3.6.17
probability of dangerous failure on demand
PFD
safety unavailability (see IEC 60050-191) of an E/E/PE safety-related system to perform the specified safety function when a demand occurs from the EUC or EUC control system

NOTE 1 The [instantaneous] unavailability (as per IEC 60050-191) is the probability that an item is not in a state to perform a required function under given conditions at a given instant of time, assuming that the required external resources are provided. It is generally noted by U (t).

NOTE 2 The [instantaneous] availability does not depend on the states (running or failed) experienced by the item before t. It characterizes an item which only has to be able to work when it is required to do so, for example, an E/E/PE safety related system working in low demand mode

NOTE 3 If periodically tested, the PFD of an E/E/PE safety-related system is, in respect of the specified safety function, represented by a saw tooth curve with a large range of probabilities ranging from low, just after a test, to a maximum just before a test.

3.6.18
average probability of dangerous failure on demand
PFD_{avg}
mean unavailability (see IEC 60050-191) of an E/E/PE safety-related system to perform the specified safety function when a demand occurs from the EUC or EUC control system

NOTE 1 The mean unavailability over a given time interval [t1, t2] is generally noted by U (t1, t2).

NOTE 2 Two kind of failures contribute to PFD and PFD_{avg}: the *dangerous undetected failures* occurred since the last proof test and genuine *on demand failures* caused by the demands (proof tests and safety demands) themselves. The first one is *time dependent* and characterized by their dangerous failure rate $\lambda_{DU}(t)$ whilst the second one is dependent only on the number of demands and is characterized by a *probability of failure per demand* (denoted by γ).

NOTE 3 As genuine on demand failures cannot be detected by tests, it is necessary to identify them and take them into consideration when calculating the target failure measures.

3.6.19
average frequency of a dangerous failure per hour
PFH
average frequency of a dangerous failure of an E/E/PE safety related system to perform the specified safety function over a given period of time

NOTE 1 The term “probability of dangerous failure per hour” is not used in this standard but the acronym PFH has been retained but when it is used it means “average frequency of dangerous failure [h]".

NOTE 2 From a theoretical point of view, the PFH is the average of the *unconditional failure intensity,* also called *failure frequency,* and which is generally designated w(t). It should not be confused with a failure rate (see Annex B of IEC 61508-6).

NOTE 3 When the E/E/PE safety-related system is the ultimate safety layer, the PFH should be calculated from its *unreliability* F(T)=1-R(t) (see “failure rate” above). When it is not the ultimate safety-related system its PFH should be calculated from its *unavailability* U(t) (see PFD above). PFH approximations are given by F(T)/T and 1/MTTF in the first case and 1/MTBF in the second case.

NOTE 4 When the E/E/PE safety-related system implies only quickly repaired revealed failures then an asymptotic failure rate λ_{as} is quickly reached. It provides an estimate of the PFH.

3.6.20
process safety time
period of time between a failure, that has the potential to give rise to a hazardous event, occurring in the EUC or EUC control system and the time by which action has to be completed in the EUC to prevent the hazardous event occurring

3.6.21
mean time to restoration
MTTR
expected time to achieve restoration

NOTE MTTR encompasses:

- the time to detect the failure (a); and,
- the time spent before starting the repair (b); and,
- the effective time to repair (c); and,
- the time before the component is put back into operation (d)

The start time for (b) is the end of (a); the start time for (c) is the end of (b); the start time for (d) is the end of (c).

3.6.22
mean repair time
MRT
expected overall repair time

NOTE MRT encompasses the times (b), (c) and (d) of the times for MTTR (see 3.6.21).

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 and other risk reduction measures are no longer available for use

NOTE 1 The term “functional safety lifecycle” is 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
software lifecycle
activities occurring during a period of time that starts when software is conceived and ends when the software is permanently decommissioned

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
configuration baseline
information that allows the software release to be recreated in an auditable and systematic way, including: all source code, data, run time files, documentation, configuration files, and installation scripts that comprise a software release; information about compilers, operating systems, and development tools used to create the software release

3.7.5
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

[ISO 8402, definition 2.17, modified]

NOTE In the context of this standard, verification is the activity of demonstrating for each phase of the relevant safety lifecycle (overall, E/E/PE system and software), by analysis, mathematical reasoning and/or tests, that, for the specific inputs, the outputs 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

[ISO 8402, definition 2.18, modified]

NOTE 1 In this standard there are three validation phases:

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

– E/E/PE system validation (see Figure 3 of IEC 61508-1);

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

NOTE 2 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
functional safety assessment
investigation, based on evidence, to judge the functional safety achieved by one or more E/E/PE safety-related systems and/or other risk reduction measures

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 dangerous hidden failures in a safety-related system so that, if necessary, a repair can restore the system to an “as new” condition or as close as practical to this condition

NOTE 1 In this standard the term “proof test” is used but it is recognised that a synonymous term is “periodical test”.

NOTE 2 The effectiveness of the proof test will be dependent both on failure coverage and repair effectiveness. In practice detecting 100 % of the hidden dangerous failures 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/EP system safety requirements specification. If separate channels are used, these tests are done for each channel separately. For complex elements, an analysis may need to be performed in order to demonstrate that the probability of hidden dangerous failure not detected by proof tests is negligible over the whole life duration of the E/E/EP safety related system.

NOTE 3 A proof test needs some time to be achieved. During this time the E/E/PE safety related system may be inhibited partially or completely. The proof test duration can be neglected only if the part of the E/E/PE safety related system under test remains available in case of a demand for operation or if the EUC is shut down during the test.

NOTE 4 During a proof test, the E/E/PE safety related system may be partly or completely unavailable to respond to a demand for operation. The MTTR can be neglected for SIL calculations only if the EUC is shut down during repair or if other risk measures are put in place with equivalent effectiveness.

3.8.6
diagnostic coverage
DC
fraction of dangerous failures detected by automatic on-line diagnostic tests. The fraction of dangerous failures is computed by using the dangerous failure rates associated with the detected dangerous failures divided by the total rate of dangerous failures

NOTE 1 The dangerous failure diagnostic coverage is computed using the following equation, where *DC* is the diagnostic coverage, λ_{DD} is the detected dangerous failure rate and $\lambda_{D\ total}$ is the total dangerous failure rate:

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

NOTE 2 This definition is applicable providing the individual components have constant failure rates.

3.8.7
diagnostic test interval
interval between on-line tests to detect faults in a safety-related system that has 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.

NOTE A dangerous failure detected by diagnostic test is a revealed failure and can be considered a safe failure only if effective measures, automatic of manual, are taken.

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
assessor
person, persons or organization that performs the functional safety assessment in order to arrive at a judgement on the functional safety achieved by the E/E/PE safety-related systems and other risk reduction measures

NOTE See also Clause 8 of IEC 61508-1.

3.8.11
independent person
person who is separate and distinct from the activities which take place during the specific phase of the overall, E/E/PE system or software safety lifecycle that is subject to the functional safety assessment or validation, and does not have direct responsibility for those activities

3.8.12
independent department
department that is separate and distinct from the departments responsible for the activities which take place during the specific phase of the overall, E/E/PE system or software safety lifecycle that is subject to the functional safety assessment or validation

3.8.13
independent organisation
organisation that is separate and distinct, by management and other resources, from the organisations responsible for the activities that take place during the specific phase of the overall, E/E/PE system or software safety lifecycle that is subject to the functional safety assessment or validation

3.8.14
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.

3.8.15
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 or hardware to be in operation.

3.8.16
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).

3.8.17
safety manual for compliant items
document that provides all the information relating to the functional safety of an element, in respect of specified element safety functions, that is required to ensure that the system meets the requirements of IEC 61508 series

3.8.18
proven in use
demonstration, based on an analysis of operational experience for a specific configuration of an element, that the likelihood of dangerous systematic faults is low enough so that every safety function that uses the element achieves its required safety integrity level

Bibliography

[1] IEC 61511 (all parts), *Functional safety – Safety instrumented systems for the process industry sector*

[2] IEC 62061:2005, *Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems*

[3] IEC 61800-5-2, *Adjustable speed electrical power drive systems – Part 5-2: Safety requirements – Functional*

[4] IEC 61508-5:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 5: Examples of methods for the determination of safety integrity levels*)

[5] IEC 61508-6:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3*

[6] IEC 61508-7:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 7: Overview of techniques and measures*

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

[8] IEC 61131-3:2003, *Programmable controllers – Part 3: Programming languages*

[9] IEC/TR 62059-11, *Electricity metering equipment – Dependability – Part 11:General concepts*

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

[11] IEC 60601 (all parts), *Medical electrical equipment*

[12] IEC 60050-191:1990, *International Electrotechnical Vocabulary – Chapter 191: Dependability and quality of service*

[13] IEC 60050-351:2006, *International Electrotechnical Vocabulary – Part 351: Control technology*

[14] IEC 61508-1:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General requirements*

[15] IEC 61508-2:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems*

[16] IEC 61508-3:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 3: Software requirements*

[17] ISO/IEC 2382-14:1997, *Information technology – Vocabulary – Part 14: Reliability, maintainability and availability*

[18] ISO 9000:2005, *Quality management systems – Fundamentals and vocabulary*

Index

SOMMAIRE

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

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

Partie 4: Définitions et abréviations

AVANT-PROPOS

1) La Commission Electrotechnique Internationale (CEI) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de la CEI). La CEI a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. A cet effet, la CEI – entre autres activités – publie des Normes internationales, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés "Publication(s) de la CEI"). Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec la CEI, participent également aux travaux. La CEI collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.
2) Les décisions ou accords officiels de la CEI concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de la CEI intéressés sont représentés dans chaque comité d'études.
3) Les Publications de la CEI se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de la CEI. Tous les efforts raisonnables sont entrepris afin que la CEI s'assure de l'exactitude du contenu technique de ses publications; la CEI ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.
4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de la CEI s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de la CEI dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de la CEI et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
5) La CEI elle-même ne fournit aucune attestation de conformité. Des organismes de certification indépendants fournissent des services d'évaluation de conformité et, dans certains secteurs, accèdent aux marques de conformité de la CEI. La CEI n'est responsable d'aucun des services effectués par les organismes de certification indépendants.
6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.
7) Aucune responsabilité ne doit être imputée à la CEI, à ses administrateurs, employés, auxiliaires ou mandataires, y compris ses experts particuliers et les membres de ses comités d'études et des Comités nationaux de la CEI, pour tout préjudice causé en cas de dommages corporels et matériels, ou de tout autre dommage de quelque nature que ce soit, directe ou indirecte, ou pour supporter les coûts (y compris les frais de justice) et les dépenses découlant de la publication ou de l'utilisation de cette Publication de la CEI ou de toute autre Publication de la CEI, ou au crédit qui lui est accordé.
8) L'attention est attirée sur les références normatives citées dans cette publication. L'utilisation de publications référencées est obligatoire pour une application correcte de la présente publication.
9) L'attention est attirée sur le fait que certains des éléments de la présente Publication de la CEI peuvent faire l'objet de droits de propriété intellectuelle ou de droits analogues. La CEI ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de propriété et de ne pas avoir signalé leur existence.

