COMMISSION ELECTROTECHNIQUE INTERNATIONALE **CEI IEC 61508-4**

INTERNATIONAL ELECTROTECHNICAL COMMISSION

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

Part 4: Definitions and abbreviations

Contents

Figures

Tables

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

Part 4: Definitions and abbreviations

FOREWORD

1) The IEC (International Electrotechnical Commission) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC national committees). The object of the IEC is to promote international cooperation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, the IEC publishes international standards. Their preparation is entrusted to technical committees; any IEC national committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. The IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.

2) The formal decisions or agreements of the IEC on technical matters, prepared by technical committees on which all the national committees having a special interest therein are represented, express, as nearly as possible, an international consensus of opinion on the subjects dealt with.

3) They have the form of recommendations for international use published in the form of standards, technical reports or guides and they are accepted by the national committees in that sense.

4) In order to promote international unification, IEC national committees undertake to apply IEC international standards transparently to the maximum extent possible in their national and regional standards. Any divergence between the IEC standard and the corresponding national or regional standard shall be clearly indicated in the latter.

5) Attention is drawn to the possibility that some of the elements of IEC 61508 may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

6) The IEC has not laid down any procedure concerning marking as an indication of approval and has no responsibility when an item of equipment is declared to comply with one of its standards.

IEC 61508-4 has been prepared by sub-committee 65A: System aspects, of IEC technical committee FORMTEXT65: Industrial process measurement and controlFORMTEXT.

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

FDIS	Report on voting
65A/xxx	65A/xxx

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

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

— Part 1: General requirements;

— Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems;

— Part 3: Software requirements;

— Part 4: Definitions and abbreviations;

— Part 5: Examples of methods for the determination of safety integrity levels;

— Part 6: Guidelines on the application of parts 2 and 3;

— Part 7: Overview of techniques and measures.

This part 4 is to be used in conjunction with all other parts.

Introduction

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

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

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

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

This standard:

— considers all relevant overall, E/E/PES and software safety lifecycle phases (for example, from initial concept, through design, implementation, operation and maintenance to decommissioning) when E/E/PESs are used to perform safety functions;

— has been conceived with a rapidly developing technology in mind – the framework is sufficiently robust and comprehensive to cater for future developments;

— enables application sector international standards, dealing with safety-related E/E/PESs, to be developed – the development of application sector international standards, within the framework of this standard, should lead to a high level of consistency (for example, of underlying principles, terminology etc) both within application sectors and across application sectors; this will have both safety and economic benefits;

— provides a method for the development of the safety requirements specification necessary to achieve the required functional safety for E/E/PE safety-related systems;

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

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

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

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

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

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

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

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

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

Part 4: Definitions and abbreviations

1 Scope

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

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

1.3 Parts 1, 2, 3 and 4 of this standard are basic safety publications, although this status does not apply in the context of low complexity E/E/PE safety-related systems (see 3.4.4). As basic safety publications, they are intended for use by Technical Committees in the preparation of standards in accordance with the principles contained in ISO/IEC Guide 104 and ISO/IEC Guide 51. One of the responsibilities of a Technical Committee is, wherever applicable, to make use of basic safety publications in the preparation of its own publications. IEC 61508 is also intended for use as a stand-alone standard.

