

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

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

The European Standard EN 61508-2:2001 has the status of a British Standard

ICS 25.040.40; 29.020

National foreword

This British Standard is the official English language version of EN 61508-2:2001. It is identical with IEC 61508-2:2000.

The UK participation in its preparation was entrusted to Technical Committee GEL/65, Measurement and control, to Subcommittee GEL/65/1, System considerations, which has the responsibility to:

- aid enquirers to understand the text;
- present to the responsible international/European committee any enquiries on the interpretation, or proposals for change, and keep the UK interests informed;
- monitor related international and European developments and promulgate them in the UK.

A list of organizations represented on this committee can be obtained on request to its secretary.

Cross-references

The British Standards which implement international or European publications referred to in this document may be found in the BSI Standards Catalogue under the section entitled “International Standards Correspondence Index”, or by using the “Find” facility of the BSI Standards Electronic Catalogue.

A British Standard does not purport to include all the necessary provisions of a contract. Users of British Standards are responsible for their correct application.

Compliance with a British Standard does not of itself confer immunity from legal obligations.

Summary of pages

This document comprises a front cover, an inside front cover, the EN title page, pages 2 to 74, an inside back cover and a back cover.

The BSI copyright date displayed in this document indicates when the document was last issued.

Amendments issued since publication

Amd. No.	Date	Comments
13780	15 March 2002	Implementation of the European Standard

This British Standard, having been prepared under the direction of the Electrotechnical Sector Committee, was published under the authority of the Standards Committee and comes into effect on 15 July 2000

© BSI 15 March 2002

ISBN 0 580 36136 5

**Functional safety of electrical/electronic/programmable electronic
safety-related systems**
**Part 2: Requirements for electrical/electronic/programmable electronic
safety-related systems**
(IEC 61508-2:2000)

Sécurité fonctionnelle des systèmes
électriques/électroniques/électroniques
programmables relatifs à la sécurité
Partie 2: Prescriptions pour les systèmes
électriques/électroniques/électroniques
programmables relatifs à la sécurité
(CEI 61508-2:2000)

Funktionale Sicherheit
sicherheitsbezogener elektrischer/
elektronischer/programmierbarer
elektronischer Systeme
Teil 2: Anforderungen an
sicherheitsbezogene elektrische/
elektronische/programmierbare
elektronische Systeme
(IEC 61508-2:2000)

This European Standard was approved by CENELEC on 2001-07-03. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the Central Secretariat or to any CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CENELEC member into its own language and notified to the Central Secretariat has the same status as the official versions.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Czech Republic, Denmark, Finland, France, Germany, Greece, Iceland, Ireland, Italy, Luxembourg, Malta, Netherlands, Norway, Portugal, Spain, Sweden, Switzerland and United Kingdom.

CENELEC

European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung

Central Secretariat: rue de Stassart 35, B - 1050 Brussels

Foreword

The text of the International Standard IEC 61508-2:2000, prepared by SC 65A, System aspects, of IEC TC 65, Industrial-process measurement and control, was submitted to the Unique Acceptance Procedure and was approved by CENELEC as EN 61508-2 on 2001-07-03 without any modification.

The following dates were fixed:

- latest date by which the EN has to be implemented at national level by publication of an identical national standard or by endorsement (dop) 2002-08-01
- latest date by which the national standards conflicting with the EN have to be withdrawn (dow) 2004-08-01

Annexes designated "normative" are part of the body of the standard.
In this standard, annexes A, B, C and ZA are normative.
Annex ZA has been added by CENELEC.

IEC 61508 is a basic safety publication covering the functional safety of electrical, electronic and programmable electronic safety-related systems. The scope states:

"This International Standard covers those aspects to be considered when electrical/electronic/programmable electronic systems (E/E/PESs) are used to carry out safety functions. A major objective of this standard is to facilitate the development of application sector international standards by the technical committees responsible for the application sector. This will allow all the relevant factors associated with the application, to be fully taken into account and thereby meet the specific needs of the application sector. A dual objective of this standard is to enable the development of electrical/electronic/programmable electronic (E/E/PE) safety-related systems where application sector international standards may not exist".

The CENELEC Report R0BT-004, ratified by 103 BT (March 2000) accepts that some IEC standards, which today are either published or under development, are sector implementations of IEC 61508. For example:

- IEC 61511, Functional safety - Safety instrumented systems for the process industry sector;
- IEC 62061, Safety of machinery – Functional safety of electrical, electronic and programmable electronic control systems;
- IEC 61513, Nuclear power plants – Instrumentation and control for systems important to safety – General requirements for systems.