La Norme internationale CEI 61508-4 a été établie par le sous-comité 65A: Aspects systèmes, du comité d'études 65 de la CEI: Mesure, commande et automation dans les processus industriels.

Cette deuxième édition annule et remplace la première édition publiée en 1998 dont elle constitue une révision technique.

La présente édition a fait l'objet d'une révision approfondie et intègre de nombreux commentaires reçus lors des différentes phases de révision.

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

Le texte de cette norme est issu des documents suivants:

FDIS	Rapport de vote
65A/551/FDIS	65A/575/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.

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

Une liste de toutes les parties de la série CEI 61508, présentées sous le titre général *Sécurité fonctionnelle des systèmes électriques / électroniques / électroniques programmables relatifs à la sécurité*, peut être consultée sur le site web de la CEI.

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

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

INTRODUCTION

Les systèmes comprenant des composants électriques et/ou électroniques sont utilisés depuis de nombreuses années pour exécuter des fonctions relatives à la sécurité dans la plupart des secteurs d'application. Des systèmes à base d'informatique (dénommés de manière générique systèmes électroniques programmables) sont utilisés dans tous les secteurs d'application pour exécuter des fonctions non relatives à la sécurité, mais aussi de plus en plus souvent relatives 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 relatifs 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 et/ou électroniques et/ou électroniques programmables (E/E/PE) 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 systèmes électriques relatifs à la sécurité. Un objectif principal de cette approche est de faciliter le développement de normes internationales de produit et d'application sectorielle basées sur la série CEI 61508.

NOTE 1 Des exemples de normes internationales de produit et d'application sectorielle basées sur la série CEI 61508 sont donnés dans la Bibliographie (voir références [1], [2] et [3]).

Dans la plupart des cas, la sécurité est obtenue par un certain nombre de systèmes fondés sur diverses technologies (par exemple mécanique, hydraulique, pneumatique, électrique, électronique, électronique programmable). En conséquence, toute stratégie de sécurité doit non seulement prendre en compte tous les éléments d'un système individuel (par exemple, les capteurs, les appareils de commande et les actionneurs), mais également prendre en considération tous les systèmes relatifs à la sécurité comme des éléments individuels d'un ensemble complexe. Par conséquent, la présente Norme internationale, bien que traitant des systèmes E/E/PE relatifs à la sécurité, peut aussi fournir un cadre de sécurité susceptible de concerner les systèmes relatifs à la sécurité basés sur d'autres technologies.

Il est admis qu'il existe une grande variété d'applications utilisant des systèmes E/E/PE relatifs à la sécurité dans un grand nombre de secteurs, et couvrant un large éventail de complexité et de potentiel de dangers et de risques. Pour chaque application particulière, les mesures de sécurité requises dépendent de nombreux facteurs propres à l'application. La présente Norme internationale, de par son caractère général, rend désormais possible la prescription de ces mesures dans les futures normes internationales de produit et d'application sectorielle, ainsi que dans les révisions des normes déjà existantes.

La présente Norme internationale

– concerne toutes les phases appropriées du cycle de vie de sécurité global des systèmes E/E/PE et du logiciel (par exemple, depuis le concept initial, en passant par la conception, l'installation, l'exploitation et la maintenance, jusqu'à la mise hors service) lorsque les systèmes E/E/PE permettent d'exécuter des fonctions de sécurité,
– a été élaborée dans le souci de la prise en compte 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 de produit et d'application sectorielle concernant les systèmes E/E/PE relatifs à la sécurité; il convient que l'élaboration de normes internationales de produit et d'application sectorielle dans le cadre de la présente norme, permette d'atteindre un haut niveau de cohérence (par exemple, pour ce qui est des principes sous-jacents, de la terminologie, etc.) à la fois au sein de chaque secteur d'application, et d'un secteur à l'autre. La conséquence en sera une amélioration en termes de sécurité et de gains économiques,
– fournit une méthode de définition d'une spécification des exigences de sécurité nécessaire pour obtenir la sécurité fonctionnelle requise des systèmes E/E/PE relatifs à la sécurité,

– adopte une approche basée sur les risques qui permet de déterminer les exigences en matière d'intégrité de sécurité,

– introduit les niveaux d'intégrité de sécurité pour la spécification du niveau cible d'intégrité de sécurité des fonctions de sécurité devant être réalisées par les systèmes E/E/PE relatifs à la sécurité,

NOTE 2 La norme ne spécifie aucune exigence de niveau d'intégrité de sécurité pour aucune fonction de sécurité, ni comment le niveau d'intégrité de sécurité est déterminé. Elle fournit en revanche un cadre conceptuel basé sur les risques, ainsi que des exemples de méthodes.

– fixe des objectifs chiffrés de défaillance pour les fonctions de sécurité exécutées par les 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 objectifs chiffrés de défaillance pour une fonction de sécurité exécutée par un système E/E/PE relatif à la sécurité unique. Pour des systèmes E/E/PE relatifs à la sécurité fonctionnant

  – en mode de fonctionnement à faible sollicitation, la limite inférieure est fixée pour une probabilité moyenne de défaillance dangereuse de 10^{-5} en cas de sollicitation,

  – en mode de fonctionnement continu ou à sollicitation élevée, la limite inférieure est fixée à une fréquence moyenne de défaillance dangereuse de 10^{-9} [h^{-1}],

NOTE 3 Un système E/E/PE relatif à la sécurité unique n'implique pas nécessairement une architecture à un seul canal.

NOTE 4 Dans le cas de systèmes non complexes, il peut être possible de concevoir des systèmes relatifs à la sécurité ayant des valeurs plus basses pour l'intégrité de sécurité cible. Il est toutefois considéré que ces limites représentent ce qui peut être réalisé à l'heure actuelle pour des systèmes relativement complexes (par exemple, des systèmes électroniques programmables relatifs à la sécurité).

– établit des exigences fondées sur l'expérience et le jugement acquis dans le domaine des applications industrielles afin d'éviter des anomalies systématiques ou pour les maintenir sous contrôle. Même si, en général, la probabilité d'occurrence des défaillances systématiques ne peut être quantifiée, la norme permet cependant pour une fonction de sécurité spécifique, de déclarer que l'objectif chiffré de défaillance associé à cette fonction de sécurité peut être réputé atteint si toutes les exigences de la norme sont remplies,

– introduit une capabilité systématique s'appliquant à un élément du fait qu'il permet d'assurer que l'intégrité de sécurité systématique satisfait aux exigences du niveau d'intégrité de sécurité spécifié,

– 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 de manière explicite le concept de sécurité intrinsèque. Les principes de « sécurité intrinsèque » peuvent toutefois être applicables, l'adoption de ces concepts étant par ailleurs acceptable sous réserve de la satisfaction aux exigences des articles concernés de la norme.

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 la série de normes CEI 61508.

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.

1.3 Les CEI 61508-1, CEI 61508-2, CEI 61508-3 et CEI 61508-4 sont des publications fondamentales de sécurité, bien que ce statut ne soit pas applicable dans le contexte des systèmes E/E/PE de faible complexité relatifs à la sécurité (voir 3.4.3 de la CEI 61508-4). En tant que publications fondamentales de sécurité, ces normes sont destinées à être utilisées par les comités d'études pour la préparation des normes conformément aux principes contenus dans le Guide CEI 104 et le Guide ISO/CEI 51. Les CEI 61508-1, CEI 61508-2, CEI 61508-3 et CEI 61508-4 sont également destinées à être utilisées comme publications autonomes. La fonction de sécurité horizontale de la présente norme internationale ne s'applique pas aux appareils médicaux conformes à la série CEI 60601.

1.4 Une des responsabilités incombant à un comité d'études consiste, dans toute la mesure du possible, à utiliser les publications fondamentales de sécurité pour la préparation de ses publications. Dans ce contexte, les exigences, les méthodes ou les 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 d'études.

1.5 La Figure 1 illustre la structure générale de la série CEI 61508 et montre le rôle que la CEI 61508-4 joue dans la réalisation de la sécurité fonctionnelle pour les systèmes E/E/PE relatifs à la sécurité.

