COMMISSION ELECTROTECHNIQUE INTERNATIONALE

INTERNATIONAL ELECTROTECHNICAL COMMISSION

CEI
IEC
61508-2

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

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

CONTENTS

Figures

Tables

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

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

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 61508-2 has been prepared by subcommittee 65A: System aspects, of IEC technical committee 65: Industrial-process measurement and control.

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

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

Annexes A, B, and C form an integral part of this standard.

Annex D is for information only.

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

— Part 1: General requirements

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

— Part 3: Software requirements

— Part 4: Definitions and abbreviations

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

— Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3

— Part 7: Overview of techniques and measures

INTRODUCTION

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

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

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

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

This International Standard

- considers all relevant overall, E/E/PES and software safety lifecycle phases (for example, from initial concept, through design, implementation, operation and maintenance to decommissioning) when E/E/PESs are used to perform safety functions;
- has been conceived with a rapidly developing technology in mind; the framework is sufficiently robust and comprehensive to cater for future developments;
- enables application sector international standards, dealing with safety-related E/E/PESs, to be developed; the development of application sector international standards, within the framework of this International Standard, should lead to a high level of consistency (for example, of underlying principles, terminology, etc.) both within application sectors and across application sectors; this will have both safety and economic benefits;
- provides a method for the development of the safety requirements specification necessary to achieve the required functional safety for E/E/PE safety-related systems;
- 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 rely on 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 2: Requirements for electrical/electronic/programmable electronic safety-related systems

1 Scope

1.1 This part of IEC 61508:

a) is intended to be used only after a thorough understanding of IEC 61508-1, which provides the overall framework for the achievement of functional safety;

b) applies to any safety-related system, as defined by IEC 61508-1, which contains at least one electrical, electronic or programmable electronic based component;

c) applies to all subsystems and their components within an E/E/PE safety-related system (including sensors, actuators and the operator interface);

d) specifies how to refine the information developed in accordance with IEC 61508-1, concerning the overall safety requirements and their allocation to E/E/PE safety-related systems, and specifies how the overall safety requirements are refined into E/E/PES safety functions requirements and E/E/PES safety integrity requirements;

e) specifies requirements for activities that are to be applied during the design and manufacture of the E/E/PE safety-related systems (i.e. establishes the E/E/PES safety lifecycle model), except for software, which is dealt with by IEC 61508-3 (see figures 2 and 3) – these requirements include the application of techniques and measures, which are graded against the safety integrity level, for the avoidance of, and control of, faults and failures;

f) specifies the information necessary for carrying out the installation, commissioning and final safety validation of the E/E/PE safety-related systems;

g) does not apply to the operation and maintenance phase of the E/E/PE safety-related systems – this is dealt with in IEC 61508-1 – however, IEC 61508-2 does provide requirements for the preparation of information and procedures needed by the user for the operation and maintenance of the E/E/PE safety-related systems;

h) specifies requirements to be met by the organisation carrying out any modification of the E/E/PE safety-related systems.

NOTE 1 This part of IEC 61508 is mainly directed at suppliers and/or in-company engineering departments, hence the inclusion of requirements for modification.

NOTE 2 The relationship between IEC 61508-2 and IEC 61508-3 is illustrated in figure 3.

1.2 IEC 61508-1, IEC 61508-2, IEC 61508-3 and IEC 61508-4 are basic safety publications, although this status does not apply in the context of low complexity E/E/PE safety-related systems (see 3.4.4 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 IEC/ISO Guide 51. IEC61508 is also intended for use as a stand-alone standard.

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.

NOTE 1 The functional safety of an E/E/PE safety-related system can only be achieved when all related requirements are met. Therefore, it is important that all related requirements are carefully considered and adequately referenced.

NOTE 2 In the USA and Canada, until the proposed sector implementation of IEC 61508 (i.e. IEC 61511) is published as an international standard in the USA and Canada, existing national process safety standards based on IEC 61508 (i.e. ANSI/ISA S84.01-1996) can be applied to the process sector instead of IEC 61508.

1.3 Figure 1 shows the overall framework for parts 1 to 7 of IEC 61508 and indicates the role that IEC 61508-2 plays in the achievement of functional safety for E/E/PE safety-related systems. Annex A of IEC 61508-6 describes the application of IEC 61508-2 and IEC 61508-3.

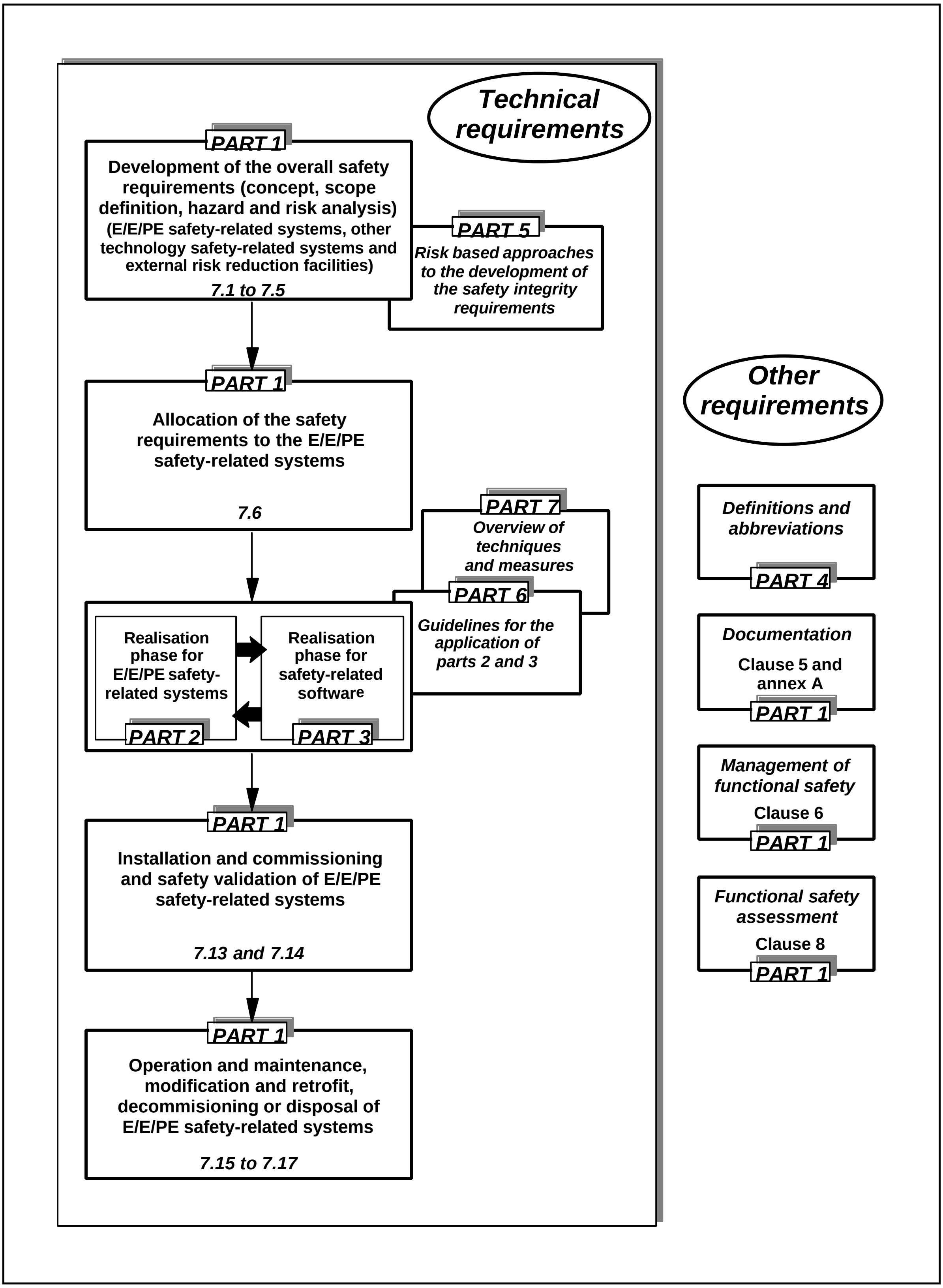

Technical requirements
PART 1
Development of the overall safety requirements (concept, scope definition, hazard and risk analysis) (E/E/PE safety-related systems, other technology safety-related systems and external risk reduction facilities)
7.1 to 7.5
PART 5
Risk based approaches to the development of the safety integrity requirements
PART 1
Allocation of the safety requirements to the E/E/PE safety-related systems
7.6
PART 7
Overview of techniques and measures
PART 6
Guidelines for the application of parts 2 and 3
Realisation phase for E/E/PE safety-related systems
PART 2
Realisation phase for safety-related software
PART 3
PART 1
Installation and commissioning and safety validation of E/E/PE safety-related systems
7.13 and 7.14
PART 1
Operation and maintenance, modification and retrofit, decommisioning or disposal of E/E/PE safety-related systems
7.15 to 7.17
Other requirements
Definitions and abbreviations
PART 4
Documentation
Clause 5 and annex A
PART 1
Management of functional safety
Clause 6
PART 1
Functional safety assessment
Clause 8
PART 1

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 61000-1-1 :1992, *Electromagnetic compatibility (EMC) – Part 1: General – Section 1: Application and interpretation of fundamental definitions and terms*

IEC 61000-2-5 :1995, *Electromagnetic compatibility (EMC) – Part 2: Environment – Section 5: Classification of electromagnetic environments*

IEC Guide 104 :1997, Guide to the drafting of safety standards, and the role of committees with safety pilot functions and safety group functions

IEC/ISO Guide 51 :1990, Guidelines for the inclusion of safety aspects in standards

3 Definitions and abbreviations

For the purposes of this standard, the definitions and abbreviations given in IEC 61508-4 apply.

4 Conformance to this standard

The requirements for conformance to this standard are as detailed in clause 4 of IEC 61508-1.

5 Documentation

The requirements for documentation are as detailed in clause 5 of IEC 61508-1.

6 Management of functional safety

The requirements for management of functional safety are as detailed in clause 6 of IEC 61508-1.

7 E/E/PES safety lifecycle requirements

7.1 General

7.1.1 Objectives and requirements: General

7.1.1.1 This subclause sets out the objectives and requirements for the E/E/PES safety lifecycle phases.

NOTE The objectives and requirements for the overall safety lifecycle, together with a general introduction to the structure of the standard are given in IEC 61508-1.

7.1.1.2 For all phases of the E/E/PES safety lifecycle, table 1 indicates

— the objectives to be achieved;

— the scope of the phase;

— a reference to the subclause containing the requirements;

— the required inputs to the phase;

— the outputs required to comply with the subclause.

7.1.2 Objectives

7.1.2.1 The first objective of the requirements of this subclause is to structure, in a systematic manner, the phases in the E/E/PES safety lifecycle that shall be considered in order to achieve the required functional safety of the E/E/PE safety-related systems.

7.1.2.2 The second objective of the requirements of this subclause is to document all information relevant to the functional safety of the E/E/PE safety-related systems throughout the E/E/PES safety lifecycle.

7.1.3 Requirements

7.1.3.1 The E/E/PES safety lifecycle that shall be used in claiming conformance with this standard is that specified in figure 2. If another E/E/PES safety lifecycle is used, it shall be specified during functional safety planning (see clause 6 of IEC 61508-1), and all the objectives and requirements of each subclause of IEC 61508-2 shall be met.

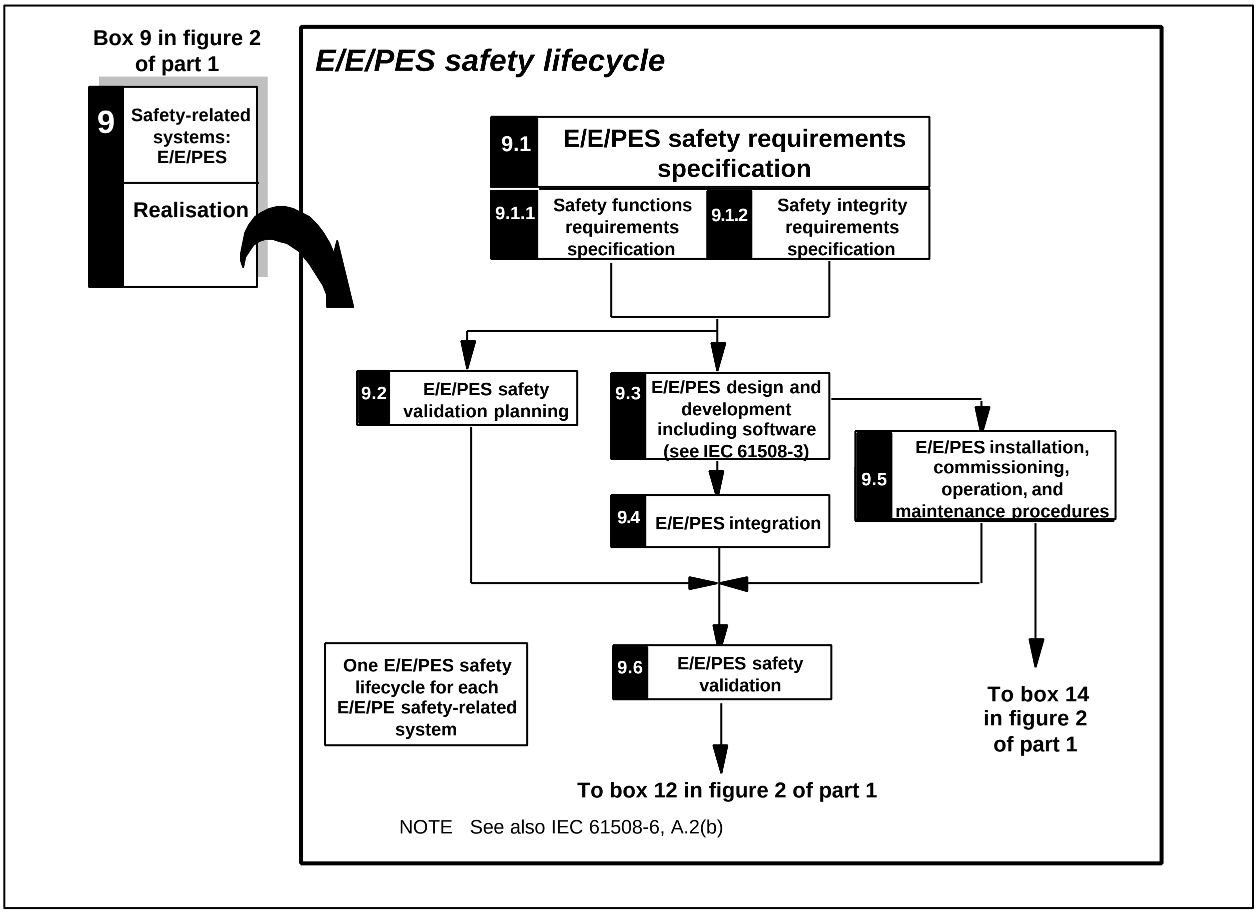
NOTE The relationship and scope for IEC 61508-2 and IEC 61508-3 is shown in figure 3.

7.1.3.2 The procedures for management of functional safety (see clause 6 of IEC 61508-1) shall run in parallel with the E/E/PES safety lifecycle phases.

7.1.3.3 Each phase of the E/E/PES safety lifecycle shall be divided into elementary activities, with the scope, inputs and outputs specified for each phase (see table 1).

7.1.3.4 Unless justified during functional safety planning, the outputs of each phase of the E/E/PES safety lifecycle shall be documented (see clause 5 of IEC 61508-1).

7.1.3.5 The outputs for each E/E/PES safety lifecycle phase shall meet the objectives and requirements specified for each phase (see 7.2 to 7.9).


Box 9 in figure 2 of part 1
9
Safety-related systems: E/E/PES
Realisation
E/E/PES safety lifecycle
9.1
E/E/PES safety requirements specification
9.1.1
Safety functions requirements specification
9.1.2
Safety integrity requirements specification
9.2
E/E/PES safety validation planning
9.3
E/E/PES design and development including software (see IEC 61508-3)
9.4
E/E/PES integration
9.5
E/E/PES installation, commissioning, operation, and maintenance procedures
One E/E/PES safety lifecycle for each E/E/PE safety-related system
9.6
E/E/PES safety validation
To box 14 in figure 2 of part 1
To box 12 in figure 2 of part 1

NOTE See also IEC 61508-6, A.2(b)

Figure 2 — E/E/PES safety lifecycle (in realisation phase)

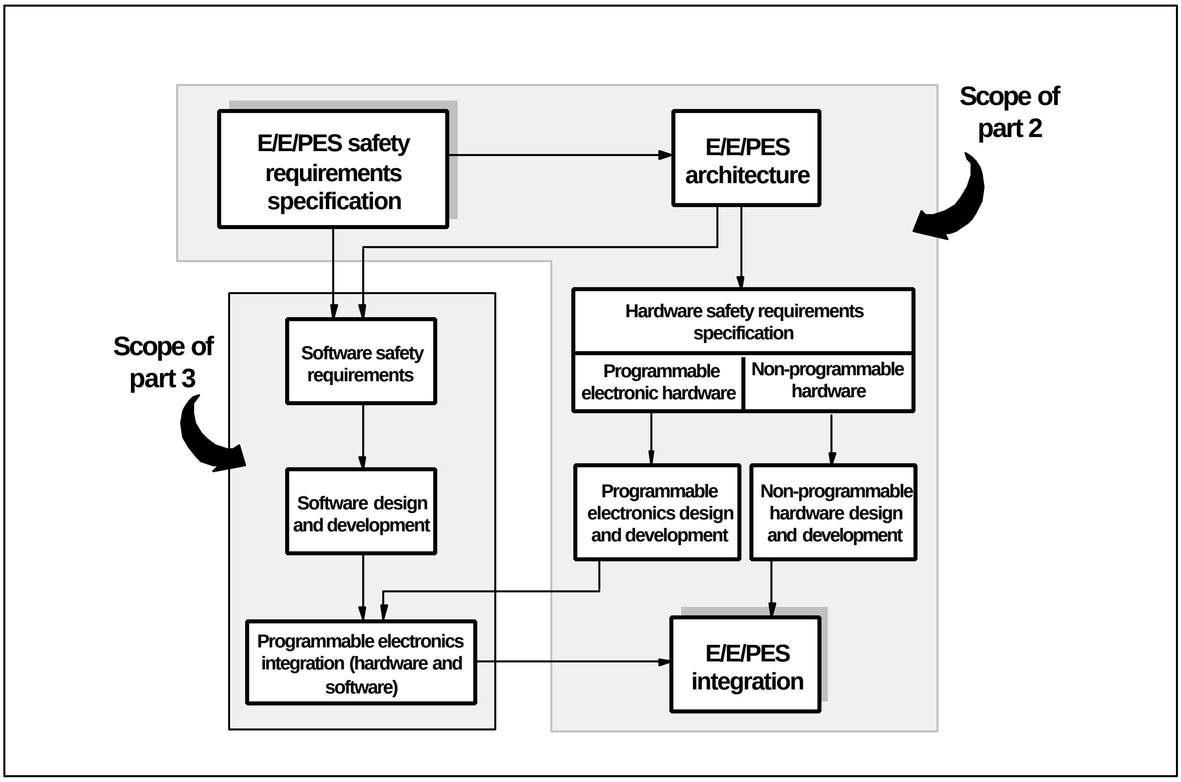

E/E/PES safety requirements specification
E/E/PES architecture
Scope of part 2
Scope of part 3
Software safety requirements
Hardware safety requirements specification
Programmable electronic hardware
Non-programmable hardware
Software design and development
Programmable electronics design and development
Non-programmable hardware design and development
Programmable electronics integration (hardware and software)
E/E/PES integration