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

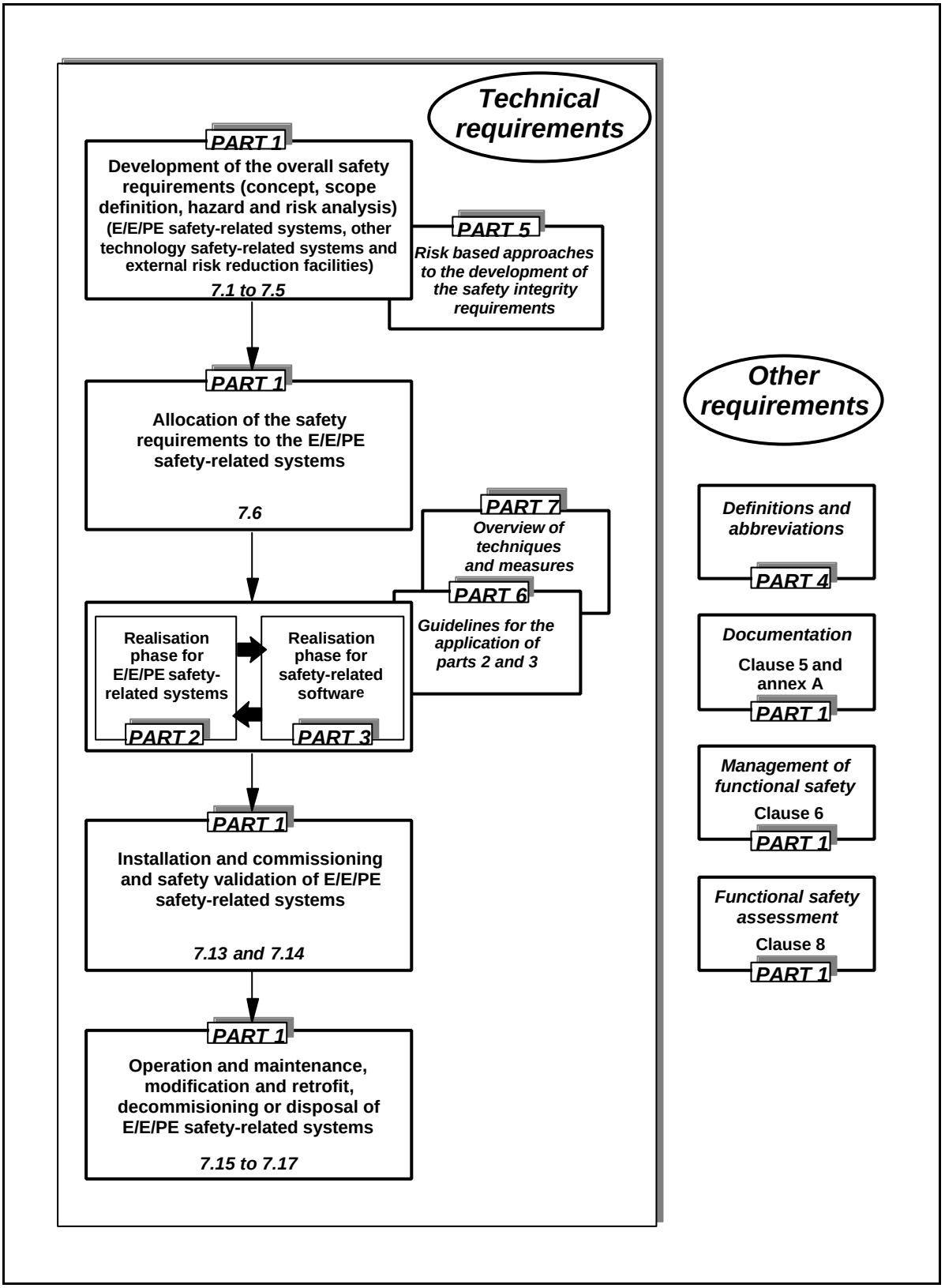


Figure 1 — Overall framework of this standard

2 Normative references

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

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

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

ISO/IEC 2382-14:1996, *Information technology – Vocabulary – Part 14: Reliability, maintainability and availability*

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

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

3 Definitions and abbreviations

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

Table 1 — Abbreviations used in this standard

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

3.1 Safety terms

3.1.1
harm
physical injury or damage to the health of people either directly, or indirectly as a result of damage to property or to the environment

[ISO/IEC Guide 51 second edition (1997 draft)]

3.1.2
hazard
potential source of harm

NOTE 1 Adapted from ISO/IEC Guide 51 second edition (1997 draft) by excluding the note.

NOTE 2 The term includes danger to persons arising within a short time scale (for example, fire and explosion) and also those that have a long term effect on a person's health (for example, release of a toxic substance).

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

[ISO/IEC Guide 51 second edition (1997 draft)]

3.1.4
hazardous event
hazardous situation which results in harm

[ISO/IEC Guide 51 second edition (1997 draft)]

3.1.5
risk
combination of the probability of occurrence of harm and the severity of that harm

[ISO/IEC Guide 51 second edition (1997 draft)]

NOTE For more discussion on this concept see annex A of part 5.

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

[ISO/IEC Guide 51 second edition (1997 draft)]

NOTE See annex B of part 5.

3.1.7
residual risk
risk remaining after protective measures have been taken

[ISO/IEC Guide 51 second edition (1997 draft)]

3.1.8
safety
freedom from unacceptable risk

[ISO/IEC Guide 51 second edition (1997 draft)]

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

3.1.10
safe state
state of the EUC when safety is achieved

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

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

[ISO/IEC Guide 51 second edition (1997 draft)]

3.2 Equipment and devices

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

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

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

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

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

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

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

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

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

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

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

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

3.2.5
programmable electronic
based on computer technology which may comprise of hardware, software, and of input and/or output units

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

EXAMPLE The following are all programmable electronic devices:

— microprocessors;

— micro-controllers;

— programmable controllers;

— application specific integrated circuits (ASICs);

— programmable logic controllers (PLCs);

— other computer based devices (for example smart sensors, transmitters, actuators).