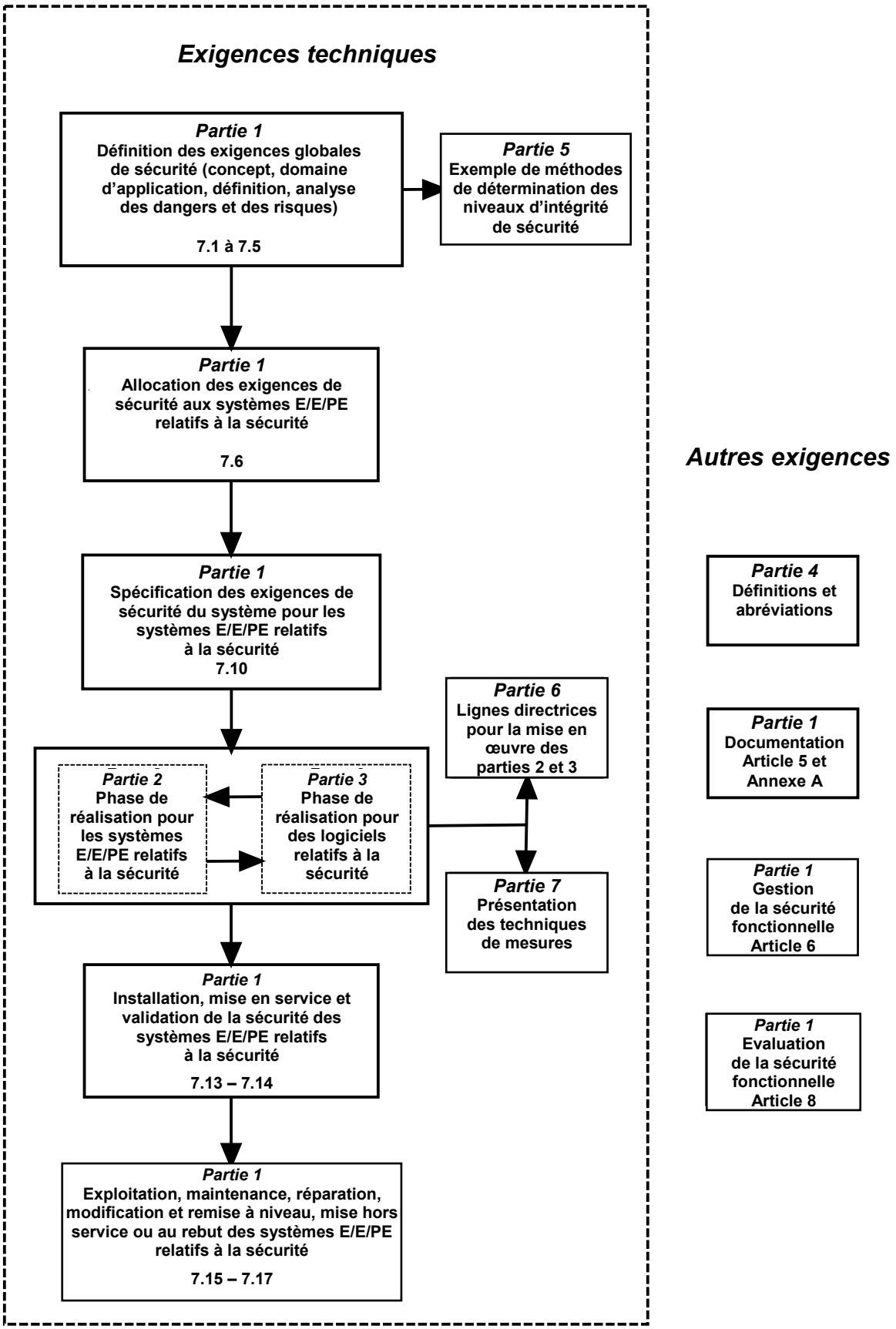


Figure 1 – Structure générale de la série CEI 61508

2 Références normatives

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

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

Guide ISO/CEI 51:1999, *Aspects liés à la sécurité – Principes directeurs pour les inclure dans les normes*

3 Définitions et abréviations

Pour les besoins du présent document, les définitions et abréviations données dans le Tableau 1 ci-dessous, ainsi que les suivantes s'appliquent.

Tableau 1 – Abréviations utilisées dans la présente norme

Abréviation	Expression complète	Définition et/ou explication du terme
ALARP	Aussi faible que raisonnablement possible	Annexe C de la CEI 61508-5
ASIC	Circuit intégré à application spécifique	3.2.15
CCF	Défaillance de cause commune	3.6.10
CPLD	Circuit logique programmable complexe	
DC	Couverture du diagnostic	3.8.6
(E)EPLD	Circuit logique programmable effaçable (électrique)	
E/E/PE	Electrique/électronique/électronique programmable	3.2.13, exemple: système E/E/PE relatif à la sécurité
E/E/PE (système)	Système électrique/électronique/électronique programmable	3.3.2
EEPROM	Mémoire morte programmable effaçable électriquement	
EPROM	Mémoire morte programmable effaçable	
EUC	Equipement commandé	3.2.1
FPGA	Matrice prédiffusée programmable	
GAL	Logique réseau générique	
HFT	Tolérance aux anomalies du matériel	7.4.4 de la CEI 61508-2
MooN	Architecture N canaux parmi M (par exemple 1oo2 est une architecture à un canal sur deux canaux, où chacun des deux canaux peut accomplir la fonction de sécurité)	Annexe B de la CEI 61508-6
MooND	Architecture N canaux parmi M, avec diagnostic	Annexe B de la CEI 61508-6
MTBF	Temps moyen entre défaillances	3.6.19, NOTE 3
MTTR	Durée moyenne de réparation, rétablissement	3.6.21
MRT	Temps moyen de dépannage	3.6.22
PAL	Logique réseau programmable	
PE	Electronique programmable	3.2.12
PE (système)	Electronique programmable	3.3.1
PFD	Probabilité de défaillance dangereuse en cas de sollicitation	3.6.17
PFD_{avg}	Probabilité moyenne de défaillance dangereuse en cas de	3.6.18

Abréviation	Expression complète	Définition et/ou explication du terme
	sollicitation	
PFH	Fréquence moyenne de défaillance dangereuse [h^{-1}]	3.6.19
PLA	Réseau logique programmable	
PLC	Automate programmable	Annexe E de la CEI 61508-6
PLD	Circuit logique programmable	
PLS	Séquenceur logique programmable	
PML	Logique macro programmable	
RAM	Mémoire vive	
ROM	Mémoire morte	
SFF	Proportion de défaillances en sécurité	3.6.15
SIL	Niveau d'intégrité de sécurité	3.5.8
VHDL	Langage de description de matériel de circuit intégré à très grande vitesse	CEI 61508-2, Annexe F, Note 5

3.1 Termes relatifs à la sécurité

3.1.1
dommage
blessure physique ou atteinte à la santé des personnes ou atteinte aux biens ou à l'environnement

[Guide 51 ISO/CEI:1999, définition 3.3]

3.1.2
danger
source potentielle de dommage

[Guide 51 ISO/CEI:1999, définition 3.5]

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

3.1.3
situation dangereuse
situation dans laquelle des personnes, des biens ou l'environnement sont exposés à un ou plusieurs dangers

[Guide 51 ISO/CEI:1999, définition 3.6, modifiée]

3.1.4
événement dangereux
événement susceptible de conduire à un dommage

NOTE Le fait qu'un événement dangereux conduise ou non à un dommage dépend de l'éventualité que des personnes, des biens ou l'environnement soient exposés aux conséquences de l'événement dangereux et, dans le cas de dommage aux personnes, que les personnes exposées puissent éviter les conséquences de l'événement après son occurrence.

3.1.5
événement préjudiciable (dangereux)
situation dangereuse ou événement dangereux qui conduit à un dommage

NOTE Adapté du Guide 51 ISO/CEI, définition 3.4, pour tenir compte d'un événement dangereux.

3.1.6
risque
combinaison de la probabilité d'un dommage et de sa gravité

[Guide 51 ISO/CEI:1999, définition 3.2]

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

3.1.7
risque tolérable
risque accepté dans un certain contexte et fondé sur les valeurs admises par la société

[Guide 51 ISO/CEI:1999, définition 3.7]

NOTE Voir Annexe C de la CEI 61508-5.

3.1.8
risque résiduel
risque subsistant après que des mesures de prévention ont été prises

[Guide 51 ISO/CEI:1999, définition 3.9]

3.1.9
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 préjudiciable spécifique pour lequel les systèmes E/E/PE relatifs à la sécurité 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 indiqué à 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 et les dispositifs externes de réduction de risque.

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

3.1.10
risque cible
risque qu'il est prévu d'obtenir pour un danger spécifique en tenant compte du risque EUC ainsi que des systèmes E/E/PE relatifs à la sécurité et des dispositifs externes de réduction de risque

3.1.11
sécurité
absence de risque inacceptable

[Guide 51 ISO/CEI:1999, définition 3.1]

3.1.12
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 et des dispositifs externes de réduction de risque

3.1.13
état de sécurité
état de l'EUC lorsque la sécurité est réalisée

NOTE Pendant 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 temps où l'EUC est continuellement commandé. Cette commande continuée peut s'étendre sur une période courte ou indéfinie.

3.1.14
mauvais usage raisonnablement prévisible
utilisation d'un produit, procédé ou service dans des conditions ou à des fins non prévues par le fournisseur, mais qui peut provenir d'un comportement humain envisageable

[Guide 51 ISO/CEI:1999, définition 3.14]

3.2 Matériel et dispositifs

3.2.1
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.

3.2.2
environnement
tous les paramètres pertinents susceptibles d'affecter la réalisation de la sécurité fonctionnelle pour l'application spécifique considérée et dans toute phase du cycle de vie de sécurité

NOTE Il peut s'agir, par exemple, de l'environnement physique, de l'environnement d'exploitation, de l'environnement légal et de l'environnement de maintenance.

3.2.3
unité fonctionnelle
entité matérielle ou logicielle, ou les deux à la fois, capable de remplir une fonction déterminée

[ISO/CEI 2382-1, 01-01-40]

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

3.2.4
application
tâche relative à l'EUC plutôt qu'au système E/E/PE

3.2.5
logiciel
création intellectuelle comprenant les programmes, les procédures, les données et les règles, ainsi que toute documentation associée 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/CEI 2382-1 (référence [7] dans la Bibliographie), par l'ajout du mot «données».

3.2.6
logiciel système
partie du logiciel d'un système PE liée au fonctionnement du dispositif programmable proprement dit et aux services qu'il fournit, contrairement au logiciel d'application qui spécifie les fonctions réalisées par une tâche relative à la sécurité de l'EUC

NOTE Se reporter à la CEI 61508-7 pour des exemples.

3.2.7
logiciel d'application
données d'application
données de configuration
partie du logiciel d'un système électronique programmable qui spécifie les fonctions réalisées par une tâche relative à l'EUC plutôt que le fonctionnement du dispositif programmable proprement dit et des services qu'il fournit

3.2.8
logiciel préexistant
élément de logiciel déjà existant et n'ayant pas été spécifiquement développé pour le projet ou le système relatif à la sécurité actuel

NOTE Le logiciel peut être un produit disponible dans le commerce ou avoir été développé par un organisme pour un produit ou système antérieur. Le logiciel préexistant peut avoir été ou non développé conformément aux exigences de la présente norme.

3.2.9
données
informations présentées de manière appropriée pour la communication, l'interprétation ou le traitement informatique

NOTE 1 Les données peuvent se présenter sous la forme d'informations statiques (par exemple, configuration d'un point de consigne ou représentation d'informations géographiques) ou d'instructions permettant de spécifier une séquence de fonctions préexistantes.

NOTE 2 Se reporter à la CEI 61508-7 pour des exemples.