Figure 3 — Relationship and scope for IEC 61508-2 and IEC 61508-3

Table 1 — Overview- Realisation phase of the E/E/PES safety lifecycle

Safety lifecycle phase or activity		Objectives	Scope	Require-ments subclause	Inputs	Outputs
Figure 2 box number	Title					
9.1	E/E/PES safety requirements specification	To specify the requirements for each E/E/PE safety-related system, in terms of the required safety functions and the required safety integrity, in order to achieve the required functional safety	E/E/PE safety-related systems	7.2.2	Description of allocation of safety requirements (see 7.6 of IEC 61508-1)	E/E/PES safety requirements Requirements for software safety as an input to the software safety requirements specification
9.2	E/E/PES safety validation planning	To plan the validation of the safety of the E/E/PE safety-related systems	E/E/PE safety-related systems	7.3.2	E/E/PES safety requirements	Plan for the safety validation of the E/E/PE safety-related systems
9.3	E/E/PES design and development	To design the E/E/PE safety-related systems to meet the requirements for safety functions and safety integrity	E/E/PE safety-related systems	7.4.2 to 7.4.9	E/E/PES safety requirements	Design of the E/E/PE safety related systems in conformance with the E/E/PES safety requirements Plan for the E/E/PES integration test PES architectural information as an input to the software requirements specification
9.4	E/E/PES integration	To integrate and test the E/E/PE safety-related systems	E/E/PE safety-related systems	7.5.2	E/E/PES design E/E/PES integration test plan Programmable electronics hardware and software	Fully functioning E/E/PE safety-related systems in conformance with the E/E/PES design Results of E/E/PES integration tests
9.5	E/E/PES installation, commissioning, operation, and maintenance procedures	To develop procedures to ensure that the functional safety of the E/E/PE safety-related systems is maintained during operation and maintenance	E/E/PE safety-related systems EUC	7.6.2	E/E/PES safety requirements E/E/PES design	E/E/PES installation, commissioning, operation and maintenance procedures for each individual E/E/PES
9.6	E/E/PES safety validation	To validate that the E/E/PE safety-related systems meet, in all respects, the requirements for safety in terms of the required safety functions and the required safety integrity	E/E/PE safety-related systems	7.7.2	E/E/PES safety requirements Plan for the safety validation of the E/E/PE safety-related systems	Fully safety validated E/E/PE safety-related systems Results of E/E/PES safety validation
-	E/E/PES modification	To make corrections, enhancements or adaptations to the E/E/PE safety-related systems, ensuring that the required safety integrity level is achieved and maintained	E/E/PE safety-related systems	7.8.2	E/E/PES safety requirements	Results of E/E/PES modification
-	E/E/PES verification	To test and evaluate the outputs of a given phase to ensure correctness	E/E/PE safety-related	7.9.2	As above - depends on the phase	As above - depends on the phase

		and consistency with respect to the products and standards provided as input to that phase	systems		Plan for the verification of the E/E/PE safety-related systems for each phase	Results of the verification of the E/E/PE safety-related systems for each phase
-	E/E/PES functional safety assessment	To investigate and arrive at a judgement on the functional safety achieved by the E/E/PE safety-related systems	E/E/PE safety-related systems	8	Plan for E/E/PES functional safety assessment	Results of E/E/PES functional safety assessment

7.2 E/E/PES safety requirements specification

NOTE This phase is box 9.1 of figure 2.

7.2.1 Objective

The objective of the requirements of this subclause is to specify the requirements for each E/E/PE safety-related system, in terms of the required safety functions and the required safety integrity, in order to achieve the required functional safety.

NOTE The safety functions may, for example, be required to put the EUC into a safe state or to maintain a safe state.

7.2.2 General requirements

7.2.2.1 The specification of the E/E/PES safety requirements shall be derived from the allocation of safety requirements, specified in 7.6 of IEC 61508-1, and from those requirements specified during functional safety planning (see clause 6 of IEC 61508-1). This information shall be made available to the E/E/PES developer.

NOTE Caution should be exercised if non-safety functions and safety functions are implemented in the same E/E/PE safety-related system. While this is allowed in the standard, it may lead to greater complexity and increase the difficulty in carrying out E/E/PE safety lifecycle activities (for example design, validation, functional safety assessment and maintenance).

7.2.2.2 The E/E/PES safety requirements shall be expressed and structured in such a way that they are

a) clear, precise, unambiguous, verifiable, testable, maintainable and feasible; and

b) written to aid comprehension by those who are likely to utilise the information at any stage of the E/E/PES safety lifecycle.

7.2.2.3 The specification of the E/E/PES safety requirements shall contain the requirements for the E/E/PES safety functions (see 7.2.3.1) and the requirements for E/E/PES safety integrity (see 7.2.3.2).

7.2.3 E/E/PES safety requirements

7.2.3.1 The E/E/PES safety functions requirements specification shall contain

a) a description of all the safety functions necessary to achieve the required functional safety, which shall, for each safety function

- provide comprehensive detailed requirements sufficient for the design and development of the E/E/PE safety-related systems,
- include the manner in which the E/E/PE safety-related systems are intended to achieve or maintain a safe state for the EUC,
- specify whether or not continuous control is required, and for what periods, in achieving or maintaining a safe state of the EUC, and
- specify whether the safety function is applicable to E/E/PE safety-related systems operating in low demand or high demand/continuous modes of operation;

b) throughput and response time performance;

c) E/E/PE safety-related system and operator interfaces which are necessary to achieve the required functional safety;

d) all information relevant to functional safety which may have an influence on the E/E/PE safety-related system design;

e) all interfaces between the E/E/PE safety-related systems and any other systems (either directly associated within, or outside, the EUC);

f) all relevant modes of operation of the EUC, including

— preparation for use including setting and adjustment,

— start-up, teach, automatic, manual, semi-automatic, steady state of operation,

— steady state of non-operation, re-setting, shut-down, maintenance,

— reasonably foreseeable abnormal conditions;

NOTE 1 Reasonably foreseeable abnormal conditions are those reasonably foreseeable to either the developers or users.

NOTE 2 Additional safety functions may be required for particular modes of operation (for example setting, adjustment or maintenance), to enable these operations to be carried out safely.

g) all required modes of behaviour of the E/E/PE safety-related systems - in particular, failure behaviour and the required response (for example alarms, automatic shut-down, etc) of the E/E/PE safety-related systems shall be detailed;

h) the significance of all hardware/software interactions – where relevant, any required constraints between the hardware and the software shall be identified and documented;

NOTE 3 Where these interactions are not known before finishing the design, only general constraints can be stated.

i) limiting and constraint conditions for the E/E/PE safety-related systems and their associated subsystems, for example timing constraints;

j) any specific requirements related to the procedures for starting-up and restarting the E/E/PE safety-related systems.

7.2.3.2 The E/E/PES safety integrity requirements specification shall contain:

a) the safety integrity level for each safety function and, when required (see note 2), the required target failure measure for the safety function;

NOTE 1 The safety integrity level of a safety function determines the target failure measure for the safety function according to IEC 61508-1, Tables 2 & 3.

NOTE 2 The target failure measure of a safety function will need to be specified when the required risk reduction for the safety function has been derived using a quantitative method (see IEC 61508-1, 7.5.2.2).

b) the mode of operation (low demand or continuous / high demand) of each safety function;

c) the requirements, constraints, functions and facilities to enable the proof testing of the E/E/PE hardware to be undertaken;

d) the extremes of all environmental conditions that are likely to be encountered during the E/E/PES safety lifecycle including manufacture, storage, transport, testing, installation, commissioning, operation and maintenance;

e) the electromagnetic immunity limits (see IEC 61000-1-1) which are required to achieve electromagnetic compatibility. – the electromagnetic immunity limits should be derived taking into account both the electromagnetic environment (see IEC 61000-2-5) and the required safety integrity levels ;

NOTE 1 It is important to recognise that the safety integrity level is a factor in determining electromagnetic immunity limits, especially since the level of electromagnetic disturbance in the environment is subject to a statistical distribution. In most practical situations it is not possible to specify an absolute level of disturbance, only a level which it is expected will not be exceeded in practice (this is the electromagnetic compatibility level). Unfortunately, practical difficulties make the probability associated with this expectation very hard to define. Therefore, the immunity limit does not guarantee that the E/E/PE safety-related system will not fail due to electromagnetic disturbances, it only provides some level of confidence that such a failure will not occur. The actual level of confidence achieved is a function of the immunity limit in relation to the statistical distribution of the disturbance levels in the operating environment. For higher safety integrity levels it may be necessary to have a higher level of confidence, which means that the margin by which the immunity limit exceeds the compatibility level should be greater for higher safety integrity levels.

NOTE 2 Also, guidance may be found in EMC product standards, but it is important to recognise that higher immunity levels than those specified in such standards may be necessary for particular locations or when the equipment is intended for use in harsher electromagnetic environments.

NOTE 3 In developing the E/E/PES safety requirements specification, the application in which the E/E/PE safety-related systems are to be used should be taken into consideration. This is particularly important for maintenance, where the specified proof test interval should not be less than can be reasonably expected for the particular application. For example, the time between services that can be realistically attained for mass-produced items used by the public is likely to be greater than in a more controlled application.

7.2.3.3 For the avoidance of mistakes during the specification of the E/E/PES safety requirements, an appropriate group of techniques and measures according to table B.1 shall be used.

7.3 E/E/PES safety validation planning

NOTE This phase is box 9.2 of figure 2. It will normally be carried out in parallel with E/E/PES design and development (see 7.4).

7.3.1 Objective

The objective of the requirements of this subclause is to plan the validation of the safety of the E/E/PE safety-related systems.

7.3.2 Requirements

7.3.2.1 Planning shall be carried out to specify the steps (both procedural and technical) that are to be used to demonstrate that the E/E/PE safety-related systems satisfy the E/E/PES safety requirements specification (see 7.2).

NOTE See IEC 61508-3 for the validation plan for the software.

7.3.2.2 Planning for the validation of the E/E/PE safety-related systems shall consider the following:

a) all of the requirements defined in the E/E/PES safety requirements specification;

b) the procedures to be applied to validate that each safety function is correctly implemented, and the pass/fail criteria for accomplishing the tests;

c) the procedures to be applied to validate that each safety function is of the required safety integrity, and the pass/fail criteria for accomplishing the tests;

d) the required environment in which the testing is to take place including all necessary tools and equipment (also plan which tools and equipment should be calibrated);

e) test evaluation procedures (with justifications);

f) the test procedures and performance criteria to be applied to validate the specified electromagnetic immunity limits;

NOTE Guidance on the specification of immunity test limits is given in IEC 61000-2-5 and IEC 61000-4.

g) policies for resolving validation failure.

7.4 E/E/PES design & development

NOTE This phase is box 9.3 of figure 2. It will normally be carried out in parallel with E/E/PES safety validation planning (see 7.3).

7.4.1 Objective

The objective of the requirements of this subclause is to ensure that the design and implementation of the E/E/PE safety-related systems meets the specified safety functions and safety integrity requirements (see 7.2).

7.4.2 General requirements

7.4.2.1 The design of the E/E/PE safety-related system shall be created in accordance with the E/E/PES safety requirements specification (see 7.2), taking into account all the requirements of 7.4.

7.4.2.2 The design of the E/E/PE safety-related system (including the overall hardware and software architecture, sensors, actuators, programmable electronics, embedded software, application software, etc.), see figure 4, shall be such as to meet all of the requirements a) to c) as follows:

a) the requirements for hardware safety integrity comprising:

— the architectural constraints on hardware safety integrity (see 7.4.3.1), and

— the requirements for the probability of dangerous random hardware failures (see 7.4.3.2)

b) the requirements for systematic safety integrity comprising:

— the requirements for the avoidance of failures (see 7.4.4), and the requirements for the control of systematic faults (see 7.4.5), or

— evidence that the equipment is ‘proven-in-use’ (see 7.4.7.6 to 7.4.7.12)

c) the requirements for system behaviour on detection of a fault (see 7.4.6).

NOTE 1 Overall E/E/PES safety integrity framework: the overall method for selecting a design approach to demonstrate achievement of a safety integrity level (for both hardware and systematic safety integrity) in E/E/PE safety-related systems is as follows:

— determine the required safety integrity level (SIL) of the safety functions - see IEC 61508-1 and IEC61508-5;

— set: hardware safety integrity = systematic safety integrity = SIL (see 7.4.3.2.1);

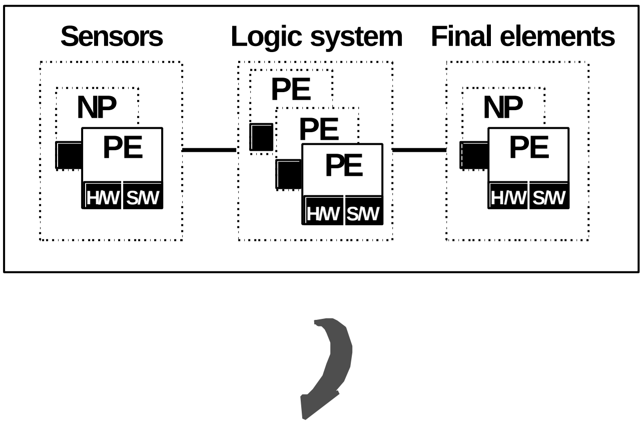
— for hardware safety integrity, determine the architecture to meet the architectural constraints (see 7.4.3.1) and demonstrate that the probabilities of failure of the safety functions due to random hardware failures meet the required target failure measures (see 7.4.3.2).;

— for systematic safety integrity, select design features that control (tolerate) systematic faults in actual operation (see 7.4.5) or confirm that the ‘proven-in-use’ requirements have been met (see 7.4.7.6 to 7.4.7.12); and

— for systematic safety integrity, select techniques and measures that avoid (prevent the introduction of) systematic faults during design and development (see 7.4.4) or confirm that the ‘proven-in-use’ requirements have been met (see 7.4.7.6 to 7.4.7.12).

NOTE 2 IEC 61508-3 contains the requirements for the software architecture (see 7.4.2.2); the requirements to produce a programmable electronics and software integration test specification (see 7.5); and the requirements to integrate the programmable electronics and software according to that specification (see 7.5). In all cases close co-operation between the developer of the E/E/PE safety-related systems and the software developer will be necessary.

Architectures shown are examples and could be:
- — single channel;
- — dual channel;
- — 1oo2, 1oo3, 2oo2 etc.



Programmable electronics architecture		
PE hardware architecture	**PE software architecture** (s/w architecture consists of embedded s/w and applications s/w)	
Generic and application specific features in PE hardware. Examples include: — diagnostic tests; — redundant processors; — dual I/O cards.	PE embedded software	PE applications software

	Examples include:
	— communications drivers;
	— fault handling;
	— executive software.
		Examples include:
		— input/output functions;
		— derived functions (for examplesensor checking if not provided as a service of the embedded software).

Key

PE	programmable electronics
NP	non-programmable devices
H/W	hardware
S/W	software
MooN	M out of N (for example 1oo2 is 1 out of 2)

Figure 4 — Relationship between the hardware and software architectures of programmable electronics

7.4.2.3 Where an E/E/PE safety-related system is to implement both safety and non-safety functions, then all the hardware and software shall be treated as safety-related unless it can be shown that the implementation of the safety and non-safety functions is sufficiently independent (i.e. that the failure of any non-safety-related functions does not cause a dangerous failure of the safety-related functions). Wherever practicable, the safety-related functions should be separated from the non-safety-related functions.

NOTE 1 Sufficient independence of implementation is established by showing that the probability of a dependent failure between the non-safety and safety-related parts is sufficiently low in comparison with the highest safety integrity level associated with the safety functions involved.

NOTE 2 Caution should be exercised if non-safety functions and safety functions are implemented in the same E/E/PE safety-related system. While this is allowed in the standard, it may lead to greater complexity and increase the difficulty in carrying out E/E/PES safety lifecycle activities (for example design, validation, functional safety assessment and maintenance).

7.4.2.4 The requirements for hardware and software shall be determined by the safety integrity level of the safety function having the highest safety integrity level unless it can be shown that the implementation of the safety functions of the different safety integrity levels is sufficiently independent.

NOTE 1 Sufficient independence of implementation is established by showing that the probability of a dependent failure between the parts implementing safety functions of different integrity levels is sufficiently low in comparison with the highest safety integrity level associated with the safety functions involved.

NOTE 2 Where several safety functions are implemented in an E/E/PE safety-related system then it will be necessary to consider the possibility that a single fault could cause a failure of several safety functions. In such a situation, it may be appropriate to determine the requirements for hardware and software on the basis of a higher safety integrity level than is associated with any one of the safety functions, depending on the risk associated with such a failure.

7.4.2.5 When independence between safety functions is required (see 7.4.2.3 and 7.4.2.4) then the following shall be documented during the design:

a) the method of achieving independence;

b) the justification of the method.

7.4.2.6 The requirements for safety-related software (see IEC 61508-3) shall be made available to the developer of the E/E/PE safety-related system.

7.4.2.7 The developer of the E/E/PE safety-related system shall review the requirements for safety-related software and hardware to ensure that they are adequately specified. In particular, the E/E/PES developer shall consider the following:

a) safety functions;

b) E/E/PE safety-related system safety integrity requirements;

c) equipment and operator interfaces.

7.4.2.8 The E/E/PE safety-related system design documentation shall specify those techniques and measures necessary during the E/E/PES safety lifecycle phases to achieve the safety integrity level.

7.4.2.9 The E/E/PE safety-related system design documentation shall justify the techniques and measures chosen to form an integrated set which satisfies the required safety integrity level.

NOTE The adoption of an overall approach employing independent type approval of the E/E/PE safety-related systems (including sensors, actuators, etc) for hardware and software, diagnostic tests and programming tools, and using appropriate languages for software wherever possible, has the potential to reduce the complexity of E/E/PES application engineering.

7.4.2.10 During the design and development activities, the significance (where relevant) of all hardware and software interactions shall be identified, evaluated and documented.

7.4.2.11 The design shall be based on a decomposition into subsystems with each subsystem having a specified design and set of integration tests (see 7.4.7).

NOTE 1 A subsystem may be considered to comprise a single component or any group of components. A complete E/E/PE safety-related system is made up from a number of identifiable and separate subsystems, which when put together implement the safety function under consideration. A subsystem can have more than one channel. See 7.4.7.3.

