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 It also gives information on projects, withdrawn and replaced publications.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.

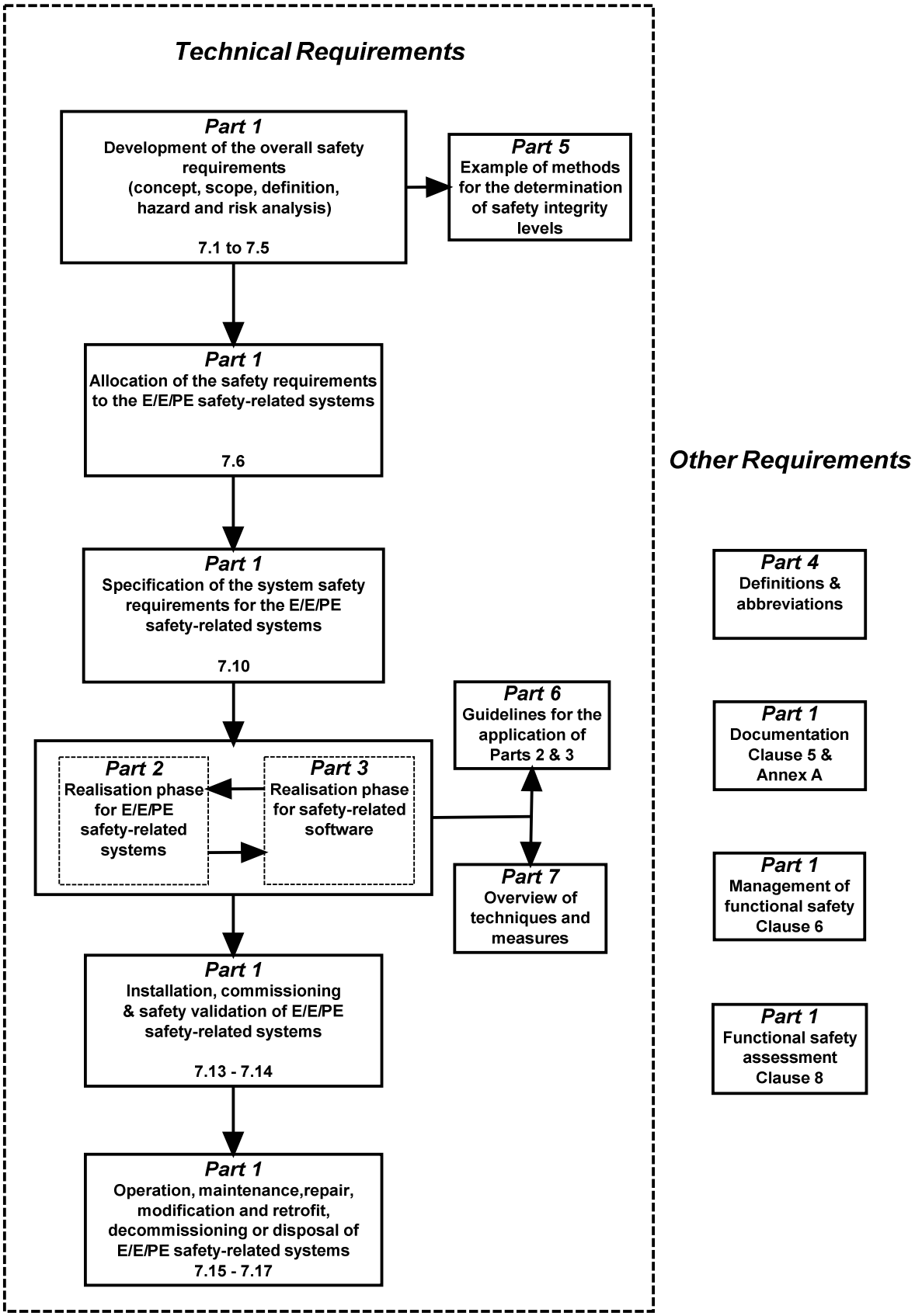


Figure 1 – Overall framework of the IEC 61508 series

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

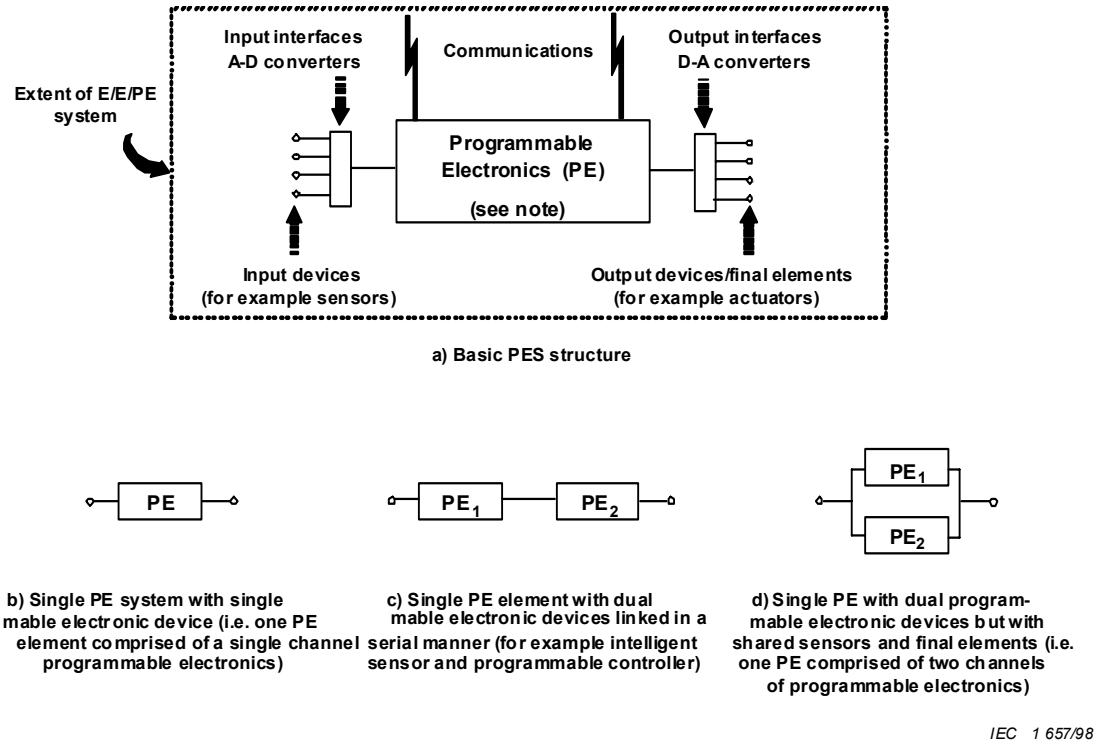
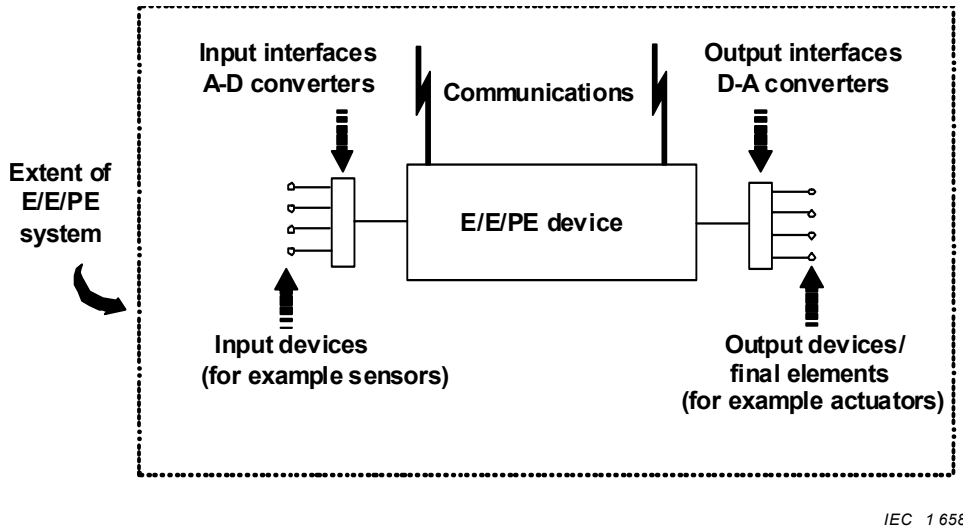