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

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

EXAMPLE Electrical/electronic/programmable electronic devices include:

— electro-mechanical devices (electrical);

— solid state non-programmable electronic devices (electronic);

— electronic devices based on computer technology (programmable electronic) - see 3.2.5.

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

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

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

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

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

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

3.3 Systems: general aspects

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

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

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

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

NOTE The structure of a PES is shown in figure 2 a). Figure 2 b) illustrates the way in which a PES is represented in this 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 (ie two channel), but with a single sensor and a single actuator.

3.3.3
electrical/electronic/programmable electronic system (E/E/PES)
system for control, protection or monitoring based on one or more 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 3)

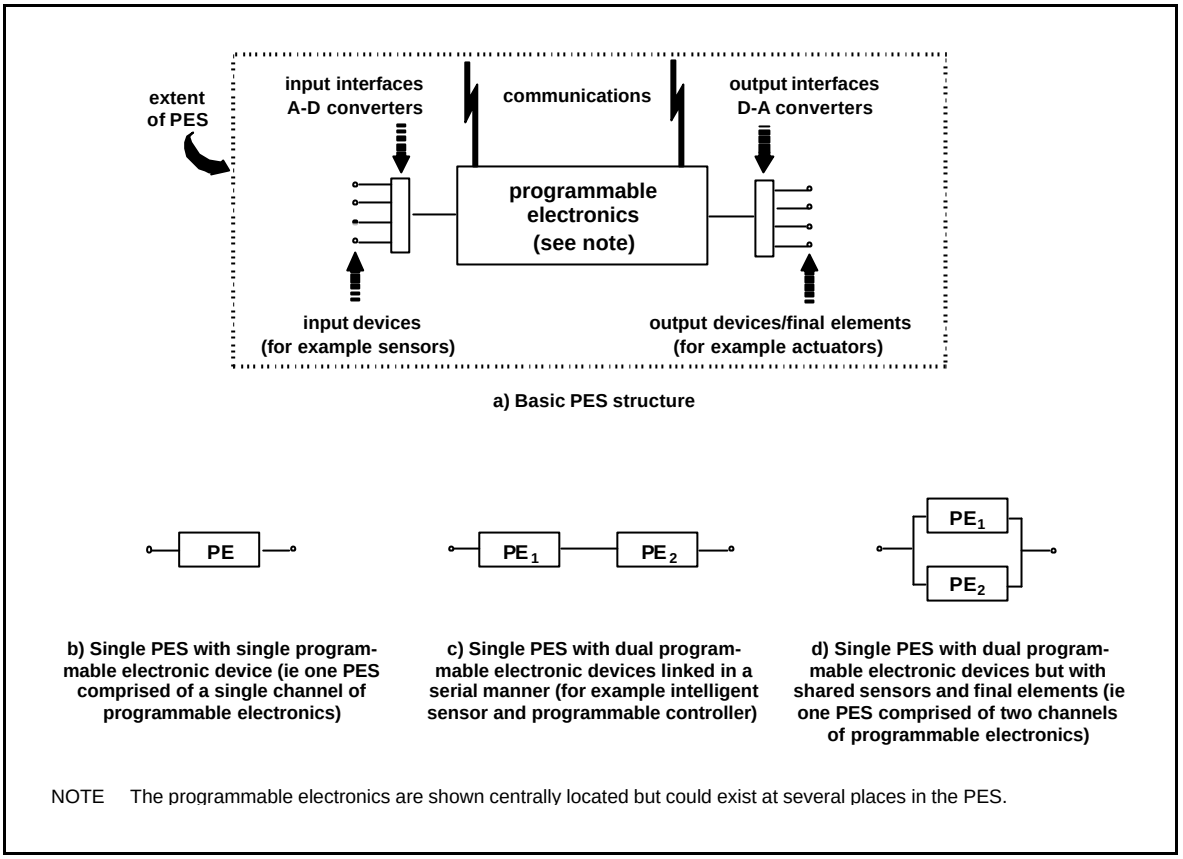
3.3.4
EUC control system
system which responds to input signals from the process and/or from an operator and generates output signals causing the EUC to operate in the desired manner