NOTE 2 Wherever practicable, existing verified subsystems should be used in the implementation. This statement is generally valid only if there is almost 100 % mapping of the existing subsystem functionality, capacity and performance on to the new requirement or the verified subsystem is structured in such a way that the user is able to select only the functions, capacity or performance required for the specific application. Excessive functionality, capacity or performance can be detrimental to system safety if the existing subsystem is overly complicated or has unused features and if protection against unintended functions cannot be obtained.

7.4.2.12 Where a subsystem has multiple outputs then it is necessary to determine whether some combination of output states, which may be caused by a failure of the E/E/PE safety-related system, can directly cause a hazardous event (as determined by the hazard and risk analysis, see IEC 61508-1, 7.4.2.10). Where this has been established, then the prevention of that combination of output states shall be regarded as a safety function operating in the high demand / continuous mode of operation (see 7.4.6.3 and 7.4.3.2.5).

7.4.2.13 De-rating (see IEC 61508-7, A.2.8) shall be used as far as possible for all components. Justification for operating any components at their limits shall be documented (see IEC 61508-1, clause 5).

NOTE Where de-rating is appropriate, a de-rating factor of at least 0.67 should be used.

7.4.3 Requirements for hardware safety integrity

NOTE Clause A.2 of IEC 61508-6 gives an overview of the necessary steps in achieving required hardware safety integrity, and shows how this subclause relates to other requirements of this standard.

7.4.3.1 Architectural constraints on hardware safety integrity

7.4.3.1.1 In the context of hardware safety integrity, the highest safety integrity level that can be claimed for a safety function is limited by the hardware fault tolerance and safe failure fraction of the subsystems that carry out that safety function. Tables 2 and 3 specify the highest safety integrity level that can be claimed for a safety function which uses a subsystem taking into account the hardware fault tolerance and safe failure fraction of that subsystem. The requirements of tables 2 and 3 shall be applied to each subsystem carrying out a safety function and hence every part of the E/E/PE safety related system; 7.4.3.1.2 to 7.4.3.1.4 specify which one of tables 2 and 3 apply to any particular subsystem. 7.4.3.1.5 and 7.4.3.1.6 specify how the highest safety integrity level that can be claimed for a safety function is derived. With respect to these requirements:

a) a hardware fault tolerance of N means that N+1 faults could cause a loss of the safety function. In determining the hardware fault tolerance no account shall be taken of other measures that may control the effects of faults such as diagnostics, and

b) where one fault directly leads to the occurrence of one or more subsequent faults, these are considered as a single fault.

c) in determining hardware fault tolerance, certain faults may be excluded, provided that the likelihood of them occurring is very low in relation to the safety integrity requirements of the subsystem. Any such fault exclusions shall be justified and documented (see note 3).

d) the safe failure fraction of a subsystem is defined as the ratio of the average rate of safe plus detected failures of the subsystem to the total average failure rate of the subsystem (see annex C).

NOTE 1 The architectural constraints have been included in order to achieve a sufficiently robust architecture, taking into account the level of subsystem complexity. The hardware safety integrity level for the E/E/PE safety-related system, derived through applying these requirements, is the maximum that is permitted to be claimed even though, in some cases, a higher safety integrity level could theoretically be derived if a solely mathematical approach had been adopted for the E/E/PE safety-related system.

NOTE 2 The architecture and subsystem derived to meet the hardware fault tolerance requirements is that used under normal operating conditions. The fault tolerance requirements may be relaxed while the E/E/PE safety-related system is being repaired on-line. However, the key parameters relating to any relaxation must have been previously evaluated (for example mean time to restoration compared to the probability of a demand).

NOTE 3 This is necessary because if a component clearly has a very low probability of failure by virtue of properties inherent to its design and construction (for example, a mechanical actuator linkage), then it would not normally be considered necessary to constrain (on the basis of hardware fault tolerance) the safety integrity of any safety function which uses the component.

7.4.3.1.2 A subsystem (see 7.4.2.11, note 1) can be regarded as type A if, for the components required to achieve the safety function

a) the failure modes of all constituent components are well defined; and

b) the behaviour of the subsystem under fault conditions can be completely determined; and

c) there is sufficient dependable failure data from field experience to show that the claimed rates of failure for detected and undetected dangerous failures are met (see 7.4.7.3 and 7.4.7.4).

7.4.3.1.3 A subsystem (see 7.4.2.11, note 1) shall be regarded as type B if for the components required to achieve the safety function

a) the failure mode of at least one constituent component is not well defined; or

b) the behaviour of the subsystem under fault conditions cannot be completely determined; or

c) there is insufficient dependable failure data from field experience to support claims for rates of failure for detected and undetected dangerous failures (see 7.4.7.3 and 7.4.7.4).

NOTE This means that if at least one of the components of a subsystem itself satisfies the conditions for a type B subsystem then that subsystem must be regarded as type B rather than type A. See also 7.4.2.11, Note 1.

7.4.3.1.4 The architectural constraints of either table 2 or table 3 shall apply to each subsystem carrying out a safety function, so that

a) the hardware fault tolerance requirements shall be achieved for the whole of the E/E/PE safety-related system;

b) table 2 applies for every type A subsystem forming part of the E/E/PE safety-related systems;

NOTE 1 If the E/E/PE safety-related system contains only type A subsystems then the requirements in table 2 will apply to the entire E/E/PE safety-related system.

c) table 3 applies for every type B subsystem forming part of the E/E/PE safety-related systems;

NOTE 2 If the E/E/PE safety-related system contains only type B subsystems then the requirements in table 3 will apply to the entire E/E/PE safety-related system.

d) both tables 2 and 3 will be applicable to E/E/PE safety-related systems comprising both type A and type B subsystems, since the requirements in table 2 shall apply for the type A subsystems and the requirements in table 3 shall apply for the type B subsystems.

Table 2 — Hardware safety integrity: architectural constraints on type A safety-related subsystems

Safe failure fraction	**Hardware fault tolerance** (see note 2)		
	0	**1**	**2**
< 60 %	SIL1	SIL2	SIL3
60 % - < 90 %	SIL2	SIL3	SIL4
90 % - < 99 %	SIL3	SIL4	SIL4
≥ 99 %	SIL3	SIL4	SIL4
NOTE 1 See 7.4.3.1.1 to 7.4.3.1.4 for details on interpreting this table. NOTE 2 A hardware fault tolerance of N means that N+1 faults could cause a loss of the safety function. NOTE 3 See annex C for details of how to calculate safe failure fraction.			

Table 3 — Hardware safety integrity: architectural constraints on type B safety-related subsystems

Safe failure fraction	**Hardware fault tolerance** (see note 2)		
	0	**1**	**2**
< 60 %	not allowed	SIL1	SIL2
60 % - < 90 %	SIL1	SIL2	SIL3
90 % - < 99 %	SIL2	SIL3	SIL4
≥ 99 %	SIL3	SIL4	SIL4

NOTE 1 See 7.4.3.1.1 to 7.4.3.1.4 for details on interpreting this table.

NOTE 2 A hardware fault tolerance of N means that N+1 faults could cause a loss of the safety function.

NOTE 3 See annex C for details of how to calculate safe failure fraction.

7.4.3.1.5 In E/E/PE safety-related systems where a safety function is implemented through a single channel (such as in figure 5), the maximum hardware safety integrity level that can be claimed for the safety function under consideration shall be determined by the subsystem that has met the lowest hardware safety integrity level requirements (determined by consideration of tables 2 and 3).

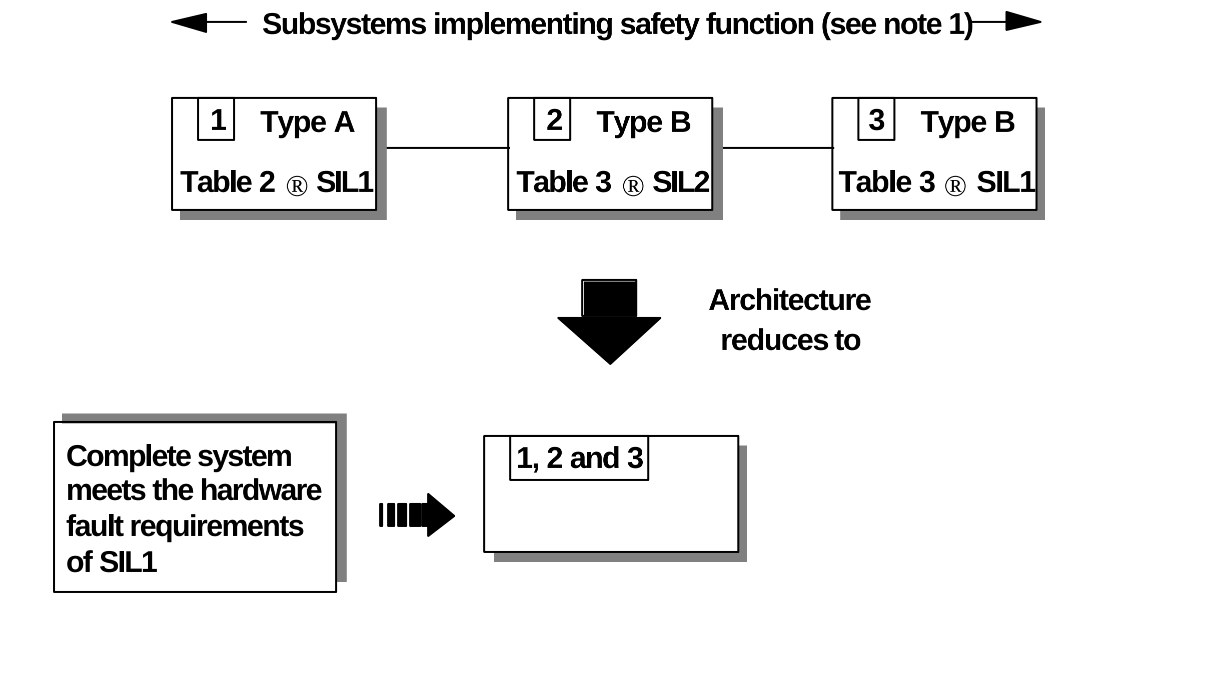
EXAMPLE Assume an architecture in which a particular safety function is performed by a single channel of subsystems 1, 2 and 3 as in figure 5 and the subsystems meet the requirements of tables 2 and 3 as follows:

— subsystem 1 achieves the hardware fault tolerance requirements, for a specific safe failure fraction, of SIL1;

— subsystem 2 achieves the hardware fault tolerance requirements, for a specific safe failure fraction, of SIL2;

— subsystem 3 achieves the hardware fault tolerance requirements, for a specific safe failure fraction, of SIL1.

For this particular architecture, subsystems 1 and 3 are each only able to achieve the hardware fault tolerance requirements of SIL1, while subsystem 2 is able to achieve the hardware fault tolerance requirements of SIL2. Therefore, both subsystem 1 and subsystem 3 restrict the hardware safety integrity level that can be claimed, in respect of the hardware fault tolerance, for the safety function under consideration, to just SIL1.


Subsystems implementing safety function (see note 1)
1 Type A
Table 2 ® SIL1
2 Type B
Table 3 ® SIL2
3 Type B
Table 3 ® SIL1
Architecture reduces to
Complete system meets the hardware fault requirements of SIL1
1, 2 and 3

NOTE 1 The subsystems implementing the safety function will be across the entire E/E/PE safety-related system in terms of ranging from the sensors to the actuators.

NOTE 2 For details on interpreting this figure, see the example to 7.4.3.1.5.

Figure 5 — Example limitation on hardware safety integrity for a single-channel safety function

7.4.3.1.6 In E/E/PE safety-related systems where a safety function is implemented through multiple channels of subsystems (such as in figure 6), the maximum hardware safety integrity level that can be claimed for the safety function under consideration shall be determined by

a) assessing each subsystem against the requirements of table 2 or 3 (as specified in 7.4.3.1.2 to 7.4.3.1.4); and

b) grouping the subsystems into combinations; and

c) analysing those combinations to determine the overall hardware safety integrity level.

EXAMPLE The grouping and analysis of these combinations may be carried out in various ways. To illustrate one possible method, assume an architecture in which a particular safety function is performed by either a combination of subsystems 1, 2 and 3 or a combination of subsystems 4, 5 and 3, as in figure 6. In this case, the combination of subsystems 1 and 2 and the combination of subsystems 4 and 5 have the same functionality as regards the safety function, and provide separate inputs into subsystem 3. In this example, the combination of parallel subsystems is based on each subsystem implementing the required part of the safety function independent of the other (parallel) subsystem. The safety function will be performed:

— in the event of a fault in either subsystem 1 or subsystem 2 (because the combination of subsystems 4 and 5 is able to perform the safety function); or

— in the event of a fault in either subsystem 4 or subsystem 5 (because the combination of subsystems 1 and 2 is able to perform the safety function).

Each subsystem meets the requirements of tables 2 and 3 as follows:

— subsystem 1 achieves the hardware fault tolerance requirements, for a specific safe failure fraction, of SIL3;

— subsystem 2 achieves the hardware fault tolerance requirements, for a specific safe failure fraction, of SIL2;

— subsystem 3 achieves the hardware fault tolerance requirements, for a specific safe failure fraction, of SIL2;

— subsystem 4 achieves the hardware fault tolerance requirements, for a specific safe failure fraction, of SIL2;

— subsystem 5 achieves the hardware fault tolerance requirements, for a specific safe failure fraction, of SIL1.

The determination of the maximum hardware safety integrity level that can be claimed, for the safety function under consideration, is detailed in the following steps.

a) Combining subsystems 1 and 2: The hardware fault tolerance and safe failure fraction achieved by the combination of subsystems 1 and 2 (each separately meeting the requirements for SIL3 and SIL2 respectively) meets the requirements of SIL2 (determined by subsystem 2).

b) Combining subsystems 4 and 5: The hardware fault tolerance and safe failure fraction achieved by the combination of subsystems 4 and 5 (each separately meeting the requirements for SIL2 and SIL1 respectively) meets the requirements of SIL1 (determined by subsystem 5).

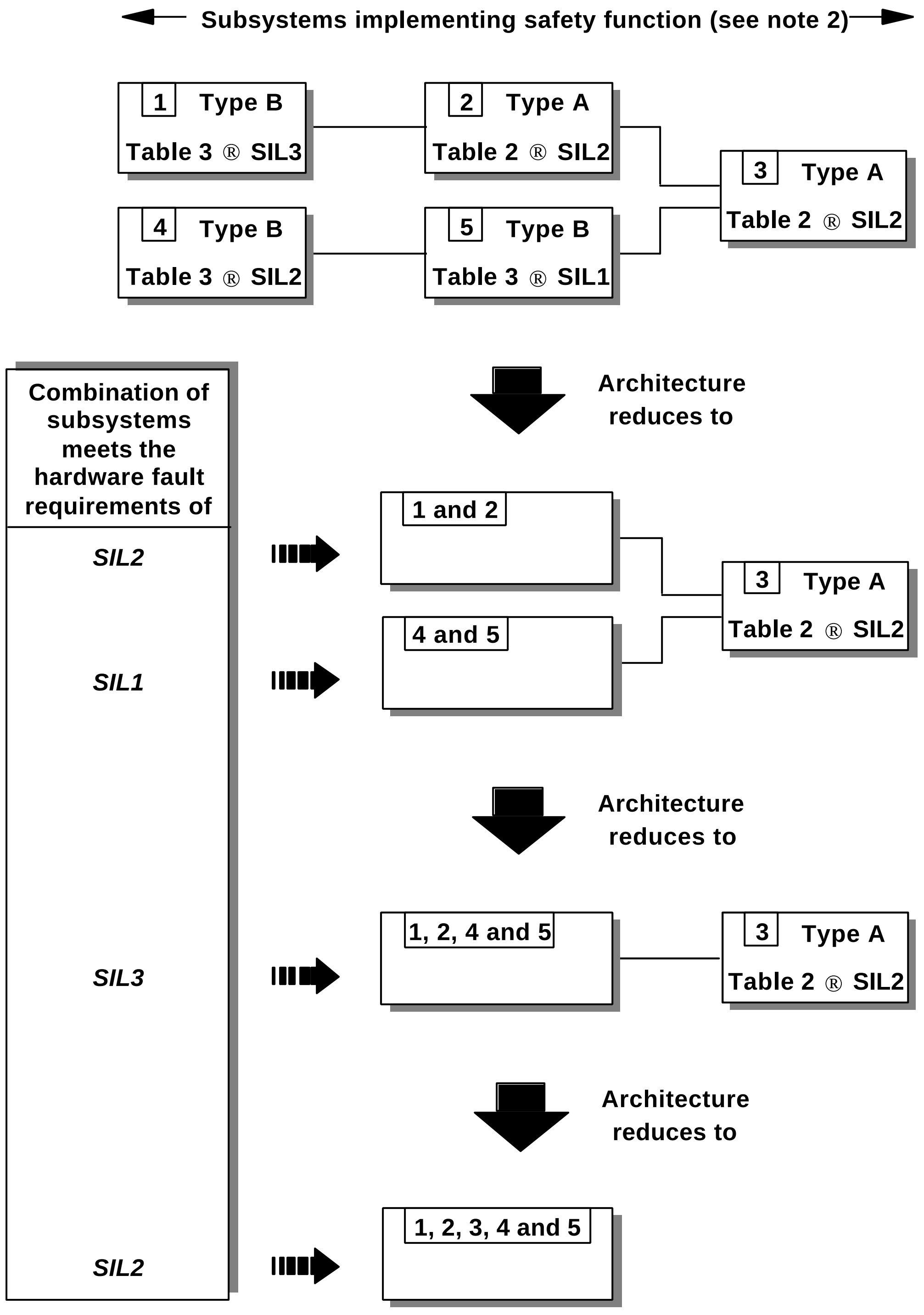
c) Further combining the combination of subsystems 1 and 2 with the combination of subsystems 4 and 5: The hardware safety integrity level, in respect of the hardware fault tolerance, of the combination of subsystems 1, 2, 4 and 5 is determined by:

   — deciding which of the subsystem combinations (i.e. the combination of subsystems 1 and 2 or the combination of subsystems 4 and 5) has achieved the highest claimable hardware safety integrity level (in terms of meeting the hardware fault tolerance); and

   — analysing the effect the other subsystem combination has on the hardware fault tolerance for the combination of subsystems 1, 2, 4 and 5.