3.2.10
outil de support logiciel direct
outil logiciel susceptible d'avoir une influence directe sur le système relatif à la sécurité pendant sa durée d'exécution

3.2.11
outil de support logiciel autonome
outil logiciel qui prend en charge une phase du cycle de vie de développement du logiciel et ne pouvant avoir une influence directe sur le système relatif à la sécurité pendant son exécution. Les outils logiciels autonomes peuvent être répartis dans les classes suivantes:

– **T1**

ne génère aucune sortie susceptible de contribuer, directement ou indirectement, au code exécutable (y compris les données) du système relatif à la sécurité,

NOTE 1 Parmi les exemples de T1 on peut citer: un éditeur de texte ou un outil de support aux exigences ou un outil d'aide à la conception sans capacité de génération automatique de code; des outils de contrôle de la configuration.

– **T2**

prend en charge l'essai ou la vérification de la conception ou du code exécutable lorsque des erreurs propres à l'outil peuvent empêcher de détecter des défauts mais ne peuvent directement créer des erreurs dans le logiciel exécutable,

NOTE 2 Parmi les exemples de T2 on peut citer: un simulateur d'essai, un outil de mesure de couverture d'essai, un outil d'analyse statique.

– **T3**

génère des sorties susceptibles de contribuer, directement ou indirectement, au code exécutable du système relatif à la sécurité.

NOTE 3 Parmi les exemples de T3 on peut citer: un compilateur d'optimisation lorsque la relation entre le programme de code source et le code objet généré n'est pas évidente, un compilateur intégrant un progiciel d'exécution exécutable dans le code exécutable.

3.2.12
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 dispositifs micro-électroniques basés sur une ou plusieurs unités centrales de traitement (CPU) associées à des mémoires, etc.

EXEMPLE Tous les dispositifs suivants sont des dispositifs électroniques programmables:

– microprocesseurs,

– microcontrôleurs,

– automates programmables,

– circuits intégrés à application spécifique (ASIC),

– automates logiques programmables (PLC),

– autres dispositifs basés sur la technologie informatique (par exemple, les capteurs intelligents, les transmetteurs, les actionneurs).

3.2.13
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 dispositifs ou systèmes 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 3.2.12.

3.2.14
langage de variabilité limitée
langage de programmation de logiciel, textuel ou graphique ou ayant des caractéristiques des deux, pour les automates électroniques 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 (référence [8] dans la Bibliographie) 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,

– diagramme de 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.

3.2.15
circuit intégré à application spécifique
ASIC
circuit intégré conçu et fabriqué pour une fonction spécifique et dont la fonctionnalité est définie par le développeur de produit

NOTE Le terme ASIC couvre, de manière générale, tous les types de circuits intégrés suivants:

– ASIC complètement personnalisé: ASIC dont la conception et la production sont similaires à celles d'un circuit intégré standard, et dont la fonctionnalité est définie par le développeur de produit.

  Un circuit intégré standard est fabriqué en grandes quantités et peut être utilisé pour différentes applications. La fonctionnalité, la validation, la production et l'essai de production incombent au fournisseur de semi-conducteurs. Des traitements et optimisations manuels réalisés au niveau de la configuration sont fréquemment utilisés pour réduire la surface requise. Ils ne sont pas conçus pour les systèmes relatifs à la sécurité. Les modifications courantes apportées au procédé de production, à la technologie de procédé et à la configuration concernent plus généralement l'optimisation des coûts et du rendement. Le nombre de composants fabriqués sur la base d'un procédé ou d'une révision des masques donné(e) n'est pas accessible du public.

– ASIC à macrocellules: ASIC basé sur des macrocellules préconfigurées, préconçues ou générées, pris en charge par une logique supplémentaire.

  EXEMPLE 1 Des exemples de macros préconfigurées sont les cœurs de microprocesseurs standards, les composants périphériques, les interfaces de communication, les blocs analogiques, les cellules d'E/S de fonction spéciales.

  EXEMPLE 2 Des exemples de macros préconçues identifiées comme Propriété Intellectuelle (PI) sont des variétés de composants similaires à ceux mentionnés dans l'Exemple 1, à la différence que les données de conception comportent un langage de description de matériel de haut niveau (VHDL, Verilog HDL) tel que décrit pour l'ASIC précaractérisé.

  EXEMPLE 3 Des exemples de macros générées comprennent les mémoires RAM, ROM, EEPROM ou FLASH intégrées. La construction des blocs générés est supposée correctement établie sur la base de règles de conception. Les macros préconfigurées ou générées sont spécifiques au procédé mais elles peuvent être appliquées à différentes technologies. Dans la plupart des cas, les macrocellules ne sont pas identiques aux composants discrets d'origine du commerce (procédé différent fourni par une tierce partie).

– ASIC pré-caractérisé: ASIC basé sur des primitives logiques (telles que ET, OU, Bascule, Verrou) issues d'une bibliothèque de cellules.

  La liste d'interconnexions matricielle contenant les primitives logiques et les interconnexions est généralement créée à partir d'un langage de description de matériel de haut niveau (VHDL, Verilog) au moyen d'outils de synthèse. Les caractéristiques fonctionnelles et de synchronisation des primitives logiques sont caractérisées dans la bibliothèque de cellules; ces paramètres sont utilisés pour piloter l'outil de synthèse ainsi que pour la simulation. Par ailleurs, les outils de configuration sont utilisés pour placer les cellules et tracer les interconnexions.

– Matrice prédiffusée: puce de silicium préfabriquée comportant un nombre fixe de cellules assurant un point de départ commun à différents composants.

  La fonctionnalité est définie par la matrice d'interconnexion (couche métallique) entre les cellules préfabriquées. Le processus de conception est très similaire à celui d'un ASIC précaractérisé, l'étape de configuration étant toutefois remplacée par une étape de routage pour connecter les cellules déjà existantes.

– Matrice prédiffusée programmable (FPGA): circuit intégré standard, utilisant des éléments programmables uniques ou reprogrammables pour définir la connexion entre les blocs fonctionnels et pour configurer la fonctionnalité des blocs individuels.

  Il n'est pas possible de soumettre complètement au test des FPGA programmables à application unique pendant la production du fait de la nature même de l'élément programmable.

– Circuit logique programmable (PLD): circuit intégré standard, de complexité faible à moyenne, utilisant des éléments programmables une seule fois ou des éléments électriques effaçables (fusibles) pour définir des éléments logiques combinatoires – généralement basés sur des termes de produit ET ou OU – et des éléments de mémoire configurables.

  Les PLD, du fait de leur structure régulière, fournissent une synchronisation prévisible et une fréquence d'exploitation maximale garantie pour une conception synchrone.

  Des exemples de types de PLD sont: PAL, GAL, PML, (E)EPLD, PLA, PLS.

– Circuit logique programmable complexe (CPLD): blocs à PLD multiple sur une puce, connectés par une matrice d'interconnexion programmable (réseau matriciel).

  L'élément logique programmable est, dans la plupart des cas, reprogrammable (EPROM ou EEPROM).

3.3 Systèmes – aspects généraux

3.3.1
système électronique programmable
système PE

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 et les autres dispositifs d'entrée, les autoroutes de données et les autres voies de communication, ainsi que les actionneurs et les autres dispositifs de sortie (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 un PES dans la présente Norme internationale, l'électronique programmable étant représentée comme une unité distincte des capteurs et des actionneurs de l'EUC et de leurs interfaces. Cependant, l'électronique programmable peut être répartie en divers endroits du PES. La Figure 2 c) présente un PES comportant deux unités discrètes d'électronique programmable. La Figure 2 d) illustre un PES comportant une électronique programmable doublée (c'est-à-dire à deux canaux), mais avec un seul capteur et un seul actionneur.

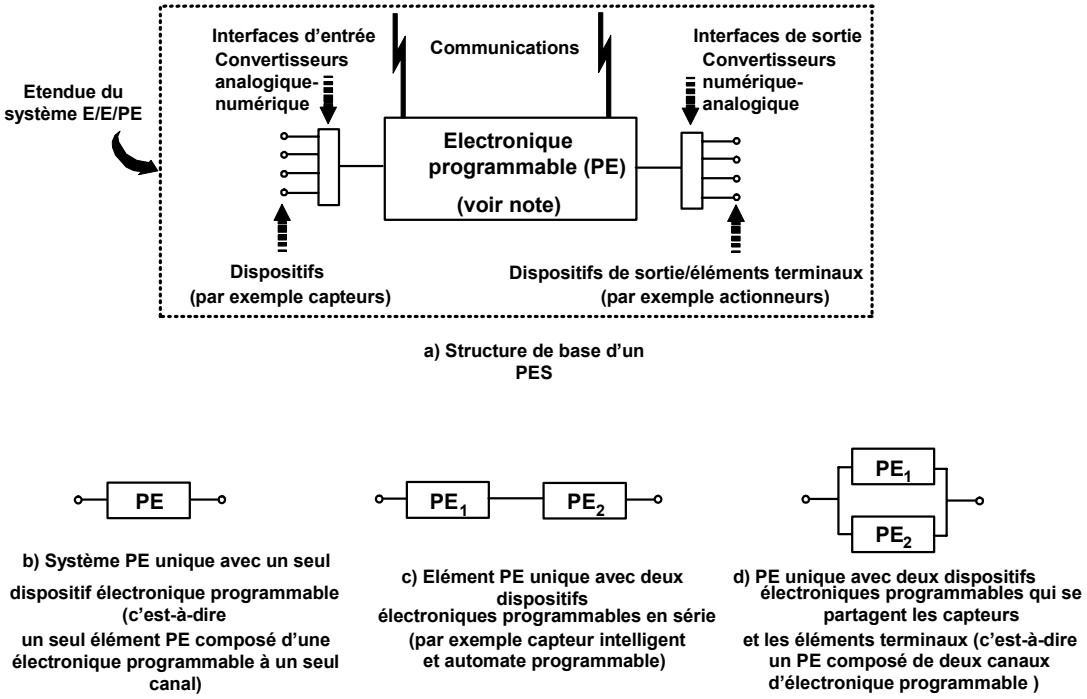
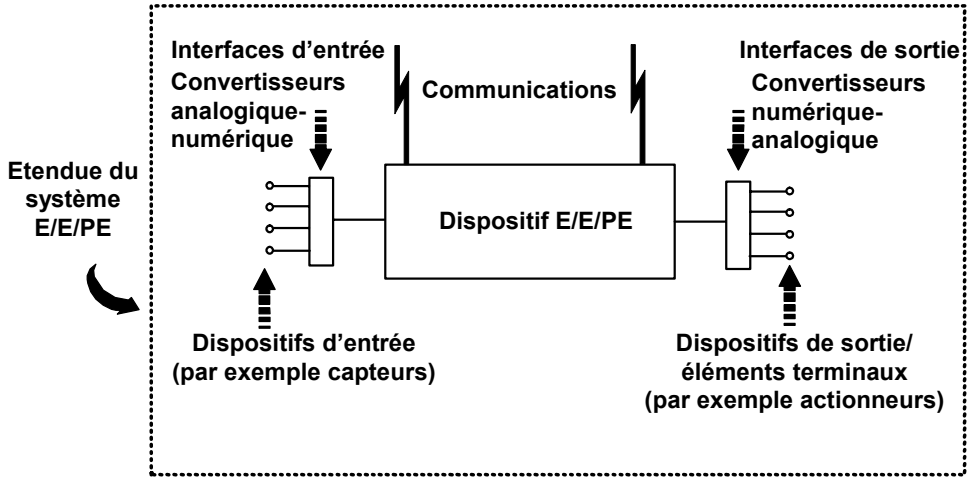