Figure 2 – Programmable electronic system

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.

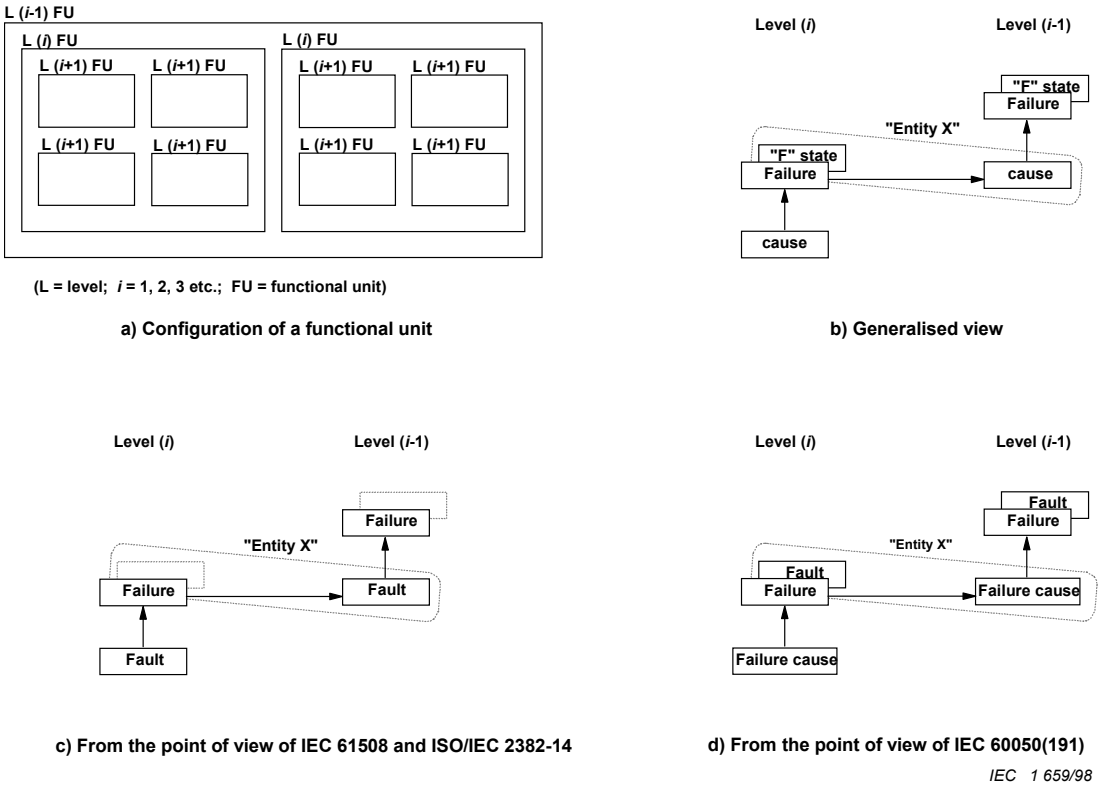
3.6.4
failure
termination of the ability of a functional unit to provide a required function or operation of a functional unit in any way other than as required

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.



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