   In this example, the combination of subsystems 1 and 2 has a maximum allowable claim of SIL2 (see a) above) while the combination of subsystems 4 and 5 has a maximum allowable claim of SIL1 (see b) above). However, in the event of a fault occurring in the combination of subsystems 1 and 2, the safety function could be performed by the combination of subsystems 4 and 5. To take account of this effect, the hardware fault tolerance achieved by the combination of subsystems 1 and 2 is increased by 1. Increasing the hardware fault tolerance by 1 has the effect of increasing the hardware safety integrity level that can be claimed by 1 (see tables 2 and 3). Therefore, the combination of subsystems 1, 2, 4 and 5 has a maximum claimable hardware safety integrity level, with respect to the hardware fault tolerance and safe failure fraction, of SIL3 (i.e. the hardware safety integrity level achieved by the combination of subsystems 1 and 2 (which was SIL2) plus 1).

d) The complete E/E/PE safety-related system: The hardware safety integrity level, in respect of the hardware fault tolerance, that can be claimed for the safety function under consideration, is determined by analysing the combination of subsystems 1, 2, 4 and 5 (which achieved the fault tolerance requirements of SIL3 (see c)) and subsystem 3 (which achieved the fault tolerance requirements of SIL2). It is the subsystem that has achieved the lowest hardware safety integrity level requirements, in this case subsystem 3, which determines the hardware safety integrity level for the complete E/E/PE safety-related system. Therefore, for this example, the hardware safety integrity level, in respect of the hardware fault tolerance, that has been achieved for the safety function, is SIL2.



NOTE 1 Subsystems 1 and 2 and subsystems 4 and 5 have the same functionality as regards implementing the safety function, and provide separate inputs into subsystem 3.

NOTE 2 The subsystems implementing the safety function will be across the entire E/E/PE safety-related system in terms of ranging from the sensors to the actuators.

NOTE 3 For details on interpreting this figure, see the example to 7.4.3.1.6.

Figure 6 — Example limitation on hardware safety integrity for a multiple-channel safety function

7.4.3.2 Requirements for estimating the probability of failure of safety functions due to random hardware failures

7.4.3.2.1 The probability of failure of each safety function due to random hardware failures, estimated according to 7.4.3.2.2 and 7.4.3.2.3, shall be equal to or less than the target failure measure as specified in the safety requirements specification (see 7.2.3.2).

NOTE 1 In the case of a safety function operating in the low demand mode of operation, the target failure measure will be expressed in terms of the average probability of failure to perform its design function on demand, as determined by the safety integrity level of the safety function (see IEC 61508-1, Table 2), unless there is a requirement in the E/E/PES safety integrity requirements specification (see 7.2.3.2) for the safety function to meet a specific target failure measure, rather than a specific SIL. For example, when a target failure measure of 1.5 x 10^{-2} (probability of failure on demand) is specified in order to meet the required risk reduction, then the probability of failure on demand of the safety function due to random hardware failures will need to be equal to or less than 1.5 x 10^{-2}.

NOTE 2 In the case of a safety function operating in the high demand / continuous mode of operation, the target failure measure will be expressed in terms of the average probability of a dangerous failure per hour, as determined by the safety integrity level of the safety function (see IEC 61508-1, Table 3), unless there is a requirement in the E/E/PES safety integrity requirements specification (see 7.2.3.2) for the safety function to meet a specific target failure measure, rather than a specific SIL. For example, when a target failure measure of 1.5 x 10^{-6} (probability of failure of dangerous failure per hour) is specified in order to meet the required risk reduction, then the probability of failure of the safety function due to random hardware failures will need to be equal to or less than 1.5 x 10^{-6} dangerous failures per hour.

NOTE 3 In order to demonstrate that this has been achieved it is necessary to carry out a reliability prediction for the relevant safety function using an appropriate technique (see 7.4.3.2.2) and compare the result to the target failure measure of the safety integrity requirement for the relevant safety function (see IEC 61508-1, Tables 2 & 3).

7.4.3.2.2 The probability of failure of each safety function, due to random hardware failures shall be estimated taking into account:

a) the architecture of the E/E/PE safety-related system as it relates to each safety function under consideration;

NOTE 1 This involves deciding which failure modes of the subsystems are in a series configuration (i.e. any failure causes failure of the relevant safety function to be carried out) and which are in a parallel configuration (i.e. co-incident failures are necessary for the relevant safety function to fail).

b) the estimated rate of failure of each subsystem in any modes which would cause a dangerous failure of the E/E/PE safety-related system but which are detected by diagnostic tests (see 7.4.7.3 & 7.4.7.4);

c) the estimated rate of failure of each subsystem in any modes which would cause a dangerous failure of the E/E/PE safety-related system which are undetected by the diagnostic tests (see 7.4.7.3 & 7.4.7.4);

d) the susceptibility of the E/E/PE safety-related system to common cause failures (see notes 2 & 11);

NOTE 2 For example, see IEC 61508-6, annex D

e) the diagnostic coverage of the diagnostic tests (determined according to annex C) and the associated diagnostic test interval;

NOTE 3 The diagnostic test interval and the subsequent time for repair together constitute the mean time for restoration which will be considered in the reliability model. Also, for E/E/PE safety-related systems operating in high demand or continuous mode of operation where any dangerous failure of a channel results in a dangerous failure of the E/E/PE safety-related system, the diagnostic test interval will need to be considered directly (ie in addition to the mean time to restoration) in the reliability model if it is not at least a magnitude less than the expected demand rate (see 7.4.3.2.5).

NOTE 4 When establishing the diagnostic test interval, the intervals between all of the tests which contribute to the diagnostic coverage will need to be considered.

f) the intervals at which proof tests are undertaken to reveal dangerous faults which are undetected by diagnostic tests;

g) the repair times for detected failures.

NOTE 5 The repair time will constitute one part of the mean time to restoration (see IEV 191-13-08), which will also include the time taken to detect a failure and any time period during which repair is not possible (see IEC 61508-6, annex B) for an example of how the mean time to restoration can be used to calculate the probability of failure). For situations where the repair can only be carried out during a specific period of time, for example while the EUC is shut down and in a safe state, it is particularly important that full account is taken of the time period when no repair can be carried out, especially when this is relatively large.

h) the probability of undetected failure of any data communication process (see Note 11 and 7.4.8.1)

NOTE 6 IEC 61508-6, Annex B describes a simplified approach which may be used to estimate the probability of dangerous failure of a safety function due to random hardware failures in order to determine that an architecture meets the required target failure measure.

NOTE 7 IEC 61508-6, Annex A, A.2 gives an overview of the necessary steps in achieving required hardware safety integrity, and shows how this subclause relates to other requirements of this standard.

NOTE 8 It is necessary to quantify separately for each safety function the reliability of the E/E/PE safety-related systems because different component failure modes will apply and the architecture of the E/E/PE safety-related systems (in terms of redundancy) may also vary.

NOTE 9 A number of modelling methods are available and the most appropriate method is a matter for the analyst and will depend on the circumstances. Available methods include:

—

— cause consequence analysis (see B.6.6.2 of IEC 61508-7);

— fault tree analysis (see B.6.6.5 of IEC 61508-7);

— Markov models (see C.6.4 of IEC 61508-7);

— reliability block diagrams (see C.6.5 of IEC 61508-7).

NOTE 10 The mean time to restoration (see IEV 191-13-08) which is considered in the reliability model will need to take into account the diagnostic test interval, the repair time and any other delays prior to restoration.

NOTE 11 Failures due to common cause effects and data communication processes may result from effects other than actual failures of hardware components (e.g. electromagnetic interference, decoding errors etc.), however, such failures are considered, for the purposes of this standard, as random hardware failures.

7.4.3.2.3 The diagnostic test interval of any subsystem having a hardware fault tolerance of more than zero shall be such as to enable the E/E/PE safety-related system to meet the requirement for the probability of random hardware failure (see 7.4.3.2.1).

7.4.3.2.4 The diagnostic test interval of any subsystem having a hardware fault tolerance of zero, on which a safety function is entirely dependent (see note), and which is only implementing safety function(s) operating in the low demand mode, shall be such as to enable the E/E/PE safety-related system to meet the requirement for the probability of random hardware failure (see 7.4.3.2.1).

NOTE 1 A safety function is considered to be entirely dependent on a subsystem if a failure of the subsystem causes a failure of the safety function in the E/E/PE safety-related system under consideration, and the safety function has not also been allocated to another safety-related system (see IEC 61508-1, 7.6).

NOTE 2 When there is a possibility that some combination of output states of a subsystem can directly cause a hazardous event (as determined by the hazard & risk analysis, see IEC 61508-1, 7.4.2.10) and when the combination of output states in the presence of a fault in the subsystem cannot be determined (for example, in the case of Type B subsystems), then it will be necessary to regard the detection of dangerous faults in the subsystem as a safety function operating in the high demand / continuous mode and the requirements of 7.4.6.3 and 7.4.3.2.5 will apply.

7.4.3.2.5 The diagnostic test interval of any subsystem having a hardware fault tolerance of zero, on which a safety function is entirely dependent (see note 1), and which is implementing any safety function operating in the high / continuous mode (see note 2), shall be such that the sum of the diagnostic test interval and the time to perform the specified action (fault reaction) to achieve or maintain a safe state (see 7.2.3.1 (g) is less than the process safety time. The process safety time is defined as the period of time between a failure occurring in the EUC or the EUC control system (with the potential to give rise to a hazardous event) and the occurrence of the hazardous event if the safety function is not performed..

NOTE 1 A safety function is considered to be entirely dependent on a subsystem if a failure of the subsystem causes a failure of the safety function in the E/E/PE safety-related system under consideration, and the safety function has not also been allocated to another safety-related system (see IEC 61508-1, 7.6).

NOTE 2 In the case of a subsystem implementing particular safety function where the ratio of the diagnostic test rate to the demand rate exceeds 100, then the subsystem can be treated as if it is implementing a safety function operating in the low demand mode (see 7.4.3.2.4), provided that the safety function is not preventing a combination of output states which could lead to a hazardous event (see note 3).

NOTE 3 If the safety function is to prevent a particular combination of output states which could directly cause a hazardous event, then it will always be necessary to regard such a safety function as operating in the high / continuous mode (see 7.4.2.12).

7.4.3.2.6 If, for a particular design, the target failure measure of the safety integrity requirement for the relevant safety function is not achieved then:

- determine the critical components, subsystems and/or parameters;
- evaluate the effect of possible improvement measures on the critical components, subsystems or parameters (for example, more reliable components, additional defences against common mode failures, increased diagnostic coverage, increased redundancy, reduced proof test interval, etc);
- select and implement the applicable improvements;
- repeat the necessary steps to establish the new probability of a hardware failure.

7.4.4 Requirements for the avoidance of failures

NOTE Clauses 7.4.4.1 to 7.4.4.6 do not apply in the case of a subsystem which meets the requirements to be considered as ‘proven-in-use’ (see 7.4.7.6 to 7.4.7.12)

7.4.4.1 An appropriate group of techniques and measures shall be used that are designed to prevent the introduction of faults during the design and development of the hardware of the E/E/PE safety-related system (see table B.2).

7.4.4.2 In accordance with the required safety integrity level the design method chosen shall possess features that facilitate

a) transparency, modularity and other features which control complexity;

b) clear and precise expression of:

- functionality,
- subsystem interfaces,
- sequencing and time-related information,
- concurrency and synchronisation;

c) clear and precise documentation and communication of information;

d) verification and validation.

7.4.4.3 Maintenance requirements, to ensure the safety integrity of the E/E/PE safety-related systems is kept at the required level, shall be formalised at the design stage.

7.4.4.4 Where applicable, automatic testing tools and integrated development tools shall be used.

7.4.4.5 During the design, E/E/PES integration tests shall be planned. Documentation of the test planning shall include:

a) the types of tests to be performed and procedures to be followed;

b) the test environment, tools, configuration and programs;

c) the pass/fail criteria.

7.4.4.6 During the design, those activities which can be carried out on the developer's premises shall be distinguished from those that require access to the user's site.

7.4.5 Requirements for the control of systematic faults

NOTE Clauses 7.4.5.1 to 7.4.5.3 do not apply in the case of a subsystem which meets the requirements to be considered as 'proven-in-use' (see 7.4.7.6 to 7.4.7.12)

7.4.5.1 For controlling systematic faults, the E/E/PES design shall possess design features that make the E/E/PE safety-related systems tolerant against

a) any residual design faults in the hardware, unless the possibility of hardware design faults can be excluded (see table A.16);

b) environmental stresses, including electromagnetic disturbances (see table A.17);

c) mistakes made by the operator of the EUC (see table A.18);

d) any residual design faults in the software (see 7.4.3 of IEC 61508-3 and associated table);

e) errors and other effects arising from any data communication process (see 7.4.8).

7.4.5.2 Maintainability and testability shall be considered during the design and development activities in order to facilitate implementation of these properties in the final E/E/PE safety-related systems.

7.4.5.3 The design of the E/E/PE safety-related systems shall take into account human capabilities and limitations and be suitable for the actions assigned to operators and maintenance staff. The design of all interfaces shall follow good human-factor practice and shall accommodate the likely level of training or awareness of operators, for example in mass-produced E/E/PE safety-related systems where the operator is a member of the public.

NOTE 1 The design goal should be that foreseeable critical mistakes made by operators or maintenance staff are prevented or eliminated by design wherever possible, or that the action requires secondary confirmation before completion.

NOTE 2 Some mistakes made by operators or maintenance staff may not be recoverable by E/E/PE safety-related systems, for example if they are not detectable or realistically recoverable except by direct inspection, such as some mechanical failures in the EUC.

7.4.6 Requirements for system behaviour on detection of a fault

7.4.6.1 The detection of a dangerous fault (by diagnostic tests, proof tests or by any other means) in any subsystem which has a hardware fault tolerance of more than zero shall result in either:

a) a specified action to achieve or maintain a safe state (see note), or

b) the isolation of the faulty part of the subsystem to allow continued safe operation of the EUC whilst the faulty part is repaired. If the repair is not completed within the mean time to restoration (MTTR) assumed in the calculation of the probability of random hardware failure (see 7.4.3.2.2), then a specified action shall take place to achieve or maintain a safe state (see note).

NOTE The specified action (fault reaction) required to achieve or maintain a safe state will be specified in the E/E/PES safety requirements (see 7.2.3.1). It may consist, for example, of the safe shut-down of the EUC, or that part of the EUC which relies, for risk reduction, on the faulty subsystem.

7.4.6.2 The detection of a dangerous fault (by diagnostic tests, proof tests or by any other means) in any subsystem having a hardware fault tolerance of zero and on which a safety function is entirely dependent (see note 1) shall, in the case that the subsystem is used only by safety function(s) operating in the low demand mode, result in either:

a) a specified action to achieve or maintain a safe state, or

b) the repair of the faulty subsystem within the mean time to restoration (MTTR) period assumed in the calculation of the probability of random hardware failure (see 7.4.3.2.2). During this time the continuing safety of the EUC shall be ensured by additional measures and constraints. The risk reduction provided by these measures and constraints shall be at least equal to the risk reduction provided by the E/E/PE safety-related system in the absence of any faults. The additional measures and constraints shall be specified in the E/E/PES Operation and Maintenance procedures (see 7.6). If the repair is not undertaken within the specified mean time to restoration (MTTR) then a specified action shall be performed to achieve or maintain a safe state (see note 2).

NOTE 1 A safety function is considered to be entirely dependent on a subsystem if a failure of the subsystem causes a failure of the safety function in the E/E/PE safety-related system under consideration, and the safety function has not also been allocated to another safety-related system (see IEC 61508-1, 7.6).

NOTE 2 The specified action (fault reaction) required to achieve or maintain a safe state will be specified in the E/E/PES safety requirements (see 7.2.3.1). It may consist, for example, of the safe shut-down of the EUC, or that part of the EUC which relies, for risk reduction, on the faulty subsystem.

7.4.6.3 The detection of a dangerous fault (by diagnostic tests, proof tests or by any other means) in any subsystem having a hardware fault tolerance of zero, and on which a safety function is entirely dependent (see note 1) shall, in the case of a subsystem which is implementing any safety function(s) operating in the high / continuous demand mode (see notes 2,3), result in a specified action to achieve or maintain a safe state (see note 3).

NOTE 1 A safety function is considered to be entirely dependent on a subsystem if a failure of the subsystem causes a failure of the safety function in the E/E/PE safety-related system under consideration, and the safety function has not also been allocated to another safety-related system (see IEC 61508-1, 7.6).

NOTE 2 When there is a possibility that some combination of output states of a subsystem can directly cause a hazardous event (as determined by the hazard & risk analysis, (see 7.4.2.12)) and when the combination of output states in the presence of a fault in the subsystem cannot be determined (for example, in the case of Type B subsystems), then it will be necessary to regard the detection of dangerous faults in the subsystem as a safety function operating in the high demand / continuous mode and the requirements of 7.4.6.3 and 7.4.3.2.5 will apply.

NOTE 3 The specified action (fault reaction) required to achieve or maintain a safe state will be specified in the E/E/PES safety requirements (see 7.2.3.1). It may consist, for example, of the safe shut-down of the EUC, or that part of the EUC which relies, for risk reduction, on the faulty subsystem.

7.4.7 Requirements for E/E/PES implementation

7.4.7.1 The E/E/PE safety-related system shall be implemented according to the E/E/PES design.

7.4.7.2 All subsystems which are used by one or more safety functions shall be identified and documented as safety-related subsystems.

7.4.7.3 The following information shall be available for each safety-related subsystem (see also 7.4.7.4):

a) a functional specification of those functions and interfaces of the subsystem which can be used by safety functions;

b) the estimated rates of failure (due to random hardware failures) in any modes which would cause a dangerous failure of the E/E/PE safety-related system, which are detected by diagnostic tests (see 7.4.7.4);

c) the estimated rates of failure (due to random hardware failures) in any modes which would cause a dangerous failure of the E/E/PE safety-related system, which are undetected by diagnostic tests (see 7.4.7.4);

d) any limits on the environment of the subsystem which should be observed in order to maintain the validity of the estimated rates of failure due to random hardware failures;

e) any limit on the lifetime of the subsystem which should not be exceeded in order to maintain the validity of the estimated rates of failure due to random hardware failures;

f) any periodic proof test and / or maintenance requirements;

g) the diagnostic coverage derived according to annex C (when required, see note 1)

h) the diagnostic test interval (when required, see note 1);

NOTE 1 Items g) and h) above relate to diagnostic tests which are internal to the subsystem. This information is only required when credit is claimed for the action of the diagnostic tests performed in the subsystem in the reliability model of the E/E/PE safety-related system (see 7.4.3.2.2).

i) any additional information (e.g. repair times) which is necessary to allow the derivation of a mean time to restoration (MTTR) following detection of a fault by the diagnostics;

NOTE 2 Items b) to i) are needed to allow the probability of failure on demand, or the probability of failure per hour of the safety function to be estimated (see 7.4.3.2.2)

NOTE 3 Items b), c), g), h) and i) are only required as separate parameters for subsystems such as sensors and actuators which may be combined in redundant architectures to improve hardware safety integrity. For items such as logic solvers which will not themselves be combined in redundant architectures in the E/E/PE safety-related system, it is acceptable to specify performance in terms of probability of failure on demand, or probability of dangerous failure per hour taking into account items b), c), g), h) and i). For such items it will also be necessary to establish the proof test interval for failures which are undetected.

j) all information which is necessary to enable the derivation of the safe failure fraction (SFF) of the subsystem as applied in the E/E/PE safety-related system, determined according to annex C;

k) the hardware fault tolerance of the subsystem;

NOTE 4 Items j) and k) are needed to determine the highest safety integrity level that can be claimed for a safety function according to the architectural constraints (see 7.4.3.1)

l) any limits on the application of the subsystem which should be observed in order to avoid systematic failures;

m) the highest safety integrity level that can be claimed for a safety function which uses the subsystem on the basis of:

— measures and techniques used to prevent systematic faults being introduced during the design and implementation of the hardware and software of the subsystem (see 7.4.4.1 and 61508-3, 7.4),

— the design features which make the subsystem tolerant against systematic faults (see 7.4.5.1);

NOTE 5 This is not required in the case of those subsystems which are considered to have been proven-in-use (see 7.4.7.5).

n) any information which is required to identify the hardware and software configuration of the subsystem in order to enable the configuration management of the E/E/PE safety-related system in accordance with IEC 61508-1, 6.2.1.

o) documentary evidence that the subsystem has been validated according to clause 7.7 (E/E/PES safety validation) of this standard.