Figure 2 – Système électronique programmable

3.3.2
système électrique/électronique/électronique programmable
système E/E/PE
système de commande, de protection ou de surveillance basé sur un ou plusieurs dispositifs électriques/électroniques/électroniques programmables (E/E/PE). Ce terme recouvre tous les éléments du système, tels que l'alimentation, les capteurs, et les autres dispositifs d'entrée, les autoroutes de données et les autres voies de communication, ainsi que les actionneurs et les autres dispositifs de sortie (voir la Figure 3)



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 système E/E/PE.

Figure 3 – Système électrique/électronique/électronique programmable (système E/E/PE) – structure et terminologie

3.3.3
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.

3.3.4
architecture
configuration spécifique des éléments matériels et logiciels dans un système

3.3.5
module logiciel
construction consistant en des procédures et/ou déclarations de données pouvant aussi être en interaction avec d'autres constructions de même nature

3.3.6
canal
élément ou groupe d'éléments exécutant la fonction de sécurité d'un élément de manière indépendante

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

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

3.3.7
diversité
moyens différents pour réaliser une fonction requise

NOTE La diversité peut être réalisée en utilisant des méthodes physiques ou des approches conceptuelles différentes.

3.4 Systèmes – aspects relatifs à la sécurité

3.4.1
système relatif à la sécurité
système désigné qui, à la fois,

– met en œuvre les fonctions de sécurité requises pour atteindre ou maintenir un état de sécurité de l'EUC et
– est prévu pour atteindre, par lui-même ou grâce à d'autres systèmes E/E/PE relatifs à la sécurité, et aux dispositifs externes de réduction de risque, l'intégrité de sécurité nécessaire pour les fonctions de sécurité requises

NOTE 1 Ce terme fait référence aux systèmes désignés comme systèmes relatifs à la sécurité qui, avec les dispositifs externes de réduction de risque (voir 3.4.2), sont destinés à réaliser la réduction de risque nécessaire, afin de satisfaire au niveau de risque tolérable requis (voir 3.1.7). Voir également l'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 de détection d'une condition susceptible d'occasionner un événement dangereux. La défaillance d'un système relatif à la sécurité serait incluse dans les événements à l'origine du ou des dangers 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 obtenir à leur façon le niveau de risque tolérable requis. Les systèmes relatifs à la sécurité peuvent globalement être répartis en systèmes relatifs à la sécurité de commande et en systèmes relatifs à la sécurité de protection.

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 œuvre les fonctions de sécurité dans le système de commande de l'EUC (et éventuellement également par l'adjonction 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 conçu 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 conçu pour réduire les effets de l'événement préjudiciable, réduisant ainsi le risque en limitant les conséquences de ce risque,

c) être conçu pour réaliser une combinaison de a) e de b).

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

NOTE 6 Un système relatif à la sécurité recouvre l'ensemble des matériels, logiciels, ainsi que tous les équipements annexes (par exemple, alimentation) nécessaires pour exécuter 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
dispositif externe de réduction de risque
mesure destinée à réduire ou atténuer le risque, qui est séparée et distincte et n'utilise pas de systèmes E/E/PE relatifs à la sécurité

EXEMPLE Une soupape de sécurité est un dispositif externe de réduction de risque.

3.4.3
système E/E/PE relatif à la sécurité de faible complexité
système E/E/PE relatif à la sécurité (voir 3.2.13 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 par l'intermédiaire de relais électromécaniques interposés, un ou plusieurs contacteurs destinés à couper l'alimentation d'un moteur électrique est un système E/E/PE relatif à la sécurité de faible complexité.

3.4.4
sous-système
entité de la conception architecturale de haut niveau d'un système relatif à la sécurité où une défaillance dangereuse conforme au 3.6.7 (a) du sous-système conduit à une défaillance dangereuse d'une fonction de sécurité conforme au 3.6.7 (a)

3.4.5
élément
partie d'un sous-système comprenant un seul composant ou n'importe quel groupe de composants et réalisant une ou plusieurs fonctions de sécurité de l'élément

[CEI 62061, définition 3.2.6, modifiée]

NOTE 1 Un élément peut comporter le matériel et/ou le logiciel.

NOTE 2 Un élément typique est un capteur, un automate programmable ou un élément terminal.

3.4.6
redondance
existence de plusieurs moyens pour accomplir une fonction requise ou pour représenter des informations.

[définition basée sur la CEI 62059-11]

EXEMPLE Des éléments fonctionnels en double et l'adjonction de bits de parité constituent deux exemples de redondance.

NOTE 1 La redondance sert essentiellement à améliorer la fiabilité (probabilité de bon fonctionnement sur une période de temps donnée) ou la disponibilité (probabilité de fonctionnement à un moment donné). Elle peut également être utilisée pour réduire au niveau minimum des actions parasites par des architectures telles que 2oo3.

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

NOTE 3 La redondance peut être « active » (tous les articles redondants fonctionnant en même temps), « froide » ou « passive » (uniquement un seul article redondant fonctionnant en même temps), "mixte" (un ou plusieurs articles en fonctionnement et un ou plusieurs articles en redondance passive en même temps).

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 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 et 3.4.2)

EXEMPLE Des exemples de fonctions de sécurité comprennent:

– les fonctions devant être réalisées en tant qu'actions positives pour éviter des situations dangereuses (par exemple, arrêt d'un moteur) et

– les fonctions de prévention de réalisation d'actions (par exemple, empêcher le démarrage d'un moteur).

3.5.2
fonction de sécurité globale
moyen permettant d'atteindre ou de maintenir un état de sécurité de l'EUC, par rapport à un événement dangereux spécifique

3.5.3
fonction de sécurité de l'élément
partie d'une fonction de sécurité (voir 3.5.1) mise en œuvre par un élément

3.5.4
intégrité de sécurité
probabilité pour qu'un système E/E/PE relatif à la sécurité exécute de manière satisfaisante les fonctions de sécurité spécifiées dans toutes les conditions énoncées et dans une période de temps spécifiée

NOTE 1 Plus le niveau d'intégrité de sécurité d'un système relatif à la sécurité est élevé, plus la probabilité d'une défaillance du système dans l'exécution des fonctions de sécurité spécifiées ou dans l'adoption d'un état spécifié lorsque requis est faible.

NOTE 2 Il existe quatre niveaux d'intégrité de sécurité (voir 3.5.8).

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 aléatoires du matériel, peuvent être quantifiées à l'aide de mesures telles que la fréquence moyenne de défaillance en mode de défaillance dangereux, ou la probabilité de non fonctionnement en cas de sollicitation d'un système de protection relatif à la sécurité. Cependant, l'intégrité de sécurité 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 3.5.7) ainsi que l'intégrité de sécurité systématique (voir 3.5.6).

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

3.5.5
intégrité de sécurité du logiciel
partie de l'intégrité de sécurité d'un système relatif à la sécurité qui se rapporte aux défaillances systématiques dans un mode de défaillance dangereux imputables au logiciel

3.5.6
intégrité de sécurité systématique
partie de l'intégrité de sécurité d'un système relatif à la sécurité qui se rapporte aux défaillances systématiques dans un mode de défaillance dangereux

NOTE L'intégrité de sécurité systématique ne peut normalement pas être quantifiée (à la différence de l'intégrité de sécurité du matériel qui, habituellement, peut l'être).

3.5.7
intégrité de sécurité du matériel
partie de l'intégrité de sécurité d'un système relatif à la sécurité qui se rapporte aux défaillances aléatoires du matériel en mode de défaillance dangereux

NOTE 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. Dans ce contexte, les deux paramètres à prendre en compte sont la fréquence moyenne de défaillance dangereuse et la probabilité de non fonctionnement en cas de sollicitation. 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 de fiabilité, quant à lui, est utilisé dans le contexte des systèmes de protection relatifs à la sécurité.

3.5.8
niveau d'intégrité de sécurité
SIL
niveau discret (parmi quatre possibles) correspondant à une gamme de valeurs d'intégrité de sécurité où le niveau 4 d'intégrité de sécurité possède le plus haut degré d'intégrité et le niveau 1 possède le plus bas

NOTE 1 Les objectifs chiffrés de défaillance (voir 3.5.17) pour les quatre niveaux d'intégrité de sécurité sont indiqués dans les Tableaux 2 et 3 de la CEI 61508-1.

NOTE 2 Les niveaux d'intégrité de sécurité sont utilisés pour spécifier les exigences concernant l'intégrité de sécurité des fonctions de sécurité à allouer aux systèmes E/E/PE relatifs à la sécurité.

NOTE 3 Un niveau d'intégrité de sécurité (SIL) ne constitue pas une propriété d'un système, sous-système, élément ou composant. L'interprétation correcte de l'expression "Système relatif à la sécurité à SIL n" (où n est 1, 2, 3 ou 4) signifie que le système est potentiellement capable de prendre en charge les fonctions de sécurité avec un niveau d'intégrité de sécurité jusqu'à n.

3.5.9
capabilité systématique
mesure (exprimée sur une échelle de SC 1 à SC 4) de la confiance dans le fait que l'intégrité de sécurité systématique d'un élément satisfait aux exigences du niveau SIL spécifié, par rapport à la fonction de sécurité spécifiée de l'élément, lorsque l'élément est appliqué conformément aux instructions spécifiées dans le manuel de sécurité d'articles conformes pour l'élément

NOTE 1 La capabilité systématique est déterminée par référence aux exigences concernant l'évitement et à la maîtrise des anomalies systématiques (voir CEI 61508-2 et CEI 61508-3).