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

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

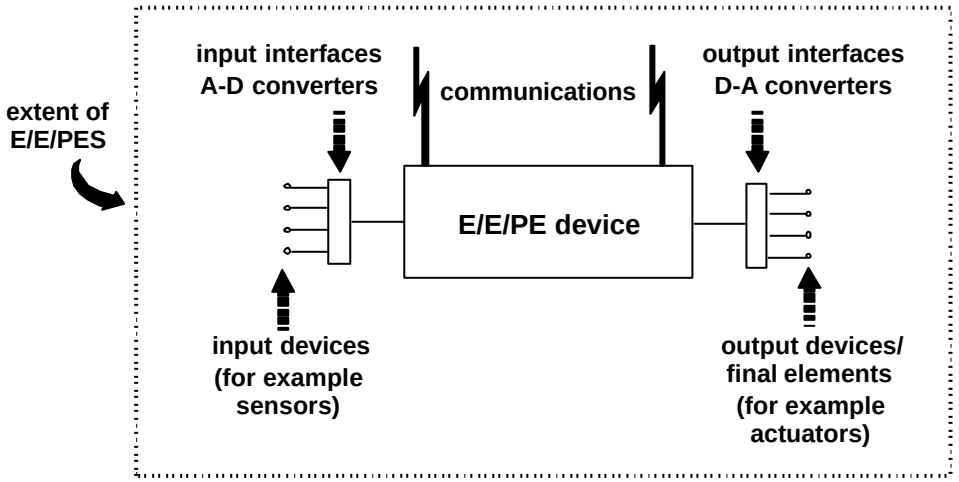
3.3.6
module
routine, discrete component or a functional set of encapsulated routines or discrete components belonging together

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



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

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



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

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

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

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

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

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

3.3.9
diversity
different means of performing a required function

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

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

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

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

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

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

3.4 Systems: safety-related aspects

3.4.1
safety-related system
designated system that both:

— implements the required safety functions necessary to achieve or maintain a safe state for the EUC; and

— is intended to achieve, on its own or with other E/E/PE safety-related systems, other technology safety-related systems or external risk reduction facilities, the necessary safety integrity for the required safety functions

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

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

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

NOTE 4 A safety-related system may:

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

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

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

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

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

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

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

EXAMPLE A relief valve is an other technology safety-related system.

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

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

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

— the failure modes of each individual component are well defined; and

— the behaviour of the system under fault conditions can be completely determined

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

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

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

NOTE In this standard the following logic systems are used:

— electrical logic systems for electro-mechanical technology;

— electronic logic systems for electronic technology;

— programmable electronic logic systems for programmable electronic systems.

3.5 Safety functions and safety integrity

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

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

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

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

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

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

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

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

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

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

NOTE 2 See 3.5.2, 3.5.5 and 3.6.6.

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

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

NOTE 2 See 3.5.2, 3.5.4 and 3.6.5.

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

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

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

NOTE See 3.5.3 and 3.5.6.

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

NOTE This specification is divided into the:

— safety functions requirements specification (see 3.5.9);

— safety integrity requirements specification (see 3.5.10).

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

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

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

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

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

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

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

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

— **high demand or continuous mode** – where the frequency of demands for operation made on a safety-related system is greater than one per year or greater than twice the proof check frequency

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

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

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

— the average probability of failure to perform the design function on demand (for a low demand mode of operation); or

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

NOTE The numerical values for the target failure measures are given in tables 2 and 3 of part 1.