NOTE 6 Evidence of validation is not required in the case of a subsystem which is considered to have been proven-in-use (see 7.4.7.5)

7.4.7.4 The estimated rates of failure, due to random hardware failures, for subsystems (see 7.4.7.3 b) and c)) can be determined either

a) by a failure modes and effects analysis of the design using component failure data from a recognised industry source, NOTE 1 Any failure rate data used should have a confidence level of at least 70%. The statistical determination of confidence level is defined in IEEE 352. An equivalent term, significance level, is used in IEC 61164.

NOTE 2 If site specific failure data are available then this is preferred. If this is not the case then generic data may have to be used.

NOTE 3 Although a constant failure rate is assumed by most probabilistic estimation methods this only applies provided that the useful lifetime of components is not exceeded. Beyond their useful lifetime (ie as the probability of failure significantly increases with time) the results of most probabilistic calculation methods are therefore meaningless. Thus any probabilistic estimation should include a specification of the components' useful lifetimes. The useful lifetime is highly dependent on the component itself and its operating conditions – temperature in particular (for example, electrolyte capacitors can be very sensitive). Experience has shown that the useful lifetime often lays within a range of 8 to 12 years. It can, however, be significantly less if components are operated near to their specification limits. Components with longer useful lifetimes tend to be considerably more expensive.

or;

b) from experience of the previous use of the subsystem in a similar environment (see 7.4.7.9).

7.4.7.5 In the case of a subsystem which is regarded as proven-in-use (see 7.4.7.6), then information regarding the measures and techniques for the prevention and control of systematic faults (see 7.4.7.3 m)) and evidence of validation (see 7.4.7.3 o)) is not required

7.4.7.6 A previously developed subsystem shall only be regarded as proven-in-use when it has a clearly restricted functionality and when there is adequate documentary evidence which is based on the previous use of a specific configuration of the subsystem (during which time all failures have been formally recorded, see 7.4.7.10), and which takes into account any additional analysis or testing, as required (see 7.4.7.8). The documentary evidence shall demonstrate that the likelihood of any failure of the subsystem (due to random hardware and systematic faults) in the E/E/PE safety-related system is low enough so that the required safety integrity level(s) of the safety function(s) which use the subsystem is achieved.

7.4.7.7 The documentary evidence required by 7.4.7.6 shall demonstrate that the previous conditions of use (see note) of the specific subsystem are the same as, or sufficiently close to, those which will be experienced by the subsystem in the E/E/PE safety-related system, in order to determine that the likelihood of any unrevealed systematic faults is low enough so that the required safety integrity level(s) of the safety function(s) which use the subsystem is achieved.

NOTE The conditions of use (operational profile) include all the factors which may influence the likelihood of systematic faults in the hardware and software of the subsystem. For example, environment, modes of use, functions performed, configuration, interfaces to other systems, operating system, translator, human factors.

7.4.7.8 When there is any difference between the previous conditions of use and those which will be experienced in the E/E/PE safety-related system, then any such difference(s) shall be identified and there shall be an explicit demonstration, using a combination of appropriate analytical methods and testing, in order to determine that the likelihood of any unrevealed systematic faults is low enough so that the required safety integrity level(s) of the safety function(s) which use the subsystem is achieved.

7.4.7.9 The documentary evidence required by 7.4.7.6 shall establish that the extent of previous use of the specific configuration of the subsystem (in terms of operational hours), is sufficient to support the claimed rates of failure on a statistical basis. As a minimum, sufficient operational time is required to establish the claimed failure rate data to a single-sided lower confidence limit of at least 70 % (see IEC 61508-7, Annex D & IEEE 352). An operational time of any individual subsystem of less than one year shall not be considered as part of the total operational time in the statistical analysis (see note).

NOTE The necessary time, in terms of operational hours, required to establish the claimed rates of failure may result from the operation of a number of identical subsystems, provided that failures from all the subsystems have been effectively detected and reported (see 7.4.7.10). If, for example, 100 subsystems each work fault free for 10,000 hours, then the total time of fault free operation may be considered as 1,000,000 hours. In this case, each subsystem has been in use for over a year and the operation therefore counts towards the total number of operational hours considered.

7.4.7.10 Only previous operation where all failures of the subsystem have been effectively detected and reported (for example, when failure data has been collected in accordance with the recommendations of IEC 300-3-2) shall be taken into account when determining whether the above requirements (7.4.7.6 to 7.4.7.9) have been met.

7.4.7.11 The following factors shall be taken into account when determining whether or not the above requirements (7.4.7.6 to 7.4.7.9) have been met, in terms of both the coverage and degree of detail of the available information (see also IEC 61508-1, 4.1):

a) the complexity of the subsystem;

b) the contribution made by the subsystem to the risk reduction;

c) the consequence associated with a failure of the subsystem;

d) the novelty of design.

7.4.7.12 The application of a ‘proven-in-use’ safety-related subsystem in the E/E/PE safety-related system should be restricted to those functions and interfaces of the subsystem which meet the relevant requirements (see 7.4.7.6 to 7.4.7.10).

NOTE The measures 7.4.7.4 to 7.4.7.12 are also applicable for subsystems which contain software. In this case it has to be assured that the subsystem performs in its safety related application only that function for which evidence of the required safety integrity is given. See also IEC 61508-3, 7.4.2.11.

7.4.8 Requirements for data communications

7.4.8.1 When any form of data communication is used in the implementation of a safety function then the probability of undetected failure of the communication process shall be estimated taking into account transmission errors, repetitions, deletion, insertion, re-sequencing, corruption, delay and masquerade (see also 7.4.8.2). This probability shall be taken into account when estimating the probability of dangerous failure of the safety function due to random hardware failures (see 7.4.3.2.2).

NOTE The term masquerade means that the true contents of a message are not correctly identified. For example a message from a non-safety component is incorrectly identified as a message from a safety component.

7.4.8.2 In particular, the following parameters shall be taken into account when estimating the probability of failure of the safety function due to the communication process:

a) the residual error rate (see IEV 371-08-05);

b) the rate of residual information loss (see IEV 371-08-09);

c) the limits, and variability, of the rate of information transfer (bit rate);

d) the limits, and variability, of the information propagation delay time.

NOTE 1 It can be shown that the probability of a dangerous failure per hour is equal to the quotient of the residual error probability and the message length (in bits) multiplied by the bus transmission rate for safety-related messages and a factor of 3600.

NOTE 2 Further information can be found in IEC 870-5-1 “Telecontrol equipment & systems - part 5: Transmission protocols - section 1: Transmission frame formats” and in EN 50159-1 “Railway applications - Safety-related communication in closed transmission systems” and EN 50159-2 “Railway applications - Safety-related communication in open transmission systems.”

7.5 E/E/PES integration

NOTE This phase is box 9.4 of figure 2.

7.5.1 Objective

The objective of the requirements of this subclause is to integrate and test the E/E/PE safety-related systems.

7.5.2 Requirements

7.5.2.1 The E/E/PE safety-related systems shall be integrated according to the specified E/E/PES design and shall be tested according to the specified E/E/PES integration tests (see 7.4.2.11).

7.5.2.2 As part of the integration of all modules into the E/E/PE safety-related systems, the E/E/PE safety-related systems shall be tested as specified (see 7.4). These tests shall show that all modules interact correctly to perform their intended function and are designed not to perform unintended functions.

NOTE 1 This does not imply testing of all input combinations. Testing all equivalence classes (see B.5.2 of IEC 61508-7) may suffice. Static analysis (see B.6.4 of IEC 61508-7), dynamic analysis (see B.6.5 of IEC 61508-7) or failure analysis (see B.6.6 of IEC 61508-7) may reduce the number of test cases to an acceptable level. In case of development according to the rules leading to structured design (see B.3.2 of 61508-7) or semi-formal methods (see B.2.3 of 61508-7) the requirements are easier to fulfil than if not.

NOTE 2 Where the development uses formal methods (see B.2.2 of IEC 61508-7) or by using formal proofs or assertions (see C.5.13 and C.3.3 of 61508-7), such tests may be reduced in scope.

NOTE 3 Statistical evidence may be used as well (see B.5.3 of IEC 61508-7).

7.5.2.3 The integration of safety-related software into the PES shall be done according to 7.5 of IEC 61508-3.

7.5.2.4 Appropriate documentation of the integration testing of the E/E/PE safety-related systems shall be produced, stating the test results and whether the objectives and criteria specified during the design and development phase have been met. If there is a failure, the reasons for the failure and its correction shall be documented.

7.5.2.5 During the integration and testing, any modifications or change to the E/E/PE safety-related systems shall be subject to an impact analysis which shall identify all components affected and the necessary re-verification activities.

7.5.2.6 The E/E/PES integration testing shall document the following information:

a) the version of the test specification used;

b) the criteria for acceptance of the integration tests;

c) the version of the E/E/PE safety-related systems being tested;

d) the tools and equipment used along with calibration data;

e) the results of each test;

f) any discrepancy between expected and actual results;

g) the analysis made and the decisions taken on whether to continue the test or issue a change request, in the case when discrepancies occur.

7.5.2.7 For the avoidance of faults during the E/E/PES integration, an appropriate group of techniques and measures according to table B.3 shall be used.

7.6 E/E/PES operation and maintenance procedures

NOTE This phase is box 9.5 of figure 2.

7.6.1 Objective

The objective of the requirements of this subclause is to develop procedures to ensure that the required functional safety of the E/E/PE safety-related systems is maintained during operation and maintenance.

7.6.2 Requirements

7.6.2.1 E/E/PES operation and maintenance procedures shall be prepared which shall specify the following:

a) the routine actions which need to be carried out to maintain the "as designed" functional safety of the E/E/PE safety-related systems, including routine replacement of components with a pre-defined life, e.g. cooling fans, batteries, etc.;

b) the actions and constraints that are necessary (for example, during installation, start-up, normal operation, routine testing, foreseeable disturbances, faults or failures, and shut-down) to prevent an unsafe state and/or reduce the consequences of a hazardous event;

c) the documentation which needs to be maintained on system failure and demand rates on the E/E/PE safety-related systems;

d) the documentation which needs to be maintained showing results of audits and tests on the E/E/PE safety-related systems;

e) the maintenance procedures to be followed when faults or failures occur in the E/E/PE safety-related systems, including:

— procedures for fault diagnoses and repair,

— procedures for revalidation,

— maintenance reporting requirements;

f) the procedures for reporting maintenance performance shall be specified. In particular:

— procedures for reporting failures,

— procedures for analysing failures;

g) the tools necessary for maintenance and revalidation and procedures for maintaining the tools and equipment.

NOTE 1 It may be beneficial, for reasons of both safety and economics, to integrate the E/E/PES operation and maintenance procedures with the EUC overall operation and maintenance procedures.

NOTE 2 The E/E/PES operation and maintenance procedures should include the software modification procedures (see IEC 61508-3, 7.8).

7.6.2.2 The E/E/PE safety-related system operation and maintenance procedures shall be continuously upgraded from inputs such as (1) the results of functional safety audits and (2) tests on the E/E/PE safety-related systems.

7.6.2.3 The routine maintenance actions required to maintain the required functional safety (as designed) of the E/E/PE safety-related systems shall be determined by a systematic method. This method shall determine unrevealed failures of all safety-related components (from sensors through to final elements) which would cause a reduction in the safety integrity achieved. Suitable methods include:

— examination of fault trees;

— failure mode and effect analysis;

— reliability centred maintenance.

NOTE 1 A consideration of human factors is a key element in determining the actions required and the appropriate interface(s) with the E/E/PE safety-related systems.

NOTE 2 Proof tests will be carried out with a frequency necessary to achieve the target failure measure.

NOTE 3 The frequency of the proof tests, the diagnostic test interval and the time for subsequent repair will be dependent upon several factors (see annex B of IEC 61508-6), including:

— the target failure measure associated with the safety integrity level;

— the architecture;

— the diagnostic coverage of the diagnostic tests, and

— the expected demand rate.

NOTE 4 The frequency of the proof tests and the diagnostic test interval are likely to have a crucial bearing on the achievement of hardware safety integrity. One of the principal reasons for carrying out hardware reliability analysis (see 7.4.3.2.2) is to ensure that the frequencies of the two types of tests are appropriate for the target hardware safety integrity.

7.6.2.4 The E/E/PES operation and maintenance procedures shall be assessed for the impact they may have on the EUC.

7.6.2.5 For the avoidance of faults and failures during the E/E/PES operation and maintenance procedures, an appropriate group of techniques and measures according to table B.4 shall be used.

7.7 E/E/PES safety validation

NOTE This phase is box 9.6 of figure 2.

7.7.1 Objective

The objective of the requirements of this subclause is to validate that the E/E/PE safety-related systems meet, in all respects, the requirements for safety in terms of the required safety functions and the safety integrity (see 7.2).

7.7.2 Requirements

7.7.2.1 The validation of the E/E/PES safety shall be carried out in accordance with a prepared plan (see also 7.7 of IEC 61508-3).

NOTE 1 The E/E/PES safety validation is shown on the E/E/PES safety lifecycle as being carried out prior to installation but in some cases the E/E/PES safety validation cannot be carried out until after installation (for example, when the application software development is not finalised until after installation).

NOTE 2 Validation of a programmable electronic safety-related system comprises validation of both hardware and software. The requirements for validation of software are contained in IEC 61508-3.

7.7.2.2 All test measurement equipment used for validation shall be calibrated against a standard traceable to a national standard, if available, or to a well-recognized procedure. All test equipment shall be verified for correct operation.

7.7.2.3 Each safety function specified in the requirements for E/E/PES safety (see 7.2), and all the E/E/PES operation and maintenance procedures shall be validated by test and/or analysis.

7.7.2.4 Appropriate documentation of the E/E/PES safety validation testing shall be produced which shall state for each safety function:

a) the version of the E/E/PES safety validation plan being used;

b) the safety function under test (or analysis), along with the specific reference to the requirement specified during E/E/PES safety validation planing;

c) tools and equipment used, along with calibration data;

d) the results of each test;

e) discrepancies between expected and actual results.

NOTE Separate documentation is not needed for each safety function, but the information in a) to e) must apply to every safety function and where it differs by safety function the relationship must be stated.

7.7.2.5 When discrepancies occur (i.e. the actual results deviate from the expected results by more than the stated tolerances), the results of the E/E/PES safety validation testing shall be documented, including:

a) the analysis made; and

b) the decision taken on whether to continue the test or issue a change request and return to an earlier part of the validation test.

7.7.2.6 The supplier or developer shall make available results of the E/E/PES safety validation testing to the developer of the EUC and the EUC control system so as to enable them to meet the requirements for overall safety validation in IEC 61508-1.

7.7.2.7 For the avoidance of faults during the E/E/PES safety validation, an appropriate group of techniques and measures according to table B.5 shall be used.

7.8 E/E/PES modification

7.8.1 Objective

The objective of the requirements of this subclause is to ensure that the required safety integrity is maintained after corrections, enhancements or adaptations to the E/E/PE safety-related systems.

7.8.2 Requirements

7.8.2.1 Appropriate documentation shall be established and maintained for each E/E/PES modification activity. The documentation shall include:

a) the detailed specification of the modification or change;

b) an analysis of the impact of the modification activity on the overall system, including hardware, software (see IEC 61508-3), human interaction and the environment and possible interactions;

c) all approvals for changes;

d) progress of changes;

e) test cases for components including revalidation data;

f) E/E/PES configuration management history;

g) deviation from normal operations and conditions;

h) necessary changes to system procedures;

i) necessary changes to documentation.

7.8.2.2 Manufacturers or system suppliers which claim compliance with all or part of this standard shall maintain a system to initiate changes as a result of defects being detected in hardware or software and to inform users of the need for modification in the event of the defect affecting safety.

7.8.2.3 Modifications shall be performed with at least the same level of expertise, automated tools (see 7.4.4.2 of IEC61508-3), and planning and management as the initial development of the E/E/PE safety-related systems.

7.8.2.4 After modification, the E/E/PE safety-related systems shall be reverified and revalidated.

NOTE See also 7.16.2.6 of IEC 61508-1.

7.9 E/E/PES verification

7.9.1 Objective

The objective of the requirements of this subclause is to test and evaluate the outputs of a given phase to ensure correctness and consistency with respect to the products and standards provided as input to that phase.

NOTE For convenience all verification activities have been drawn together under 7.9, but they are actually performed across several phases.

7.9.2 Requirements

7.9.2.1 The verification of the E/E/PE safety-related systems shall be planned concurrently with the development (see 7.4), for each phase of the E/E/PES safety lifecycle, and shall be documented.

7.9.2.2 The E/E/PES verification planning shall refer to all the criteria, techniques and tools to be utilised in the verification for that phase.

7.9.2.3 The E/E/PES verification planning shall specify the activities to be performed to ensure correctness and consistency with respect to the products and standards provided as input to that phase.

7.9.2.4 The E/E/PES verification planning shall consider the following:

a) the selection of verification strategies and techniques;

b) the selection and utilisation of the test equipment;

c) the selection and documentation of verification activities;

d) the evaluation of verification results gained from verification equipment direct and from tests.

7.9.2.5 In each design and development phase it shall be shown that the functional and safety integrity requirements are met.

7.9.2.6 The result of each verification activity shall be documented, stating either that the E/E/PE safety-related systems have passed the verification, or the reasons for the failures. The following shall be considered:

a) items which do not conform to one or more relevant requirements of the E/E/PES safety lifecycle (see 7.2);

b) items which do not conform to one or more relevant design standards (see 7.4);

c) items which do not conform to one or more relevant safety management requirements (see clause 6).

7.9.2.7 For E/E/PES safety requirements verification, after E/E/PES safety requirements have been established (see 7.2), and before the next phase (design and development) begins, verification shall:

a) determine whether the E/E/PES safety requirements are adequate to satisfy the requirements set out in the E/E/PES safety requirements allocation (see IEC 61508-1) for safety, functionality, and other requirements specified during safety planning, and

b) check for incompatibilities between:

- the E/E/PES safety requirements (7.2),
- the safety requirements allocation (IEC 61508-1),
- the E/E/PES tests (see 7.4), and

— the user documentation and all other system documentation.