NOTE 2 La détermination d'un mécanisme de défaillance systématique pertinent dépend de la nature de l'élément. Par exemple, pour un élément comprenant uniquement un logiciel, seuls les mécanismes de défaillance du logiciel doivent être considérés. Pour un élément comprenant du matériel et du logiciel, il est nécessaire de considérer à la fois les mécanismes de défaillance systématique du matériel et du logiciel.

NOTE 3 Une capabilité systématique de SC N pour un élément, par rapport à la fonction de sécurité spécifiée de l'élément, signifie que l'intégrité de sécurité systématique de SIL N a été satisfaite lorsque l'élément est appliqué conformément aux instructions spécifiées dans le manuel de sécurité d'article conforme pour l'élément.

3.5.10
niveau d'intégrité de sécurité du logiciel
capabilité systématique d'un élément de logiciel faisant partie intégrante d'un sous-système d'un système relatif à la sécurité

NOTE Le niveau SIL caractérise la fonction de sécurité globale, mais pas tous les sous-systèmes ou éléments distincts prenant en charge la fonction de sécurité. Le logiciel, en lui-même, ne dispose donc pas d'un niveau SIL commun avec tout élément. Cependant, il est préférable de parler de « logiciel à SIL N » pour signifier un « logiciel pour lequel la confiance est justifiée (exprimée sur une échelle de 1 à 4) dans le fait que la fonction de sécurité de l'élément (logiciel) ne présente pas de défaillance du fait des mécanismes de défaillance systématique pertinents lorsque l'élément (logiciel) est appliqué conformément aux instructions spécifiées dans le manuel de sécurité d'article conforme pour l'élément ».

3.5.11
spécification des exigences de sécurité concernant les systèmes E/E/PE
spécification qui contient les exigences concernant les fonctions de sécurité et leurs niveaux d'intégrité de sécurité associés

3.5.12
spécification des exigences concernant les fonctions de sécurité des systèmes E/E/PE
spécification qui contient les exigences concernant les 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 exigences de sécurité concernant les systèmes E/E/PE (voir 7.10 et 7.10.2.6 de la CEI 61508-1). Elle contient le détail précis des fonctions de sécurité qui doivent être réalisées par les systèmes relatifs à la sécurité.

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

3.5.13
spécification des exigences concernant l'intégrité de sécurité des systèmes E/E/PE
spécification qui contient les exigences d'intégrité de sécurité des fonctions de sécurité qui doivent 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 exigences de sécurité concernant les systèmes E/E/PE (voir 7.10 et 7.10.2.7 de la CEI 61508-1).

3.5.14
spécification des exigences concernant la conception des systèmes E/E/PE
spécification qui contient les exigences de conception des systèmes E/E/PE relatifs à la sécurité en termes des sous-systèmes et des éléments

3.5.15
logiciel de sécurité
logiciel utilisé pour exécuter des fonctions de sécurité dans un système relatif à la sécurité

3.5.16
mode de fonctionnement
mode de fonctionnement d'une fonction de sécurité qui peut être

– **mode faible sollicitation:** la fonction de sécurité n'est réalisée que sur sollicitation, afin de faire passer l'EUC dans un état de sécurité spécifié, et où la fréquence des sollicitations n'est pas supérieure à une par an, ou

NOTE Le système E/E/PE relatif à la sécurité qui réalise la fonction de sécurité n'a généralement pas d'influence sur l'EUC ou son système de commande jusqu'à l'occurrence d'une sollicitation. Cependant, si le système E/E/PE relatif à la sécurité n'est plus en mesure de réaliser la fonction de sécurité du fait d'une défaillance, il peut alors faire passer l'EUC à un état de sécurité (voir 7.4.6 de la CEI 61508-2).

– **mode sollicitation élevée:** la fonction de sécurité n'est réalisée que sur sollicitation, afin de faire passer l'EUC dans un état de sécurité spécifié, et où la fréquence des sollicitations est supérieure à une par an, ou

– **mode continu:** la fonction de sécurité maintient l'EUC dans un état de sécurité en fonctionnement normal

3.5.17
objectif chiffré de défaillance
probabilité prévisionnelle d'un mode de défaillance dangereux, à réaliser en fonction des exigences d'intégrité de sécurité, spécifiée en termes de

– probabilité moyenne d'une défaillance dangereuse lors de l'exécution sur sollicitation de la fonction de sécurité (en mode faible sollicitation),
– fréquence moyenne d'une défaillance dangereuse par heure [h^{-1}] (en mode sollicitation élevée ou en un mode continu)

NOTE Les valeurs numériques des objectifs chiffrés de défaillance sont présentées aux Tableaux 2 et 3 de la CEI 61508-1.

3.5.18
réduction de risque nécessaire
réduction de risque à réaliser par les systèmes E/E/PE relatifs à la sécurité et/ou par les dispositifs externes de réduction de risque afin d'assurer que le risque tolérable n'est pas dépassé

3.6 Anomalie, défaillance et erreur (voir Figure 4)

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

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

NOTE Le VEI 191-05-01 définit le terme '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. Voir la Figure 4 pour une illustration de ces deux points de vue.

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

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

NOTE La définition 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.

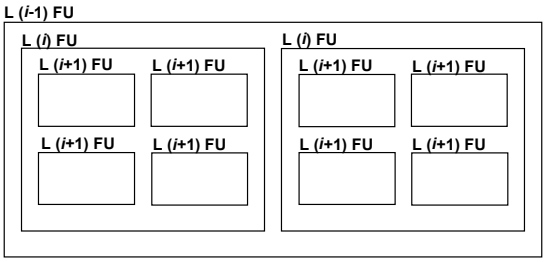
3.6.4
défaillance
cessation de l'aptitude d'une unité fonctionnelle à accomplir une fonction requise ou à fonctionner comme prévu

NOTE 1 Cette définition est fondée sur le VEI 191-04-01 avec des modifications apportées pour inclure les défaillances systématiques dues, par exemple, à des lacunes dans la spécification ou le logiciel.

NOTE 2 Voir la Figure 4 pour la relation entre anomalies (pannes) et défaillances, tant dans la série CEI 61508 que dans la CEI 60050-191.

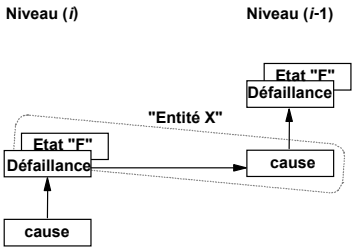
NOTE 3 L'accomplissement des fonctions requises exclut nécessairement certains comportements, et certaines fonctions peuvent être spécifiées en termes de comportement à éviter. L'occurrence d'un comportement à éviter est une défaillance.

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.

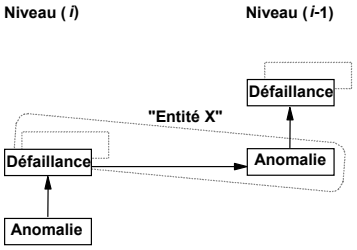


(L = niveau; *i* = 1, 2, 3 etc.; FU = unité fonctionnelle)

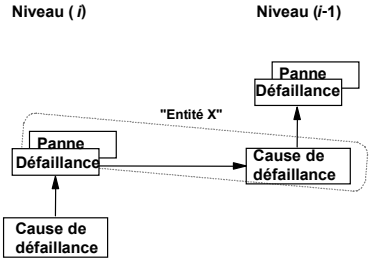
a) Configuration d'une unité fonctionnelle



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)

NOTE 1 Comme le montre a), une unité fonctionnelle peut être considérée comme organisée hiérarchiquement en plusieurs 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, à la suite de laquelle l'unité se trouve dans un état «F» où elle n'est plus apte à accomplir une fonction requise (voir b)). Cet état «F» de l'unité fonctionnelle de niveau (*i*) peut à son tour se manifester sous forme d'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 de 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 trouve après défaillance, et également comme la cause de la défaillance de l'unité fonctionnelle de niveau (*i*-1). Cette «Entité X» combine la notion de «fault» (en français «anomalie») dans la CEI 61508 et 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 série CEI 61508 et dans l'ISO/CEI 2382-14.

NOTE 3 Dans certains cas, une défaillance ou une erreur 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. Un exemple de ce type d'anomalie (ou panne) est une anomalie (ou une panne) de conception.

Figure 4 – Modèle de défaillance

3.6.5
défaillance aléatoire du matériel

défaillance survenant de manière aléatoire et résultant d'un ou de plusieurs mécanismes de dégradation potentiels au sein du matériel

NOTE 1 Il existe de nombreux 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 (c'est-à-dire 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 d'autres mesures appropriées), 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 du matériel peuvent être quantifiés de manière assez fiable, mais que ceux issus des défaillances systématiques ne peuvent être quantifiés de manière statistique avec précision du fait que les événements à leur origine ne peuvent être facilement prédits.

3.6.6
défaillance systématique
défaillance liée 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

[VEI 191-04-19]

NOTE 1 Une maintenance corrective sans modification n'élimine généralement pas la cause de la défaillance.

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

NOTE 3 Parmi les exemples de causes de défaillances systématiques figurent les erreurs humaines dans

– la spécification des exigences de sécurité,

– la conception, fabrication, installation et exploitation du matériel,

– la conception, mise en œuvre, 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 (voir 3.6.5) ou en défaillances systématiques.

3.6.7
défaillance dangereuse
défaillance d'un élément et/ou sous-système et/ou système ayant une influence sur la mise en œuvre de la fonction de sécurité qui:

a) empêche le fonctionnement nécessaire de la fonction de sécurité (mode de sollicitation) ou provoque la défaillance d'une fonction de sécurité (mode continu) de sorte que l'EUC est mis dans un état dangereux ou potentiellement dangereux, ou

b) diminue la probabilité que la fonction de sécurité fonctionne correctement lorsque c'est nécessaire

3.6.8
défaillance en sécurité
défaillance d'un élément et/ou sous-système et/ou système ayant une influence sur la mise en œuvre de la fonction de sécurité qui:

a) conduit au fonctionnement parasite de la fonction de sécurité avec la potentialité de mettre l'EUC (ou une partie de celui-ci) dans un état de sécurité ou de maintenir un état de sécurité, ou

b) augmente la probabilité du fonctionnement parasite de la fonction de sécurité avec potentialité de mettre l'EUC (ou une partie de celui-ci) dans un état de sécurité ou de maintenir un état de sécurité

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

NOTE Deux événements A et B sont dépendants si, et seulement si*:* $P(\text{A et B}) > P(\text{A}) \times P(\text{B})$.