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

3.6 Fault, failure and error

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

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

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

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

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

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

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

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

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

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

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

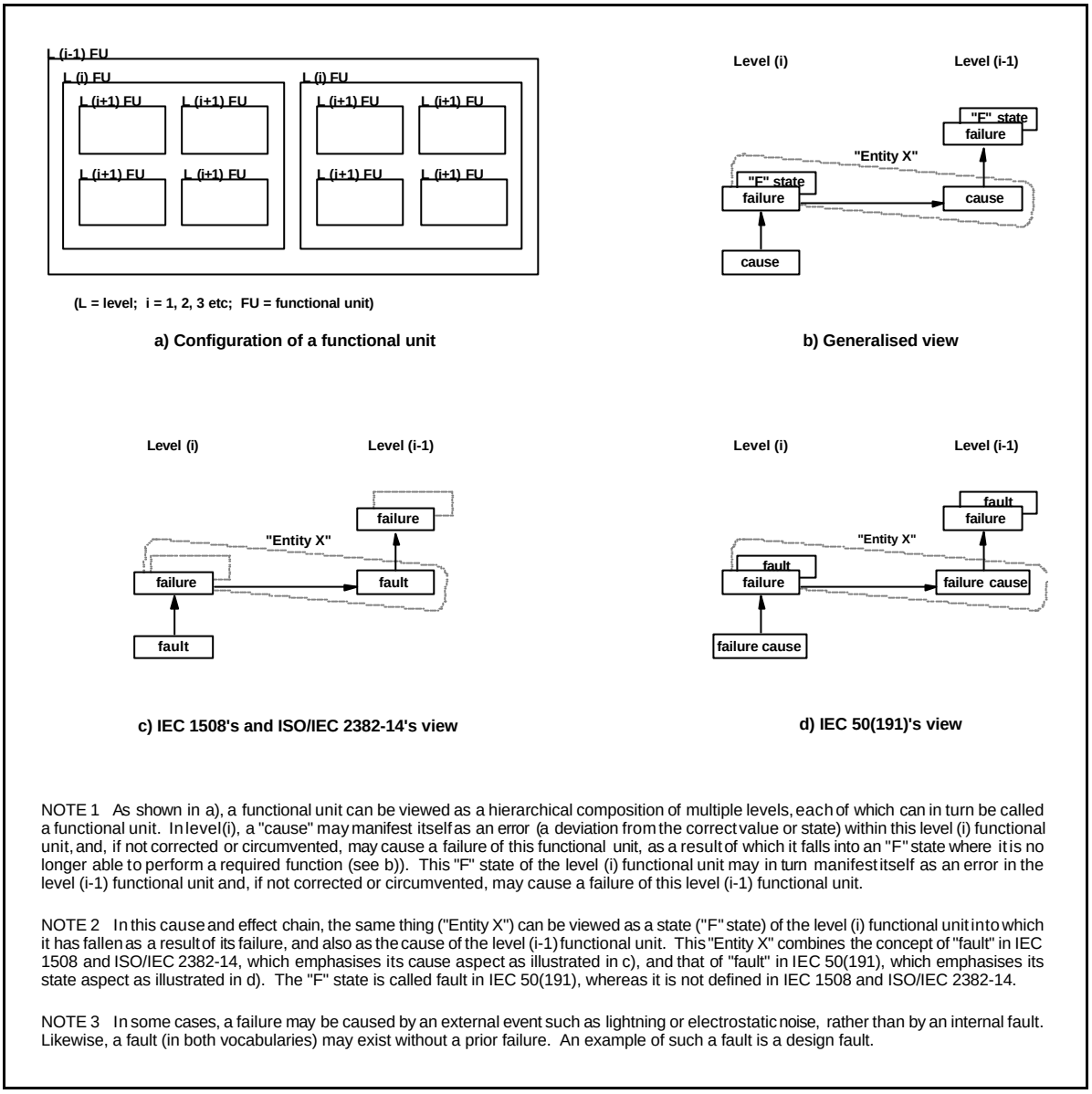
NOTE 3 Performance of required functions necessarily excludes certain behaviour, and some functions may be specified in terms of behaviour to be avoided. The occurrence of such behaviour is a failure.

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

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

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



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 level (i-1) functional unit. This "Entity X" combines the concept of "fault" in IEC 1508 and ISO/IEC 2382-14, which emphasises its cause aspect as illustrated in c), and that of "fault" in IEC 50(191), which emphasises its state aspect as illustrated in d). The "F" state is called fault in IEC 50(191), whereas it is not defined in IEC 1508 and ISO/IEC 2382-14.

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

Figure 4 — Failure model

3.6.6
systematic failure
failure related in a deterministic way to a certain cause, which can only be eliminated by a modification of the design or of the manufacturing process, operational procedures, documentation or other relevant factors

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

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

[IEV 191-04-19]

NOTE 3 Examples 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 categorised as random hardware failures or systematic failures (see 3.6.4 and 3.6.5).

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

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

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

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

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

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

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

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

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

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

3.6.12
human error
mistake
human action or inaction that produces an unintended result

[ISO/IEC 2382-14-02-03]

NOTE Adapted from IEV 191-05-25 by the addition of “or inaction”.

3.7 Lifecycle activities

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

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

NOTE 2 The safety lifecycle models used in this standard are specified in figures 2, 3 and 4 of part 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 disused

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

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

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

NOTE For details on software configuration management see C.5.24 of part 7.

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

NOTE In the context of software, see C.5.23 of part 7.

3.8 Confirmation of safety measures

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

NOTE 1 Adapted from ISO 8402 by excluding the notes.

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

EXAMPLE Verification activities include:

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

— design reviews;

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

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

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

NOTE 1 Adapted from ISO 8402 by excluding the notes.

NOTE 2 In this standard there are three validation phases:

— overall safety validation (see figure 2 of part 1);

— E/E/PES validation (see figure 3 of part 1); and

— software validation (see figure 4 of part 1).

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Index