7.9.2.8 For E/E/PES design and development verification, after E/E/PES design and development (see 7.4) has been completed and before the next phase (integration) begins, verification shall:

a) determine whether the E/E/PES tests (see 7.4) are adequate for the E/E/PES design and development (see 7.4);

b) determine the consistency and completeness (down to and including module level) of the E/E/PES design and development (see 7.4) with respect to the E/E/PES safety requirements (see 7.2); and

c) check for incompatibilities between:

   — the E/E/PES safety requirements (7.2),

   — the E/E/PES design and development (7.4), and

   — the E/E/PES tests (see 7.4).

NOTE 1 Table B.5 recommends safety validation, failure analysis and testing techniques that are also applicable to verification.

NOTE 2 Verification that the diagnostic coverage has been achieved will take into account table A.1, which gives the faults and failures that must be detected.

7.9.2.9 For E/E/PES integration verification, the integration of the E/E/PE safety-related systems shall be verified to establish that the requirements of 7.5 have been achieved.

7.9.2.10 Test cases and their results shall be documented.

8 Functional safety assessment

The requirements for functional safety assessment are as detailed in clause 8 of IEC 61508-1.

Annex A
(normative)

Techniques and measures for E/E/PE safety-related systems: control of failures during operation

A.1 General

This annex shall be used in conjunction with 7.4. It limits the maximum diagnostic coverage that may be claimed for relevant techniques and measures. For each safety integrity level, the annex recommends techniques and measures for controlling random hardware, systematic, environmental and operational failures. More information about architectures and measures can be found in annex B of IEC 61508-6 and annex A of IEC 61508-7.

It is not possible to list every individual physical cause of a failure in complex hardware for two main reasons:

— the cause/effect relationship between faults and failures is often difficult to determine;

— the emphasis on failures changes from random to systematic when complex hardware and software is used.

Failures in E/E/PE safety-related systems may be categorised, according to the time of their origin, into:

— failures caused by faults originating **before or during system installation** (for example, software faults include specification and program faults, hardware faults include manufacturing faults and incorrect selection of components); and

— failures caused by faults or human errors originating **after system installation** (for example random hardware failures, or failures caused by incorrect use).

In order to avoid or control such failures when they occur, a large number of measures are normally necessary. The structure of the requirements in annexes A and B results from dividing the measures into those used to **avoid failures** during the different phases of the E/E/PES safety lifecycle (annex B), and those used to **control failures** during operation (this annex). The measures to control failures are built-in features of the E/E/PE safety-related systems.

Diagnostic coverage and safe failure fraction is determined on the basis of table A.1 and according to procedures detailed in annex C. Tables A.2 to A.15 support the requirements of table A.1 by recommending techniques and measures for diagnostic tests and recommending maximum levels of diagnostic coverage that can be achieved using them. The tables do not replace any of the requirements of annex C. Tables A.2 to A.15 are not exhaustive. Other measures and techniques may be used, provided evidence is produced to support the claimed diagnostic coverage. If high diagnostic coverage is being claimed then, as a minimum, at least one technique of high diagnostic coverage should be applied from each of these tables.

Similarly, tables A.16 to A.18 recommend techniques and measures for each safety integrity level for controlling systematic failures. Table A.16 recommends overall measures to control systematic failures (see also IEC 61508-3), table A.17 recommends measures to control environmental failures and table A.18 recommends measures to control operational failures. Most of these control measures can be graded according to table A.19.

All techniques and measures in these tables are described in annex A of IEC 61508-7. Software techniques and measures required for each safety integrity level are given in IEC 61508-3. Guidelines for determining the architecture for an E/E/PE safety-related system are given in annex B of IEC 61508-6.

Following the guidelines in this annex does not guarantee by itself the required safety integrity. It is important to consider:

— the consistency of the chosen techniques and measures, and how well they will complement each other; and

— which techniques and measures are most appropriate for the specific problems encountered during the development of each particular E/E/PE safety-related system.

A.2 Hardware safety integrity

Table A.1 provides the requirements for faults or failures that shall be detected by techniques and measures to control hardware failures, in order to achieve the relevant level of diagnostic coverage (see also annex C). Tables A.2 to A.15 support the requirements of table A.1 by recommending techniques and measures for diagnostic tests and recommending maximum levels of diagnostic coverage that can be achieved using them. These tests may operate continuously or periodically. The tables do not replace any of the requirements of 7.4. Tables A.2 to A.15 are not exhaustive. Other measures and techniques may be used, provided evidence is produced to support the claimed diagnostic coverage.

NOTE 1 The overview of techniques and measures associated with these tables is in annex A of IEC 61508-7. The relevant subclause is referenced in the second column of tables A.2 to A.15.

NOTE 2 The designations low, medium and high diagnostic coverage are quantified as 60 %, 90 % and 99 % respectively.

Table A.1 — Faults or failures to be detected during operation or to be analysed in the derivation of safe failure fraction

Component	See Table(s)	Requirements for diagnostic coverage or safe failure fraction claimed		
		Low (60 %)	Medium (90 %)	High (99 %)
Electromechanical devices	A.2	Does not energize or de-energize; Welded contacts	Does not energize or de-energize; Individual contacts welded	Does not energize or de-energize; Individual contacts welded, No positive guidance of contacts (for relays this failure is not assumed if they are built and tested according to EN 50205 or equivalent), No positive opening (for position switches this failure is not assumed if they are built and tested according to EN 60947-5-1, part 5, section 1 or equivalent)
Discrete hardware	A.3, A.7, A.9, A.11			
Digital I/O		Stuck-at	DC fault model	DC fault model; drift and oscillation
Analogue I/O		Stuck-at	DC fault model; drift and oscillation	DC fault model; drift and oscillation
Power supply		Stuck-at	DC fault model; drift and oscillation	DC fault model; drift and oscillation
Bus	A.3			
General	A.7	Stuck-at of the addresses	Time out	Time out
Memory management unit	A.8	Stuck-at of data or addresses	Wrong address decoding	Wrong address decoding
Direct memory access		no or continuous access	DC fault model for data and addresses; Wrong access time	All faults which affect data in the memory; Wrong data or addresses; wrong access time
Bus-arbitration (see note 1)		Stuck-at of arbitration signals	No or continuous arbitration	No or continuous or wrong arbitration
CPU	A.4, A.10			
Register, internal RAM		Stuck-at for data and addresses	DC fault model for data and addresses	DC fault model for data and addresses; Dynamic cross-over for memory cells; No, wrong or multiple addressing
Coding and execution including flag register		Wrong coding or no execution	Wrong coding or wrong execution	No definite failure assumption
Address calculation		Stuck-at	DC fault model	No definite failure assumption
Program counter, stack pointer		Stuck-at	DC fault model	DC fault model
Interrupt handling	A.4	No or continuous interrupts	No or continuous interrupts; cross-over of interrupts	No or continuous interrupts; cross-over of interrupts
Invariable memory	A.5	Stuck-at for data and addresses	DC fault model for data and addresses	All faults which affect data in the memory
Variable memory	A.6	Stuck-at for data and addresses	DC fault model for data and addresses; change of information caused by soft-errors for DRAM with integration 1 Mbits and higher	DC fault model for data and addresses; dynamic cross-over for memory cells; no, wrong or multiple addressing; change of information caused by soft-errors for DRAM with integration 1 Mbits and higher

Clock (quartz)	A.12	Sub- or super-harmonic	Sub- or super-harmonic	Sub- or super-harmonic
Communication and mass storage	A.13	Wrong data or addresses; No transmission	All faults which affect data in the memory; Wrong data or addresses; Wrong transmission time; Wrong transmission sequence	All faults which affect data in the memory; Wrong data or addresses; Wrong transmission time; Wrong transmission sequence

Table A.1 (*concluded*)

Component	See Table	Requirements for diagnostic coverage or safe failure fraction claimed		
		Low (60 %)	Medium (90 %)	High (99 %)
Sensors	A.14	Stuck-at	DC fault model; Drift and oscillation	DC fault model; Drift and oscillation
Final elements	A.15	Stuck-at	DC fault model; Drift and oscillation	DC fault model; Drift and oscillation

NOTE 1 Bus-arbitration is the mechanism for deciding which device has control of the bus.

NOTE 2 “Stuck-at" is a fault category which can be described with continuous " 0" or " 1" or " on" at the pins of a component.

NOTE 3 "DC fault model" (DC = direct current) includes the following failure modes: stuck-at faults, stuck-open, open or high impedance outputs as well as short circuits between signal lines.

Table A.2 — Electrical subsystems

Diagnostic technique/measure	See IEC 61508-7	Maximum diagnostic coverage considered achievable	Notes
Failure detection by on-line monitoring	A.1.1	low (low demand mode) medium (high demand or continuous mode)	depends on diagnostic coverage of failure detection
Monitoring of relay contacts	A.1.2	high	high diagnostic coverage is only achievable if the relay switching time interval is much smaller than the demand rate
Comparator	A.1.3	high	high if failure modes are predominantly in a safe direction
Majority voter	A.1.4	high	depends on the quality of the voting
Idle current principle	A.1.5	low	only for E/E/PE safety-related systems where continuous control is not needed to achieve or maintain a safe state of the EUC

NOTE 1 This table does not replace any of the requirements of annex C.

NOTE 2 The requirements of annex C are relevant for the determination of diagnostic coverage.

NOTE 3 For general notes concerning this table, see the text preceding table A.1.

Table A.3 — Electronic subsystems

Diagnostic technique/measure	See IEC 61508-7	Maximum diagnostic coverage considered achievable	Notes
Failure detection by on-line monitoring	A.1.1	low (low demand mode) medium (high demand or continuous mode)	depends on diagnostic coverage of failure detection
Comparator	A.1.3	high	high if failure modes are predominantly in a safe direction
Majority voter	A.1.4	high	depends on the quality of the voting
Tests by redundant hardware	A.2.1	medium	depends on diagnostic coverage of failure detection
Dynamic principles	A.2.2	medium	depends on diagnostic coverage of failure detection
Standard test access port and boundary-scan architecture	A.2.3	high	depends on the diagnostic coverage of failure detection
Monitored redundancy	A.2.5	high	depends on the degree of redundancy and of the monitoring
Hardware with automatic check	A.2.6	high	depends on the diagnostic coverage of the tests
Analogue signal monitoring	A.2.7	low	

NOTE 1 This table does not replace any of the requirements of annex C.

NOTE 2 The requirements of annex C are relevant for the determination of diagnostic coverage.

NOTE 3 For general notes concerning this table, see the text preceding table A.1.

Table A.4 — Processing units

Diagnostic technique/measure	See IEC 61508-7	Maximum diagnostic coverage considered achievable	Notes
Comparator	A.1.3	high	depends on the quality of the comparison
Majority voter	A.1.4	high	depends on the quality of the voting
Self-test by software: limited number of patterns (one channel)	A.3.1	low	
Self-test by software: walking bit (one-channel)	A.3.2	medium	
Self-test supported by hardware (one-channel)	A.3.3	medium	
Coded processing (one-channel)	A.3.4	high	
Reciprocal comparison by software	A.3.5	high	depends on the quality of the comparison

NOTE 1 This table does not replace any of the requirements of annex C.

NOTE 2 The requirements of annex C are relevant for the determination of diagnostic coverage.

NOTE 3 For general notes concerning this table, see the text preceding table A.1.

Table A.5 — Invariable memory ranges

Diagnostic technique/measure	See IEC 61508-7	Maximum diagnostic coverage considered achievable	Notes
Word-saving multi-bit redundancy	A.4.1	medium	
Modified checksum	A.4.2	low	
Signature of one word (8-bit)	A.4.3	medium	the effectiveness of the signature depends on the width of the signature in relation to the block length of the information to be protected
Signature of a double word (16-bit)	A.4.4	high	the effectiveness of the signature depends on the width of the signature in relation to the block length of the information to be protected
Block replication	A.4.5	high	

NOTE 1 This table does not replace any of the requirements of annex C.

NOTE 2 The requirements of annex C are relevant for the determination of diagnostic coverage.

NOTE 3 For general notes concerning this table, see the text preceding table A.1.

Table A.6 — Variable memory ranges

Diagnostic technique/measure	See IEC 61508-7	Maximum diagnostic coverage considered achievable	Notes
RAM test "checkerboard" or "march"	A.5.1	low	
RAM test "walk-path"	A.5.2	medium	
RAM test "galpat" or "transparent galpat"	A.5.3	high	
RAM test "Abraham"	A.5.4	high	
Parity-bit for RAM	A.5.5	low	
RAM monitoring with a modified Hamming code, or detection of data failures with error-detection-correction codes (EDC)	A.5.6	high	
Double RAM with hardware or software comparison and read/write test	A.5.7	high	

NOTE 1 This table does not replace any of the requirements of annex C.

NOTE 2 The requirements of annex C are relevant for the determination of diagnostic coverage.

NOTE 3 For general notes concerning this table, see the text preceding table A.1.

NOTE 4 For RAM which is read/written only infrequently (e.g. during configuration) the measures A.4.1 to A.4.4 are effective if they are executed after each read/write access.

Table A.7 — I/O units and interface (external communication)

Diagnostic technique/measure	See IEC 61508-7	Maximum diagnostic coverage considered achievable	Notes
Failure detection by on-line monitoring	A.1.1	low (low demand mode) medium (high demand or continuous mode)	depends on diagnostic coverage of failure detection
Test pattern	A.6.1	high	
Code protection	A.6.2	high	
Multi-channel parallel output	A.6.3	high	only if dataflow changes within diagnostic test interval
Monitored outputs	A.6.4	high	only if dataflow changes within diagnostic test interval
Input comparison/voting (1oo2, 2oo3 or better redundancy)	A.6.5	high	only if dataflow changes within diagnostic test interval

NOTE 1 This table does not replace any of the requirements of annex C.

NOTE 2 The requirements of annex C are relevant for the determination of diagnostic coverage.

NOTE 3 For general notes concerning this table, see the text preceding table A.1.

Table A.8 — Data paths (internal communication)

Diagnostic technique/measure	See IEC 61508-7	Maximum diagnostic coverage considered achievable	Notes
One-bit hardware redundancy	A.7.1	low	
Multi-bit hardware redundancy	A.7.2	medium	
Complete hardware redundancy	A.7.3	high	
Inspection using test patterns	A.7.4	high	
Transmission redundancy	A.7.5	high	effective only against transient faults
Information redundancy	A.7.6	high	

NOTE 1 This table does not replace any of the requirements of annex C.

NOTE 2 The requirements of annex C are relevant for the determination of diagnostic coverage.

NOTE 3 For general notes concerning this table, see the text preceding table A.1.

Table A.9 — Power supply

Diagnostic technique/measure	See IEC 61508-7	Maximum diagnostic coverage considered achievable	Notes
Overvoltage protection with safety shut-off or switch-over to second power unit	A.8.1	low	recommended always to be used in addition to other techniques in this table
Voltage control (secondary) with safety shut-off or switch-over to second power unit	A.8.2	high	
Power-down with safety shut-off or switch-over to second power unit	A.8.3	high	recommended always to be used in addition to other techniques in this table
Idle current principle	A.1.5	low	useful only against power down

NOTE 1 This table does not replace any of the requirements of annex C.

NOTE 2 The requirements of annex C are relevant for the determination of diagnostic coverage.

NOTE 3 For general notes concerning this table, see the text preceding table A.1.

Table A.10 — Program sequence (watch-dog)

Diagnostic technique/measure	See IEC 61508-7	Maximum diagnostic coverage considered achievable	Notes
Watch-dog with separate time base without time-window	A.9.1	low	
Watch-dog with separate time base and time-window	A.9.2	medium	
Logical monitoring of program sequence	A.9.3	medium	depends on the quality of the monitoring
Combination of temporal and logical monitoring of programme sequences	A.9.4	high	
Temporal monitoring with on-line check	A.9.5	medium	
NOTE 1 This table does not replace any of the requirements of annex C. NOTE 2 The requirements of annex C are relevant for the determination of diagnostic coverage. NOTE 3 For general notes concerning this table, see the text preceding table A.1.			

Table A.11 — Ventilation and heating system (if necessary)

Diagnostic technique/measure	See IEC 61508-7	Maximum diagnostic coverage considered achievable	Notes
Temperature sensor	A.10.1	medium	
Fan control	A.10.2	medium	
Actuation of the safety shut-off via thermal fuse	A.10.3	high	
Staggered message of thermo-sensors and conditional alarm	A.10.4	high	
Connection of forced-air cooling and status indication	A.10.5	high	
NOTE 1 This table does not replace any of the requirements of annex C. NOTE 2 The requirements of annex C are relevant for the determination of diagnostic coverage. NOTE 3 For general notes concerning this table, see the text preceding table A.1.			

Table A.12 — Clock

Diagnostic technique/measure	See IEC 61508-7	Maximum diagnostic coverage considered achievable	Notes
Watch-dog with separate time base without time-window	A.9.1	low	
Watch-dog with separate time base and time-window	A.9.2	high	depends on time restriction for the time-window
Logical monitoring of program sequence	A.9.3	medium	only effective against clock failures if external temporal events influence the logical program flow
Temporal and logical monitoring	A.9.4	high	
Temporal monitoring with on-line check	A.9.5	medium	

NOTE 1 This table does not replace any of the requirements of annex C.

NOTE 2 The requirements of annex C are relevant for the determination of diagnostic coverage.

NOTE 3 For general notes concerning this table, see the text preceding table A.1.

Table A.13 — Communication and mass-storage

Diagnostic technique/measure	See IEC 61508-7	Maximum diagnostic coverage considered achievable	Notes
Information exchange between E/E/PE safety-related system and process	A.6	see table A.7	see I/O units and interface
Information exchange between E/E/PE safety-related systems	A.7	see table A.8	see data paths/bus
Separation of electrical energy lines from information lines	A.11.1	high	recommended to be always used in addition to other techniques in this table
Spatial separation of multiple lines	A.11.2	high	
Increase of interference immunity	A.11.3	high	
Antivalent signal transmission	A.11.4	high	

NOTE 1 This table does not replace any of the requirements of annex C.

NOTE 2 The requirements of annex C are relevant for the determination of diagnostic coverage.

NOTE 3 For general notes concerning this table, see the text preceding table A.1.

Table A.14 — Sensors

Diagnostic technique/measure	See IEC 61508-7	Maximum diagnostic coverage considered achievable	Notes
Failure detection by on-line monitoring	A.1.1	low (low demand mode) medium (high demand or continuous mode)	depends on diagnostic coverage of failure detection
Idle current principle	A.1.5	low	only for E/E/PE safety-related systems where continuous control is not needed to achieve or maintain a safe state of the EUC
Analogue signal monitoring	A.2.7	low	
Test pattern	A.6.1	high	
Input comparison/voting (1oo2, 2oo3 or better redundancy)	A.6.5	high	only if dataflow changes within diagnostic test interval
Reference sensor	A.12.1	high	depends on diagnostic coverage of failure detection
Positive-activated switch	A.12.2	high	

NOTE 1 This table does not replace any of the requirements of annex C.