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

[VEI 191-05-24, modifiée]

3.6.12
erreur intermittente
modifications erronées du contenu des données sans modification du circuit physique lui-même

NOTE 1 Après occurrence d'une erreur intermittente et réécriture des données, le circuit est rétabli dans son état d'origine.

NOTE 2 Les erreurs intermittentes peuvent se produire dans la mémoire, la logique numérique, les circuits analogiques et les lignes de transmission, etc. Elles prédominent dans la mémoire à semi-conducteurs, y compris les registres et les verrous. Des données peuvent être obtenues, par exemple, auprès des fabricants.

NOTE 3 Les erreurs intermittentes sont temporaires, et il convient de ne pas les confondre avec les erreurs de programmation de logiciel.

3.6.13
défaillance partielle
défaillance d'un composant n'ayant pas d'influence sur la mise en œuvre de la fonction de sécurité

NOTE La défaillance partielle n'est pas utilisée pour les calculs de SFF.

3.6.14
défaillance sans effet
défaillance d'un élément ayant une influence sur la mise en œuvre de la fonction de sécurité mais sans effet direct sur la fonction de sécurité

NOTE 1 La défaillance sans effet n'a par définition aucun effet sur la fonction de sécurité, elle ne peut de ce fait pas contribuer au taux de défaillance de la fonction de sécurité.

NOTE 2 La défaillance sans effet n'est pas utilisée pour les calculs de SFF.

3.6.15
proportion de défaillances en sécurité
SFF
propriété d'un élément relatif à la sécurité définie par le rapport des taux de défaillance moyens des défaillances en sécurité et dangereuses détectées et des défaillances en sécurité et dangereuses. Ce rapport est représenté par l'équation suivante:

$$SFF = (\Sigma\lambda_{S\ avg} + \Sigma\lambda_{Dd\ avg})/(\Sigma\lambda_{S\ avg} + \Sigma\lambda_{Dd\ avg} + \Sigma\lambda_{Du\ avg})$$

lorsque les taux de défaillance sont basés sur des taux de défaillance constants, l'équation peut être simplifiée comme suit:

$$SFF = (\Sigma\lambda_{S} + \Sigma\lambda_{Dd})/(\Sigma\lambda_{S} + \Sigma\lambda_{Dd} + \Sigma\lambda_{Du})$$

3.6.16
taux de défaillance
paramètre de fiabilité ($\lambda(t)$) d'une entité (composants ou systèmes simples) tel que $\lambda(t).dt$ est la probabilité de défaillance de cette entité comprise dans les limites [t, $t+dt$], à condition qu'aucune défaillance ne se soit produite pendant [0, t]

NOTE 1 D'un point de vue mathématique, $\lambda(t)$ est la probabilité conditionnelle de défaillance par unité de temps pendant [t, t+dt]. Elle est en relation étroite avec la fonction de fiabilité (c'est-à-dire la probabilité d'aucune défaillance de 0 à t) par la formule générale

$R(t) = \exp(-\int_0^t \lambda(\tau) d\tau$. Inversement, elle est définie à partir de la fonction de fiabilité par $\lambda(t) = -\frac{dR(t)}{dt}\frac{1}{R(t)}$.

NOTE 2 Les taux de défaillance et leurs incertitudes peuvent être estimés à partir du retour d'exploitation en utilisant les statistiques conventionnelles. Pendant la « durée de vie utile » (c'est-à-dire après le déverminage et avant l'usure), le taux de défaillance d'un article simple est plus ou moins constant, $\lambda(t) \equiv \lambda$.

NOTE 3 La moyenne de $\lambda(t)$ pendant une période donnée [0, T], $\lambda_{avg}(T) = (\int_0^T \lambda(\tau) d\tau) / T$, ne représente pas un taux de défaillance car elle ne peut pas être utilisée pour le calcul de R(t) comme indiqué à la Note 1. Elle peut toutefois être interprétée comme la fréquence moyenne de défaillance sur cette période (c'est-à-dire la PFH, voir Annexe B de la CEI 61508-6).

NOTE 4 Le taux de défaillance d'une série d'articles est la somme des taux de défaillance de chaque article.

NOTE 5 Le taux de défaillance de systèmes redondants est généralement non constant. Néanmoins, lorsque toutes les défaillances sont révélées rapidement, sont indépendantes et rapidement réparées, $\lambda(t)$ tend rapidement vers une valeur asymptotique λ_{as} correspondant au *taux de défaillance équivalent* des systèmes. Il convient de ne pas le confondre avec le taux de défaillance moyen décrit à la Note 3 qui ne tend pas nécessairement vers une valeur asymptotique.

3.6.17
probabilité de défaillance dangereuse en cas de sollicitation
PFD
indisponibilité de sécurité (voir CEI 60050-191) d'un système E/E/PE relatif à la sécurité pour réaliser la fonction de sécurité spécifiée sur sollicitation de l'EUC ou de son système de commande

NOTE 1 L'indisponibilité [instantanée] (selon la CEI 60050-191) est la probabilité qu'un article ne soit pas en mesure de réaliser une fonction requise dans des conditions données à un moment donné, en supposant l'existence des ressources externes requises. Elle est généralement exprimée par U (t).

NOTE 2 La disponibilité [instantanée] ne dépend pas des états (en fonctionnement ou en défaillance) dans lesquels l'article se trouve avant t. Elle caractérise un article qui doit uniquement être apte à fonctionner lorsqu'il doit le faire, par exemple, un système E/E/PE relatif à la sécurité fonctionnant en mode faible sollicitation.

NOTE 3 Si elle est vérifiée périodiquement, la PFD d'un système E/E/PE relatif à la sécurité est, par rapport à la fonction de sécurité spécifiée, représentée par une courbe en dents de scie avec une large gamme de probabilités comprises entre un niveau minimal, juste après un essai, et un niveau maximal, juste avant un essai.

3.6.18
probabilité moyenne de défaillance dangereuse en cas de sollicitation
PFD_{avg}
indisponibilité moyenne (voir CEI 60050-191) d'un système E/E/PE relatif à la sécurité pour réaliser la fonction de sécurité spécifiée sur sollicitation de l'EUC ou de son système de commande

NOTE 1 L'indisponibilité moyenne pendant un intervalle de temps donné [t1, t2] est généralement exprimée par U (t1, t2).

NOTE 2 Deux types de défaillances contribuent à la PFD et à la PFD_{avg}: les *défaillances dangereuses non détectées* s'étant produites depuis le dernier essai périodique et les *défaillances sur sollicitation* réelles engendrées par les sollicitations (essais périodiques et sollicitations de sécurité) elles-mêmes. Les premières défaillances *dépendent du temps* et sont caractérisées par leur taux de défaillance dangereuse $\lambda_{DU}(t)$ alors que les secondes défaillances ne dépendent que du nombre de sollicitations et sont caractérisées par une *probabilité de défaillance par sollicitation* (exprimée par γ).

NOTE 3 Dans la mesure où les défaillances sur sollicitation réelles ne peuvent pas être détectées par des essais, il est nécessaire de les identifier et d'en tenir compte lors du calcul des objectifs chiffrés de défaillance.

3.6.19
fréquence moyenne de défaillance dangereuse par heure
PFH
fréquence moyenne d'une défaillance dangereuse d'un système E/E/PE relatif à la sécurité pour réaliser la fonction de sécurité spécifiée pendant une période de temps donnée

NOTE 1 Le terme « probabilité de défaillance dangereuse par heure » n'est pas utilisé dans la présente norme, mais l'acronyme PFH a été conservé et signifie, lorsqu'il est employé, « fréquence moyenne de défaillance dangereuse [h-1] ».

NOTE 2 D'un point de vue théorique, la PFH est la moyenne de l'*intensité de défaillance inconditionnelle*, également désignée *fréquence de défaillance*, et qui est généralement exprimée par w(t). Il convient de ne pas la confondre avec un taux de défaillance (voir l'Annexe B de la CEI 61508-6).

NOTE 3 Lorsque le système E/E/PE relatif à la sécurité constitue la dernière couche de sécurité, il convient de calculer la PFH à partir de sa *non fiabilité* F(T)=1-R(t) (voir « taux de défaillance » ci-dessus). Lorsqu'il ne s'agit pas du dernier système relatif à la sécurité, il convient de calculer sa PFH à partir de son *indisponibilité* U(t) (voir PFD ci-dessus). Les approximations de PFH sont données par F(T)/T et 1/MTTF dans le premier cas et par 1/MTBF dans le second cas.

NOTE 4 Lorsque le système E/E/PE relatif à la sécurité n'implique que des défaillances révélées réparées rapidement, un taux de défaillance asymptotique λ_{as} est rapidement atteint. Il fournit une estimation de la PFH.

3.6.20
temps de sécurité du processus
durée entre l'occurrence d'une défaillance, avec potentialité de donner lieu à un événement dangereux, se produisant dans l'EUC ou son système de commande et le temps nécessaire pour accomplir l'action dans l'EUC pour empêcher l'occurrence de l'événement dangereux

3.6.21
durée moyenne de rétablissement
MTTR
durée prévue de rétablissement effectif

NOTE La MTTR comprend:

- le temps de détection de la défaillance (a), et
- le temps écoulé avant de commencer la réparation (b), et
- le temps de réparation effectif (c), et
- le temps écoulé avant la remise en fonctionnement du composant (d)

Le temps de démarrage applicable à (b) est la fin du temps (a); le temps de démarrage applicable à (c) est la fin du temps (b) et le temps de démarrage applicable à (d) est la fin du temps (c).

3.6.22
temps moyen de dépannage
MRT
temps de dépannage total prévu

NOTE Le MRT comprend les temps (b), (c) et (d) pour les durées applicables à la MTTR (voir 3.6.21).