NOTE 2 The requirements of annex C are relevant for the determination of diagnostic coverage.

NOTE 3 For general notes concerning this table, see the text preceding table A.1.

Table A.15 — Final elements (actuators)

Diagnostic technique/measure	See IEC 61508-7	Maximum diagnostic coverage considered achievable	Notes
Failure detection by on-line monitoring	A.1.1	low (low demand mode) medium (high demand or continuous mode)	depends on diagnostic coverage of failure detection
Monitoring of relay contacts	A.1.2	high	high diagnostic coverage is only achievable if the relay switching time interval is much smaller than the demand rate.
Idle current principle	A.1.5	low	only for E/E/PE safety-related systems where continuous control is not needed to achieve or maintain a safe state of the EUC
Test pattern	A.6.1	high	
Monitoring	A.13.1	high	depends on diagnostic coverage of failure detection
Cross-monitoring of multiple actuators	A.13.2	high	
NOTE 1 This table does not replace any of the requirements of annex C. NOTE 2 The requirements of annex C are relevant for the determination of diagnostic coverage. NOTE 3 For general notes concerning this table, see the text preceding table A.1.			

A.3 Systematic safety integrity

The following tables give recommendations for techniques and measures to:

— control failures caused by hardware and software design (see table A.16);

— control failures due to environmental stress or influences (see table A.17); and

— control failures during operation (see table A.18).

In tables A.16 to A.18, recommendations are made by safety integrity level, stating firstly the importance of the technique or measure and secondly the effectiveness required if it is used. The importance is signified as follows.

— HR: the technique or measure is highly recommended for this safety integrity level. If this technique or measure is not used then the rationale behind not using it shall be detailed;

— R: the technique or measure is recommended for this safety integrity level. At least one of the techniques in the light grey shaded group is required;

— -: the technique or measure has no recommendation for or against being used;

— NR: the technique or measure is positively not recommended for this safety integrity level. If this technique or measure is used then the rationale behind using it shall be detailed.

The required effectiveness is signified as follows.

— Mandatory: the technique or measure is required for all safety integrity levels and shall be used as effectively as possible (i.e. giving high effectiveness).

— Low: if used, the technique or measure shall be used to the extent necessary to give at least low effectiveness against systematic failures.

— Medium: if used, the technique or measure shall be used to the extent necessary to give at least medium effectiveness against systematic failures.

— High: if used, the technique or measure shall be used to the extent necessary to give high effectiveness against systematic failures.

Guidance on levels of effectiveness for most techniques and measures is given in table A.19.

If a measure is not mandatory, it is in principle replaceable by other measures (either individually or in combination); this is governed by the shading, as explained in the table.

All techniques and measures given here are built-in features of the E/E/PE safety-related systems, which may help to control failures on-line. Procedural and organisational techniques and measures are necessary throughout the E/E/PES safety lifecycle to avoid introducing faults, and validation techniques to test the E/E/PE safety-related systems' behaviour against expected external influences are necessary to demonstrate that the built-in features are appropriate for the specific application (see annex B).

Annex D of IEC 61508-6 gives information on common cause failures.

NOTE Most of the measures in tables A.16 to A.18 can be used with varying effectiveness according to table A.19, which gives examples for low and high effectiveness. The effort required for medium effectiveness lies somewhere between that specified for low and for high effectiveness.

Table A.16 — Techniques and measures to control systematic failures caused by hardware and software design

	Technique/measure	See IEC 61508-7	SIL1	SIL2	SIL3	SIL4
	Program sequence monitoring	A.9	HR low	HR low	HR medium	HR high
▨	Failure detection by on-line monitoring (see note 4)	A.1.1	R low	R low	R medium	R high
▨	Tests by redundant hardware	A.2.1	R low	R low	R medium	R high
▨	Standard test access port and boundary-scan architecture	A.2.3	R low	R low	R medium	R high
▨	Code protection	A.6.2	R low	R low	R medium	R high
▨	Diverse hardware	B.1.4	- low	- low	R medium	R high
▨	Fault detection and diagnosis	C.3.1	See table A.2 of IEC 61508-3			
▨	Error detecting and correcting codes	C.3.2				
▨	Failure assertion programming	C.3.3				
▨	Safety bag techniques	C.3.4				
▨	Diverse programming	C.3.5				
▨	Recovery block	C.3.6				
▨	Backward recovery	C.3.7				
▨	Forward recovery	C.3.8				
▨	Re-try fault recovery mechanisms	C.3.9				
▨	Memorising executed cases	C.3.10				
▨	Graceful degradation	C.3.11				
▨	Artificial intelligence fault correction	C.3.12				
▨	Dynamic reconfiguration	C.3.13				

At least one of the techniques in the light grey shaded group is required.

NOTE 1 For the meaning of the entries under each safety integrity level, see the text immediately preceding this table.

NOTE 2 The measures in this table which do not refer to table A.2 of IEC 61508-3 can be used to varying effectiveness according to table A.19, which gives examples for low and high effectiveness. The effort required for medium effectiveness lies somewhere between that specified for low and for high effectiveness.

NOTE 3 The overview of techniques and measures associated with this table is in annexes A, B and C of IEC 61508-7. The relevant subclause is referenced in the second column.

NOTE 4 For E/E/PE safety-related systems operating in a low demand mode of operation (for example emergency shutdown systems), the diagnostic coverage achieved from failure detection by on-line monitoring is generally low or none.

Table A.17 — Techniques and measures to control systematic failures caused by environmental stress or influences

	Technique/measure	See IEC 61508-7	SIL1	SIL2	SIL3	SIL4
	Measures against voltage breakdown, voltage variations, overvoltage, low voltage	A.8	HR mandatory	HR mandatory	HR mandatory	HR mandatory
	Separation of electrical energy lines from information lines (see note 4)	A.11.1	HR mandatory	HR mandatory	HR mandatory	HR mandatory
	Increase of interference immunity	A.11.3	HR mandatory	HR mandatory	HR mandatory	HR mandatory
	Measures against the physical environment (for example, temperature, humidity, water, vibration, dust, corrosive substances)	A.14	HR mandatory	HR mandatory	HR mandatory	HR mandatory
	Program sequence monitoring	A.9	HR low	HR low	HR medium	HR high
	Measures against temperature increase	A.10	HR low	HR low	HR medium	HR high
	Spatial separation of multiple lines	A.11.2	HR low	HR low	HR medium	HR high
▨	Failure detection by on-line monitoring (see note 5)	A.1.1	R low	R low	R medium	R high
▨	Tests by redundant hardware	A.2.1	R low	R low	R medium	R high
▨	Code protection	A.6.2	R low	R low	R medium	R high
▨	Antivalent signal transmission	A.11.4	R low	R low	R medium	R high
▨	Diverse hardware (see note 6)	B.1.4	- low	- low	- medium	R high
▨	Software architecture	7.4.3 of IEC 61508-3	See table A.2 of IEC 61508-3			

At least one of the techniques in the light grey shaded group is required.

NOTE 1 For the meaning of the entries under each safety integrity level, see the text immediately preceding table A.16.

NOTE 2 Most of these measures in this table can be used to varying effectiveness according to table A.19, which gives examples for low and high effectiveness. The effort required for medium effectiveness lies somewhere between that specified for low and for high effectiveness.

NOTE 3 The overview of techniques and measures associated with this table is in annexes A and B of IEC 61508-7. The relevant subclause is referenced in the second column.

NOTE 4 Separation of electrical energy lines from information lines is not necessary if the information is transported optically, nor is it necessary for low power energy lines which are designed for energising components of the E/E/PES and carrying information from or to these components.

NOTE 5 For E/E/PE safety-related systems operating in a low demand mode of operation (for example emergency shut-down systems), the diagnostic coverage achieved from failure detection by on-line monitoring is generally low or none.

NOTE 6 Diverse hardware is not required if it has been demonstrated, by validation and extensive operational experience, that the hardware is sufficiently free of design faults and sufficiently protected against common cause failures to fulfil the target failure measures.

Table A.18 — Techniques and measures to control systematic operational failures

	Technique/measure	See IEC 61508-7	SIL1	SIL2	SIL3	SIL4
	Modification protection	B.4.8	HR mandatory	HR mandatory	HR mandatory	HR mandatory
▨	Failure detection by on-line monitoring (see note 4)	A.1.1	R low	R low	R medium	R high
	Input acknowledgement	B.4.9	R low	R low	R medium	R high
	Failure assertion programming	C.3.3	See table A.2 of IEC 61508-3			

At least one of the techniques in the light grey shaded group is required.

NOTE 1 For the meaning of the entries under each safety integrity level, see the text immediately preceding table A.16.

NOTE 2 Two of these measures in this table can be used to varying effectiveness according to table A.19, which gives examples for low and high effectiveness. The effort required for medium effectiveness lies somewhere between that specified for low and for high effectiveness.

NOTE 3 The overview of techniques and measures associated with this table is in annexes A, B, and C of IEC 61508-7. The relevant subclause is referenced in the second column.

NOTE 4 For E/E/PE safety-related systems operating in a low demand mode of operation (for example emergency shut-down systems), the diagnostic coverage achieved from failure detection by on-line monitoring is generally low or none.

Table A.19 — Effectiveness of techniques and measures to control systematic failures

Technique/measure	See IEC 61508-7	Low effectiveness	High effectiveness
Failure detection by on-line monitoring (see note)	A.1.1	Trigger signals from the EUC and its control system are used to check the proper operation of the E/E/PE safety-related systems (only time behaviour with an upper time limit).	E/E/PE safety-related systems are retriggered by temporal and logical signals from the EUC and its control system (time window for temporal watch-dog function).
Tests by redundant hardware (see note)	A.2.1	Additional hardware tests the trigger signals of the E/E/PE safety-related systems (only time behaviour with an upper time limit), this hardware switches a secondary final element.	Additional hardware is retriggered by temporal and logical signals of the E/E/PE safety-related systems (time window for temporal watch-dog); voting between multiple channels.
Standard test access port and boundary-scan architecture	A.2.3	Testing the used solid-state logic, during the proof test, through defined boundary scan tests.	Diagnostic test of solid-state logic, according to the functional specification of the E/E/PE safety-related systems; all functions are checked for all integrated circuits.
Code protection	A.6.2	Failure detection via time redundancy of signal transmission.	Failure detection via time and information redundancy of signal transmission.
Program sequence monitoring	A.9	Temporal or logical monitoring of the program sequence.	Temporal and logical monitoring of the program sequence at very many checking points in the program.
Measures against temperature increase	A.10	Temperature sensor, detecting over-temperature.	Actuation of the safety shut-off via thermal fuse.
Increase of interference immunity (see note)	A.11.3	Noise filter at power supply and critical inputs and outputs; shielding, if necessary.	Filter against electromagnetic injection which is normally not expected; shielding.
Measures against physical environment	A.14	Generally accepted practice according to the application.	Techniques referred to in standards for a particular application.
Diverse hardware	B.1.4	Two or more items carrying out the same function but being different in design.	Two or more items carrying out different functions.
Input acknowledgement	B.4.9	Echoing of input actions back to the operator.	Checking strict rules for the input of data by the operator, rejecting incorrect inputs.
NOTE In the cases of the techniques with references A.1.1, A.2.1, A.11.3, and A.14 for high effectiveness of the technique or measure it is assumed that the low effectiveness approaches are also used.			

Annex B
(normative)

Techniques and measures for E/E/PE safety-related systems: avoidance of systematic failures during the different phases of the lifecycle

Tables B.1 to B.5 in this annex recommend, for each safety integrity level, techniques and measures to avoid failures in E/E/PE safety-related systems. More information about the techniques and measures can be found in annex B of IEC 61508-7. Requirements for measures to control failures during operation are given in annex A and described in annex A of IEC 61508-7.

It is not possible to list every individual cause of systematic failures, originating throughout the safety life cycle, or every remedy, for two main reasons:

— the effect of a systematic fault depends on the lifecycle phase in which it was introduced; and

— the effectiveness of any single measure to avoid systematic failures depends on the application.

A quantitative analysis for the avoidance of systematic failures is therefore impossible.

Failures in E/E/PE safety-related systems may be categorised, according to the lifecycle phase in which a causal fault is introduced, into:

— failures caused by faults originating **before or during system installation** (for example, software faults include specification and program faults, hardware faults include manufacturing faults and incorrect selection of components); and

— failures caused by faults originating **after system installation** (for example random hardware failures, or failures caused by incorrect use).

In order to avoid or control such failures when they occur, a large number of measures are normally necessary. The structure of the requirements in annexes A and B results from dividing the measures into those used to **avoid failures** during the different phases of the E/E/PES safety lifecycle (this annex), and those used to **control failures** during operation (annex A). The measures to control failures are built-in features of the E/E/PE safety-related systems, while the measures to avoid failures are performed during the safety lifecycle.

In tables B.1 to B.5, recommendations are made by safety integrity level, stating firstly the importance of the technique or measure and secondly the effectiveness required if it is used. The importance is signified as follows:

— HR: the technique or measure is highly recommended for this safety integrity level. If this technique or measure is not used then the rationale behind not using it shall be detailed;

— R: the technique or measure is recommended for this safety integrity level. At least one of the techniques in the light grey shaded group is required;

— -: the technique or measure has no recommendation for or against being used;

— NR: the technique or measure is positively not recommended for this safety integrity level. If this technique or measure is used then the rationale behind using it shall be detailed;

The required effectiveness is signified as follows.

— Mandatory: the technique or measure is required for all safety integrity levels and shall be used as effectively as possible (i.e. giving high effectiveness);

— Low: if used, the technique or measure shall be used to the extent necessary to give at least low effectiveness against systematic failures;

— Medium: if used, the technique or measure shall be used to the extent necessary to give at least medium effectiveness against systematic failures;

— High: the technique or measure shall be used to the extent necessary to give high effectiveness against systematic failures.

NOTE Most of the measures in tables B.1 to B.5 can be used with varying effectiveness according to table B.6, which gives examples for low and high effectiveness. The effort required for medium effectiveness lies somewhere between that specified for low and for high effectiveness.

If a measure is not mandatory, it is in principle replaceable by other measures (either individually or in combination); this is governed by the shading, as explained in each table.

Following the guidelines in this annex does not guarantee by itself the required safety integrity. It is important to consider

— the consistency of the chosen techniques and measures, and how well they will complement each other;

— which techniques and measures are appropriate, for every phase of the development lifecycle; and

— which techniques and measures are most appropriate for the specific problems encountered during the development of each different E/E/PE safety-related system.

Table B.1 — Recommendations to avoid mistakes during specification of E/E/PES requirements (see 7.2)

	Technique/measure	**See IEC 61508-7**	**SIL1**	**SIL2**	**SIL3**	**SIL4**
	Project management	B.1.1	HR low	HR low	HR medium	HR high
	Documentation	B.1.2	HR low	HR low	HR medium	HR high
	Separation of E/E/PE safety-related systems from non-safety-related systems	B.1.3	HR low	HR low	HR medium	HR high
	Structured specification	B.2.1	HR low	HR low	HR medium	HR high
▨	Inspection of the specification	B.2.6	- low	HR low	HR medium	HR high
▨	Semi-formal methods	B.2.3, see also table B.7 of IEC 61508-3	R low	R low	HR medium	HR high
▨	Checklists	B.2.5	R low	R low	R medium	R high
▨	Computer aided specification tools	B.2.4	- low	R low	R medium	R high
▨	Formal methods	B.2.2	- low	- low	R medium	R high

All techniques marked “R” in the grey shaded group are replaceable, but at least one of these is required.

For the verification of this safety lifecycle phase, at least one of the techniques or measures shaded grey in this table or listed in table B.5 shall be used.

NOTE 1 For the meaning of the entries under each safety integrity level, see the text preceding this table.

NOTE 2 The measures in this table can be used to varying effectiveness according to table B.6, which gives examples for low and high effectiveness. The effort required for medium effectiveness lies somewhere between that specified for low and for high effectiveness.

NOTE 3 The overview of techniques and measures associated with this table is in annex B of IEC 61508-7. Relevant subclauses are referenced in the second column.

Table B.2 — Recommendations to avoid introducing faults during E/E/PES design and development (see 7.4)

	Technique/measure	See IEC 61508-7	SIL1	SIL2	SIL3	SIL4
	Observance of guidelines and standards	B.3.1	HR mandatory	HR mandatory	HR mandatory	HR mandatory
	Project management	B.1.1	HR low	HR low	HR medium	HR high
	Documentation	B.1.2	HR low	HR low	HR medium	HR high
	Structured design	B.3.2	HR low	HR low	HR medium	HR high
	Modularisation	B.3.4	HR low	HR low	HR medium	HR high
▨	Use of well-tried components	B.3.3	R low	R low	R medium	R high
▨	Semi-formal methods	B.2.3, see also table B.7 of IEC 61508-3	R low	R low	HR medium	HR high
▨	Checklists	B.2.5	- low	R low	R medium	R high
▨	Computer-aided design tools	B.3.5	- low	R low	R medium	R high
▨	Simulation	B.3.6	- low	R low	R medium	R high
▨	Inspection of the hardware or walk-through of the hardware	B.3.7 B.3.8	- low	R low	R medium	R high
▨	Formal methods	B.2.2	- low	- low	R medium	R high

All techniques marked “R” in the grey shaded group are replaceable, but at least one of these is required.

For the verification of this safety lifecycle phase, at least one of the techniques or measures shaded grey in this table or listed in table B.5 shall be used.

NOTE 1 For the meaning of the entries under each safety integrity level, see the text preceding table B.1.

NOTE 2 Most of these measures in this table can be used to varying effectiveness according to table B.6, which gives examples for low and high effectiveness. The effort required for medium effectiveness lies somewhere between that specified for low and for high effectiveness.

NOTE 3 The overview of techniques and measures associated with this table is in annex B of IEC 61508-7. Relevant subclauses are referenced in the second column.

Table B.3 — Recommendations to avoid faults during E/E/PES integration (see 7.5)

	Technique/measure	See IEC 61508-7	SIL1	SIL2	SIL3	SIL4
	Functional testing	B.5.1	HR mandatory	HR mandatory	HR mandatory	HR mandatory
	Project management	B.1.1	HR low	HR low	HR medium	HR high
	Documentation	B.1.2	HR low	HR low	HR medium	HR high
▨	Black-box testing	B.5.2	R low	R low	R medium	R high
▨	Field experience	B.5.4	R low	R low	R medium	R high
▨	Statistical testing	B.5.3	- low	- low	R medium	R high

All techniques marked “R” in the grey shaded group are replaceable, but at least one of these is required.

For the verification of this safety lifecycle phase, at least one of the techniques or measures shaded grey in this table or listed in table B.5 shall be used.

NOTE 1 For the meaning of the entries under each safety integrity level, see the text preceding table B.1.

NOTE 2 Most of these measures in this table can be used to varying effectiveness according to table B.6, which gives examples for low and high effectiveness. The effort required for medium effectiveness lies somewhere between that specified for low and for high effectiveness.

NOTE 3 The overview of techniques and measures associated with this table is in annex B of IEC 61508-7. Relevant subclauses are referenced in the second column.

Table B.4 — Recommendations to avoid faults and failures during E/E/PES operation and maintenance procedures (see 7.6)

	Technique/measure	See IEC 61508-7	SIL1	SIL2	SIL3	SIL4
	Operation and maintenance instructions	B.4.1	HR mandatory	HR mandatory	HR mandatory	HR mandatory
	User friendliness	B.4.2	HR mandatory	HR mandatory	HR mandatory	HR mandatory
	Maintenance friendliness	B.4.3	HR mandatory	HR mandatory	HR mandatory	HR mandatory
	Project management	B.1.1	HR low	HR low	HR medium	HR high
	Documentation	B.1.2	HR low	HR low	HR medium	HR high
▨	Limited operation possibilities	B.4.4	- low	R low	HR medium	HR high
▨	Protection against operator mistakes	B.4.6	- low	R low	HR medium	HR high
▨	Operation only by skilled operators	B.4.5	- low	R low	R medium	HR high

All techniques marked “R” in the grey shaded group are replaceable, but at least one of these is required.

The verification of this safety lifecycle phase shall be done by checklists (see B.2.5 of IEC 61508-7) or inspection (see B.2.6 of IEC 61508-7).

NOTE 1 For the meaning of the entries under each safety integrity level, see the text preceding table B.1.

NOTE 2 Most of these measures in this table can be used to varying effectiveness according to table B.6, which gives examples for low and high effectiveness. The effort required for medium effectiveness lies somewhere between that specified for low and for high effectiveness.

NOTE 3 The overview of techniques and measures associated with this table is in annex B of IEC 61508-7. Relevant subclauses are referenced in the second column.

Table B.5 — Recommendations to avoid faults during E/E/PES safety validation (see 7.7)

	Technique/measure	See IEC 61508-7	SIL1	SIL2	SIL3	SIL4
	Functional testing	B.5.1	HR mandatory	HR mandatory	HR mandatory	HR mandatory
	Functional testing under environmental conditions	B.6.1	HR mandatory	HR mandatory	HR mandatory	HR mandatory
	Interference surge immunity testing	B.6.2	HR mandatory	HR mandatory	HR mandatory	HR mandatory
	Fault insertion testing (when required diagnostic coverage ≥ 90 %)	B.6.10	HR mandatory	HR mandatory	HR mandatory	HR mandatory
	Project management	B.1.1	HR low	HR low	HR medium	HR high
	Documentation	B.1.2	HR low	HR low	HR medium	HR high
▒	Static analysis, dynamic analysis and failure analysis	B.6.4 B.6.5 B.6.6	- low	R low	R medium	R high
▒	Simulation and failure analysis	B.3.6 B.6.6	- low	R low	R medium	R high
▒	“Worst-case” analysis, dynamic analysis and failure analysis	B.6.7 B.6.5 B.6.6	- low	- low	R medium	R high
▒	Static analysis and failure analysis (see note 4)	B.6.4 B.6.6	R low	R low	NR	NR
■	Expanded functional testing	B.6.8	- low	HR low	HR medium	HR high
■	Black-box testing	B.5.2	R low	R low	R medium	R high
■	Fault insertion testing (when required diagnostic coverage < 90 %)	B.6.10	R low	R low	R medium	R high
■	Statistical testing	B.5.3	- low	- low	R medium	R high
■	“Worst-case” testing	B.6.9	- low	- low	R medium	R high
■	Field experience	B.5.4	R low	R low	R medium	NR

This table is divided into three groups, as indicated by the sidebar shading. All techniques marked “R” in the grey and black shaded groups are replaceable by other techniques within that group, but at least one of the techniques of the grey shaded group (analytical techniques) and at least one of the techniques of the black shaded group (testing techniques) is required.

NOTE 1 For the meaning of the entries under each safety integrity level, see the text preceding table B.1.

NOTE 2 Most of these measures in this table can be used to varying effectiveness according to table B.6, which gives examples for low and high effectiveness. The effort required for medium effectiveness lies somewhere between that specified for low and for high effectiveness.

NOTE 3 The overview of techniques and measures associated with this table is in annex B of IEC 61508-7. Relevant subclauses are referenced in the second column.

NOTE 4 Static analysis and failure analysis is not recommended for SIL3 and SIL4, because these techniques are not sufficient unless used in combination with dynamic analysis.

Table B.6 — Effectiveness of techniques and measures to avoid systematic failures

Technique/measure	IEC 61508-7 ref	Low effectiveness	High effectiveness
Project management (see note)	B.1.1	Definition of actions and responsibilities; scheduling and resource allocation; training of relevant personnel; consistency checks after modifications.	Validation independent from design; project monitoring; standardised validation procedure; configuration management; failure statistics; computer aided engineering; computer-aided software engineering.
Documentation (see note)	B.1.2	Graphical and natural language descriptions, for example block-diagrams, flow-diagrams.	Guidelines for consistent content and layout across organization; contents checklists; computer-aided documentation management, formal change control.
Separation of E/E/PE safety-related systems from non safety-related systems	B.1.3	Well-defined interfaces between E/E/PE safety-related systems and non-safety-related systems.	Total separation of E/E/PE safety-related systems from non-safety-related systems, i.e. no write access of non-safety-related systems to E/E/PE safety-related systems and separate physical locations to avoid common cause influences.
Structured specification	B.2.1	Manual hierarchical separation into subrequirements; description of the interfaces.	Hierarchical separation described using computer-aided engineering tools; automatic consistency checks; refinement down to functional level.
Formal methods	B.2.2	Used by personnel experienced in formal methods.	Used by personnel experienced in formal methods in similar applications, with computer support tools.
Semi-formal methods	B.2.3	Describing some critical parts with semi-formal methods.	Describing total E/E/PE safety-related systems with different semi-formal methods to show different aspects; consistency check between the methods
Computer-aided specification tools	B.2.4	Tools without preference for one particular design method.	Model-oriented procedures with hierarchical subdivision; description of all objects and their relationships; common data base; automatic consistency checks.
Checklists	B.2.5	Prepared checklists for all safety life-cycle phases; concentration on the main safety issues.	Prepared detailed checklists for all safety life-cycle phases.
Inspection of the specification	B.2.6	Inspection of the safety requirements specification by an independent person.	Inspection and re-inspection by an independent organisation using a formal procedure with correction of all faults found.
Structured design	B.3.2	Hierarchical circuit design, produced manually.	Reuse of tested circuit parts; traceability between specification, design, circuit diagram and parts lists; computer-aided; based on defined methods (see also 7.4.4)
Use of well-tried components (see note)	B.3.3	Sufficient over-dimensioning; constructive characteristics	Proven in use (see 7.4.7.6).
Modularisation (see note)	B.3.4	Modules of limited size; each module functionally isolated.	Re-use of well-proven modules; easily comprehensible modules; each module has a maximum of one input, one output, and one failure exit.
Computer-aided design tools	B.3.5	Computer support for complex phases of the safety lifecycle.	Use of tools which are proven in use (see 7.4.7.6) or validated; general computer-aided development for all phases of the safety lifecycle.
Simulation	B.3.6	Modelling at a module level, including boundary data of peripheral units.	Modelling on a component level, including boundary data.
Inspection of the hardware	B.3.7	Inspection by a person independent of the design	Inspection and re-inspection by an independent organisation using a formal procedure with correction of all faults found.
Walk-through of the hardware	B.3.8	Walk-through includes a person independent of the design.	Walk-through includes an independent organisation and follows a formal procedure with correction of all faults found.
Limited operation possibilities (see note)	B.4.4	Key-operated switch or password to govern change of operating mode.	Defined, robust procedure for allowing operation.
Operation only by skilled operators	B.4.5	Basic training in the type of safety systems being operated, plus two years' relevant on-the-job experience.	Yearly training of all operators; each operator has at least five years' experience with safety-related devices at lower safety integrity levels.

Technique/measure	**IEC 61508-7 ref**	**Low effectiveness**	**High effectiveness**
Protection against operator mistakes (see note)	B.4.6	Input acknowledgement.	Confirmation and consistency checks on each input command.
Black-box testing (see note)	B.5.2	Equivalence classes and input partition testing, boundary value testing, using pre-written test cases.	Test case execution from cause consequence diagrams, combining critical cases at extreme operating boundaries.
NOTE In the cases of the techniques with references B.1.1, B.1.2, B.3.3, B.3.4, B.4.4, B.4.6 and B.5.2, for high effectiveness of the technique or measure, it is assumed that the low effectiveness approaches are also used.			

Table B.6 *(concluded)*

Technique/measure	**IEC 61508-7 ref**	**Low effectiveness**	**High effectiveness**
Statistical testing (see note)	B.5.3	Statistical distribution of all input data	Test reports by tools; very many test cases; distribution of the input data according to real-life application conditions and assumed failure models.
Field experience (see note)	B.5.4	10 000 h operation time; at least one year's experience with at least 10 devices in different applications; statistical accuracy 95 %; no safety critical failures.	10 million h operation time; at least two years' experience with at least 10 devices in different applications; statistical accuracy 99.9 %; detailed documentation of all changes (including minor) during past operation.
Surge immunity testing	B.6.2		Surge immunity shall be demonstrably higher than the boundary values for real operating conditions.
Calculation of failure rates	B.6.3	Based on typical conditions.	Based on extreme operating boundaries.
Static analysis	B.6.4	Based on block diagrams; highlighting weak points; specifying test cases.	Based on detailed diagrams; predicting expected behaviour during test cases; using testing tools.
Dynamic analysis	B.6.5	Based on block diagrams; highlighting weak points; specifying test cases.	Based on detailed diagrams; predicting expected behaviour during test cases; using testing tools.
Failure analysis	B.6.6	At module level, including boundary data of the peripheral units	At component level, including boundary data
Worst-case analysis	B.6.7	Performed on safety functions; derived using boundary value combinations for real operating conditions.	Performed on non-safety functions; derived using boundary value combinations for real operating conditions.
Expanded functional testing	B.6.8	Test that all safety functions are maintained in the case of static input states caused by faulty process or operating conditions.	Test that all safety functions are maintained in the case of static input states and/or unusual input changes, caused by faulty process or operating conditions (including those that may be very rare).
Worst-case testing	B.6.9	Test that safety functions are maintained for a combination of boundary values found in real operating conditions.	Test that non-safety functions are maintained for a combination of the boundary values found in real operating conditions.
Fault insertion testing	B.6.10	At subunit level including boundary data or the peripheral units.	At component level including boundary data.
NOTE In the cases of the techniques wth references B.5.3, and B.5.4, for high effectiveness of the technique or measure, it is assumed that the low effectiveness approaches are also used.			

Annex C
(normative)

Diagnostic coverage and safe failure fraction

C.1 Calculation of diagnostic coverage and safe failure fraction of a subsystem

The diagnostic coverage and safe failure fraction of a subsystem shall be calculated as follows:

a) Carry out a failure mode and effect analysis to determine the effect of each failure mode of each component or group of components in the subsystem on the behaviour of the E/E/PE safety-related systems in the absence of diagnostic tests Sufficient information shall be available (see notes 1 & 2) to enable the failure mode and effects analysis to be undertaken so as to enable an adequate level of confidence to be established commensurate with the safety integrity requirements.

NOTE 1 In order to undertake this analysis the following information is required:

a) a detailed block diagram of the E/E/PE safety-related system describing the subsystem together with the interconnections for that part of the E/E/PE safety-related system which will affect the safety function(s) under consideration;

b) the hardware schematics of the subsystem describing each component or group of components and the interconnections between components

c) the failure modes and rates of each component or group of components and associated percentages of the total failure probability corresponding to safe and dangerous failures.

NOTE 2 The required rigour of this analysis will depend on a number of factors (see IEC 61508-1, 4.1). In particular, the safety integrity level of the safety functions involved will need to be taken into account. For higher safety integrity levels it is expected that the failure modes and effects analysis is very specific according to particular component types and application environments. Also, a thorough and detailed analysis is very important for a subsystem which is to be used in a hardware architecture having zero hardware fault tolerance.

a) Categorize each failure mode according to whether it leads (in the absence of diagnostic tests) to:

— a safe failure (i.e. leading to the safety integrity of an E/E/PE safety-related system not being compromised, for example, a failure leading to a safe shut-down or having no impact on the safety integrity of the E/E/PE safety-related system); or

— a dangerous failure (i.e. leading to an E/E/PE safety-related system, or part thereof, failing to function, or leading to the safety integrity of the E/E/PE safety-related system being otherwise compromised).

a) From an estimate of the failure probability of each component or group of components, λ, (see notes 2 and 3) and the results of the failure mode and effect analysis, for each component or group of components, calculate the probability of safe failure, λ_S, and the probability of dangerous failure, λ_D.

NOTE 3 The failure probability of each component or group of components is the probability of a failure occurring within a relatively small period of time, t. This can be considered as being equal to λ, the failure rate per unit time, t, in cases where λt is much less than 1.

NOTE 4 The failure rate of each component or group of components can be estimated using data from a recognised industry source, taking the application environment into account. However, application specific data is preferred, particularly in cases where the subsystem consists of a small number of components and where any error in estimating the probability of safe and dangerous failures of a particular component could have a significant impact on the estimation of the safe failure fraction.

a) For each component or group of components, estimate the fraction of dangerous failures which will be detected by the diagnostic tests (see C.2) and therefore the probability of a dangerous failure which is detected by the diagnostic tests, λ_{DD}.

a) For the subsystem, calculate the total probability of dangerous failure, $\Sigma\lambda_D$, the total probability of dangerous failures that are detected by the diagnostic tests, $\Sigma\lambda_{DD}$, and the total probability of safe failures $\Sigma\lambda_S$,

a) Calculate the diagnostic coverage of the subsystem as $\Sigma\lambda_{DD} / \Sigma\lambda_D$.

a) Calculate safe failure fraction of the subsystem as $(\Sigma\lambda_S + \Sigma\lambda_{DD}) / (\Sigma\lambda_S + \Sigma\lambda_D)$.

NOTE 5 The diagnostic coverage (if any) of each subsystem in the E/E/PE safety-related system is taken into account in the calculation of the probability of random hardware failures (see 7.4.3.2.2). The safe failure fraction is taken into account when determining the architectural constraints on hardware safety integrity (see 7.4.3.1).

The analysis used to determine the diagnostic coverage and safe failure fraction shall include all of the components, including electrical, electronic, electromechanical, mechanical etc, which are necessary to allow the subsystem to process the safety function(s) as required by the E/E/PE safety-related system. All of the possible dangerous modes of failure that will lead to an unsafe state, prevent a safe response when such a response is demanded or otherwise compromise the safety integrity of the E/E/PE safety-related systems, shall be considered for each of the components.

Table A.1 provides the faults or failures that shall, as a minimum, be detected in order to achieve the relevant diagnostic coverage or that shall, as a minimum, be included in the determination of safe failure fraction

If field data is used to support the failure modes & effects analysis it shall be sufficient to support the safety integrity requirements. As a minimum, a statistical single sided lower confidence limit of at least 70% is required.

NOTE 6 An example of calculation of diagnostic coverage and safe failure fraction is included in annex C of IEC 61508-6.

NOTE 7 Alternative methods are available for calculating diagnostic coverage involving, for example, simulation of faults using a computer model containing details of both the circuitry of the E/E/PE safety-related systems and the electronic components used in its design (for example, down to the transistor level in an integrated circuit).

C.2 Determination of diagnostic coverage factors

In the calculation of diagnostic coverage for a subsystem (see C.1) it is necessary to estimate, for each component or group of components, the fraction of dangerous failures which are detected by the diagnostic tests. The diagnostic tests which can contribute to the diagnostic coverage include, but are not limited to:

— comparison checks, for example monitoring and comparison of redundant signals;

— additional built-in test routines, for example checksums on memory;

— test by external stimuli, for example sending a pulsed signal through control paths,

— continuous monitoring of an analogue signal, for example, to detect out of range values indicative of sensor failure;

In order to calculate diagnostic coverage it is necessary to determine those failure modes that are detected by the diagnostic tests. It is possible that open-circuit or short-circuit failures for simple components (resistors, capacitors, transistors) can be detected with a coverage of 100%. However, for more complex type B components (see 7.4.3.1.3), account should be taken of the limitations to diagnostic coverage for the various components shown in table A.1. This analysis shall be carried out for each component or group of components of each subsystem and for each subsystem of the E/E/PE safety-related systems.

NOTE 1 Tables A.2 to A.15 recommend techniques and measures for diagnostic tests and recommend maximum diagnostic coverage which can be claimed. These tests may operate continuously or periodically (depending on the diagnostic test interval). The tables do not replace any of the requirements of annex C.

NOTE 2 Diagnostic tests can provide significant benefits in the achievement of functional safety of an E/E/PE safety-related system. However, care must be exercised not to unnecessarily increase the complexity which, for example, may lead to increased difficulties in verification, validation, functional safety assessment, maintenance and modification activities. Increased complexity may also make it more difficult to maintain the long-term functional safety of the E/E/PE safety-related system.

NOTE 3 The calculations to obtain the diagnostic coverage, and the ways it is used, assume that the E/E/PE safety-related systems operate safely in the presence of an otherwise dangerous fault that is detected by the diagnostic tests. If this assumption is not correct then the E/E/PE safety-related system is to be treated as operating in the high demand / continuous mode of operation (see 7.4.6.3 & 7.4.3.2.5)

NOTE 4 The definition of diagnostic coverage is given in 3.8.6 of IEC 61508-4. It is important to note that alternative definitions of the diagnostic coverage are sometimes assumed but these are not applicable.

NOTE 5 The diagnostic tests used to detect a dangerous failure within a subsystem may be implemented by another subsystem within the E/E/PE safety-related system.

NOTE 6 Diagnostic tests may operate either continuously or periodically, depending on the diagnostic test interval. There may be some cases or times where a diagnostic test should not be run due to the possibility of a test affecting the system state in an adverse manner. In this case no benefits in the calculations may be claimed from the diagnostic tests.

Annex D
(informative)

Bibliography

IEC 61000-4 :(all sections) Electromagnetic compatibility – Part 4 : Testing and measurement techniques

IEC 300-3-2 Reliability of systems, equipments & components - Part 11: Collection of reliability, availability, maintainability and maintenance support data from the field.

IEC 870-5-1 Telecontrol equipment & systems - Part 5: Transmission protocols - Section 1: Transmission frame formats

IEC 61164 :1995, Reliability growth – Statistical test and estimation methods

IEEE 352 : 1987, IEEE guide for general principles of reliability analysis of nuclear power generating station safety systems

EN 50159-1 “Railway applications - Safety-related communication in closed transmission systems”

prEN 50159-2 “Railway applications - Safety-related communication in open transmission systems”