3.7 Activités liées au cycle de vie

3.7.1
cycle de vie de sécurité
activités nécessaires à la mise en œuvre 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 et des dispositifs externes de réduction de risque ne sont plus disponibles pour une utilisation

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

NOTE 2 Les modèles de cycle de vie de sécurité utilisés dans la présente norme sont spécifiés aux Figures 2, 3 et 4 de la CEI 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 d'un logiciel inclut généralement une phase d'exigences, 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
référentiel de configuration
informations permettant de recréer la version du logiciel de manière vérifiable et systématique, comprenant: tous les codes source, données, fichiers d'exécution, documentation, fichiers de configuration et macro-instructions d'installation comprenant une version du logiciel, des informations sur les compilateurs, les systèmes d'exploitation et les outils de développement utilisés pour créer la version du logiciel

3.7.5
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 ont été satisfaites

[ISO 8402, définition 2.17, modifiée]

NOTE 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, système E/E/PE et logiciel), à démontrer par analyse, raisonnement mathématique et/ou essais que, pour les entrées spécifiques, les éléments livrables remplissent en tout point les objectifs et les exigences fixés pour la phase spécifique.

EXEMPLE Les activités de vérification incluent:

– les revues relatives aux sorties d'une phase (documents concernant toutes les phases du cycle de vie de sécurité) destinées à assurer la conformité aux objectifs et aux exigences de la phase, en tenant compte des entrées spécifiques à cette phase,

– les revues de conception,

– les essais réalisés sur les produits conçus afin d'assurer que leur fonctionnement est conforme à leur spécification,

– les essais d'intégration réalisés lors de l'assemblage, élément par élément, de différentes parties d'un système et la réalisation 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

[ISO 8402, définition 2.18, modifiée]

NOTE 1 La présente norme spécifie trois phases de validation:

– validation de sécurité générale (voir Figure 2 de la CEI 61508-1),

– validation des systèmes E/E/PE (voir Figure 3 de la CEI 61508-1),

– validation du logiciel (voir Figure 4 de la CEI 61508-1).

NOTE 2 La validation est l'activité qui consiste à démontrer que le système relatif à la sécurité considéré, avant ou après installation, correspond en tout point aux exigences de sécurité contenues dans la spécification de ce système relatif à la 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 exigences de sécurité du logiciel.

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 E/E/PE relatifs à la sécurité et/ou 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 exigences concernant la sécurité fonctionnelle sont conformes aux procédures prévues, sont effectivement mises en œuvre 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
essai périodique
essai périodique destiné à détecter les défaillances dangereuses cachées d'un système relatif à la sécurité de telle sorte que, si nécessaire, une réparation puisse rétablir le système dans une condition « comme neuf » ou dans une condition aussi proche que possible de celle-ci

NOTE 1 La présente norme utilise le terme « essai périodique », mais il existe un synonyme: « test d'épreuve ».

NOTE 2 L'efficacité de l'essai périodique dépend à la fois de la couverture des défaillances et de l'efficacité de la réparation. Dans la pratique, il n'est pas facile de détecter 100 % des défaillances dangereuses cachées pour des systèmes autres que les systèmes E/E/PE relatifs à la sécurité de faible complexité. Il convient de conserver cet objectif. Au minimum, toutes les fonctions de sécurité qui sont exécutées sont contrôlées selon la spécification des exigences de sécurité des systèmes E/E/PE. Si des canaux séparés sont utilisés, ces essais sont réalisés séparément pour chacun des canaux. Pour des éléments complexes, il peut se révéler nécessaire d'effectuer une analyse pour démontrer que la probabilité de défaillance dangereuse cachée non détectée par des essais périodiques est négligeable pendant toute la durée de vie du système E/E/PE relatif à la sécurité.

NOTE 3 La réalisation d'un essai périodique nécessite un certain temps. Pendant ce temps, le système E/E/PE relatif à la sécurité peut être inhibé en totalité ou en partie. La durée de l'essai périodique peut ne pas être prise en compte uniquement si la partie du système E/E/PE relatif à la sécurité soumise à l'essai reste disponible, en cas de sollicitation de fonctionnement ou si l'EUC est arrêté pendant l'essai.

NOTE 4 Pendant un essai périodique, le système E/E/PE relatif à la sécurité peut être indisponible, en totalité ou en partie, pour réagir à une sollicitation de fonctionnement. La MTTR (durée moyenne de réparation) peut ne pas être prise en compte pour les calculs de SIL uniquement si l'EUC est arrêté pendant la réparation ou si les dispositifs externes de réduction de risque sont installés et présentent une efficacité équivalente.

3.8.6
couverture du diagnostic
DC
proportion de défaillances dangereuses détectées par les essais de diagnostic en ligne automatiques. La proportion de défaillances dangereuses est calculée en divisant les taux de défaillance dangereuse associés aux défaillances dangereuses détectées par le taux total des défaillances dangereuses

NOTE 1 La couverture du diagnostic de défaillance dangereuse est calculée selon l'équation suivante, dans laquelle *DC* est la couverture du diagnostic, λ_{DD} est la probabilité de détection d'une défaillance dangereuse et $\lambda_{D\ total}$ est la probabilité de toutes les défaillances dangereuses:

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

NOTE 2 Cette définition s'applique sous réserve que les composants individuels présentent des taux de défaillance constants.

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

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

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

NOTE Une défaillance dangereuse détectée par essai de diagnostic se comporte comme une défaillance révélée. Elle ne se comporte comme une défaillance en sécurité que si des mesures, automatiques ou manuelles, sont prises à cet effet.

3.8.9
non détecté
non révélé
non déclaré
se rapporte au matériel et signifie non détecté par les essais de diagnostic, les essais périodiques, une intervention de l'opérateur (par exemple, une inspection physique et des essais 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
évaluateur
personne(s) ou organisme chargé(s) de l'évaluation de la sécurité fonctionnelle afin de parvenir à un jugement sur la sécurité fonctionnelle atteinte par les systèmes E/E/PE relatifs à la sécurité et les dispositifs externes de réduction de risque

NOTE Voir également l'Article 8 de la CEI 61508-1.

3.8.11
personne indépendante
personne distinctement séparée des personnes responsables des activités qui se déroulent lors de la phase spécifique du cycle de vie de sécurité total des systèmes E/E/PE 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

3.8.12
département indépendant
département distinctement séparé des départements responsables des activités qui se déroulent lors de la phase spécifique du cycle de vie de sécurité total des systèmes E/E/PE ou du logiciel, chargé de l'évaluation de la sécurité fonctionnelle ou de la validation

3.8.13
organisme indépendant
organisme distinctement séparé, par sa direction et ses autres ressources, des organismes responsables des activités qui se déroulent lors de la phase spécifique du cycle de vie de sécurité total des systèmes E/E/PE ou du logiciel, chargée de l'évaluation de la sécurité fonctionnelle ou de la validation

3.8.14
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 par exemple 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 apporter une confiance supplémentaire en ce que le système remplit les exigences réelles car elle améliore la prise de conscience du comportement spécifié.

3.8.15
essai 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 L'essai dynamique diffère de l'analyse statique, qui n'exige pas l'exécution du logiciel ou le fonctionnement du matériel.

3.8.16
simulateur d'essai
moyen capable de simuler pendant le développement (jusqu'à un certain degré d'utilité) l'environnement du logiciel ou du matériel en exploitation en appliquant des cas d'essai au logiciel et en enregistrant la réponse

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

3.8.17
manuel de sécurité pour article conforme
document qui fournit toutes les informations relatives à la sécurité fonctionnelle d'un élément par rapport aux fonctions de sécurité spécifiées de l'élément, et qui est nécessaire pour garantir que le système satisfait aux exigences de la série CEI 61508

3.8.18
éprouvé par une utilisation antérieure
démonstration, réalisée sur la base d'une analyse de l'expérience d'exploitation pour une configuration spécifique d'un élément, que la probabilité d'anomalies systématiques dangereuses est suffisamment faible pour que chaque fonction de sécurité qui utilise l'élément puisse atteindre son niveau d'intégrité de sécurité requis

Bibliographie

[1] CEI 61511 (toutes les parties), *Sécurité fonctionnelle – Systèmes instrumentés de sécurité pour le secteur des industries de transformation*

[2] CEI 62061:2005, *Sécurité des machines – Sécurité fonctionnelle des systèmes de commande électriques, électroniques et électroniques programmables relatifs à la sécurité*

[3] CEI 61800-5-2, *Adjustable speed electrical power drive systems – Part 5-2: Safety requirements – Functional* (disponible en anglais seulement)

[4] CEI 61508-5 :2010, *Sécurité 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*

[5] CEI 61508-6 :2010 *Sécurité fonctionnelle des systèmes électriques/ électroniques/ électroniques programmables relatifs à la sécurité – Partie 6: Lignes directrices pour l'application de la CEI 61508-2 et de la CEI 61508-3*

[6] CEI 61508-7 :2010, *Sécurité fonctionnelle des systèmes électriques / électroniques / électroniques programmables relatifs à la sécurité – Partie 7: Présentation de techniques et mesures*

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

[8] CEI 61131-3:2003, *Programmable controllers – Part 3: Programming languages* (disponible en anglais seulement)

[9] CEI/TR 62059-11, *Equipements de comptage de l'électricité – Sûreté de fonctionnement – Partie 11: Concepts généraux*

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

[11] CEI 60601 (toutes les parties), *Appareils électromédicaux*

[12] CEI 60050-191:1990, *Vocabulaire Electrotechnique International – Chapitre 191: Sûreté de fonctionnement et qualité de service*

[13] CEI 60050-351:2006, *Vocabulaire Electrotechnique International – Partie 351: Technologie de commande et de régulation*

[14] CEI 61508-1 :2010 *Sécurité fonctionnelle des systèmes électriques/ électroniques/ électroniques programmables relatifs à la sécurité – Partie 1: Exigences générales*

[15] CEI 61508-2 : 2010 *Sécurité fonctionnelle des systèmes électriques/ électroniques/ électroniques programmables relatifs à la sécurité – Partie 2: Exigences concernant les systèmes électriques/ électroniques/électroniques programmables relatifs à la sécurité*

[16] CEI 61508-3 : 2010 *Sécurité fonctionnelle des systèmes électriques/ électroniques /électroniques programmables relatifs à la sécurité – Partie 3: Exigences concernant les logiciels*

[17] ISO/CEI 2382-14:1997, *Technologies de l'information – Vocabulaire – Partie 14: Fiabilité, maintenabilité et disponibilité*

[18] ISO 9000:2005, *Systèmes de management de la qualité – Principes essentiels et vocabulaire*

Index

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

3, rue de Varembé
PO Box 131
CH-1211 Geneva 20
Switzerland

Tel: + 41 22 919 02 11
Fax: + 41 22 919 03 00
info@iec.ch
www.iec.ch