The railways sector has also developed a set of European Standards (EN 50126; EN 50128 and prEN 50129).

NOTE EN 50126 and EN 50128 were based on earlier drafts of IEC 61508. prEN 50129 is based on the principles of the latest version of IEC 61508.

This list does not preclude other sector implementations of IEC 61508 which could be currently under development or published within IEC or CENELEC.

Endorsement notice

The text of the International Standard IEC 61508-2:2000 was approved by CENELEC as a European Standard without any modification.

In the official version, for Bibliography, the following note has to be added for the standard indicated:

IEC 61000-4	NOTE	Harmonized in the EN 61000-4 series (not modified).
IEC 60870-5-1	NOTE	Harmonized as EN 60870-5-1:1993 (not modified).

CONTENTS

	Page
INTRODUCTION	6
Clause	
1 Scope	8
2 Normative references.....	11
3 Definitions and abbreviations	12
4 Conformance to this standard	12
5 Documentation.....	12
6 Management of functional safety.....	12
7 E/E/PES safety lifecycle requirements	12
7.1 General.....	12
7.2 E/E/PES safety requirements specification.....	16
7.3 E/E/PES safety validation planning	18
7.4 E/E/PES design and development.....	19
7.5 E/E/PES integration	36
7.6 E/E/PES operation and maintenance procedures	37
7.7 E/E/PES safety validation	39
7.8 E/E/PES modification.....	40
7.9 E/E/PES verification.....	40
8 Functional safety assessment	42
Annex A (normative) Techniques and measures for E/E/PE safety-related systems: control of failures during operation	43
A.1 General.....	43
A.2 Hardware safety integrity.....	44
A.3 Systematic safety integrity.....	53
Annex B (normative) Techniques and measures for E/E/PE safety-related systems: avoidance of systematic failures during the different phases of the lifecycle	59
Annex C (normative) Diagnostic coverage and safe failure fraction	69
C.1 Calculation of diagnostic coverage and safe failure fraction of a subsystem	69
C.2 Determination of diagnostic coverage factors	70
Annex ZA (normative) Normative references to international publications with their corresponding European publications	73
Bibliography	72

	Page
Figure 1 – Overall framework of IEC 61508	10
Figure 2 – E/E/PES safety lifecycle (in realisation phase)	13
Figure 3 – Relationship and scope for IEC 61508-2 and IEC 61508-3	14
Figure 4 – Relationship between the hardware and software architectures of programmable electronics	20
Figure 5 – Example limitation on hardware safety integrity for a single-channel safety function	25
Figure 6 – Example limitation on hardware safety integrity for a multiple-channel safety function	27
Table 1 – Overview – Realisation phase of the E/E/PES safety lifecycle	15
Table 2 – Hardware safety integrity: architectural constraints on type A safety-related subsystems	24
Table 3 – Hardware safety integrity: architectural constraints on type B safety-related subsystems	24
Table A.1 – Faults or failures to be detected during operation or to be analysed in the derivation of safe failure fraction	45
Table A.2 – Electrical subsystems	46
Table A.3 – Electronic subsystems	47
Table A.4 – Processing units	47
Table A.5 – Invariable memory ranges	48
Table A.6 – Variable memory ranges	48
Table A.7 – I/O units and interface (external communication)	49
Table A.8 – Data paths (internal communication)	49
Table A.9 – Power supply	50
Table A.10 – Program sequence (watch-dog)	50
Table A.11 – Ventilation and heating system (if necessary)	51
Table A.12 – Clock	51
Table A.13 – Communication and mass-storage	52
Table A.14 – Sensors	52
Table A.15 – Final elements (actuators)	53
Table A.16 – Techniques and measures to control systematic failures caused by hardware and software design	55
Table A.17 – Techniques and measures to control systematic failures caused by environmental stress or influences	56
Table A.18 – Techniques and measures to control systematic operational failure	57
Table A.19 – Effectiveness of techniques and measures to control systematic failures	58
Table B.1 – Recommendations to avoid mistakes during specification of E/E/PES requirements (see 7.2)	61
Table B.2 – Recommendations to avoid introducing faults during E/E/PES design and development (see 7.4)	62
Table B.3 – Recommendations to avoid faults during E/E/PES integration (see 7.5)	63
Table B.4 – Recommendations to avoid faults and failures during E/E/PES operation and maintenance procedures (see 7.6)	64
Table B.5 – Recommendations to avoid faults during E/E/PES safety validation (see 7.7)	65
Table B.6 – Effectiveness of techniques and measures to avoid systematic failures	66

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 ISO/IEC Guide 51. IEC 61508 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) 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.

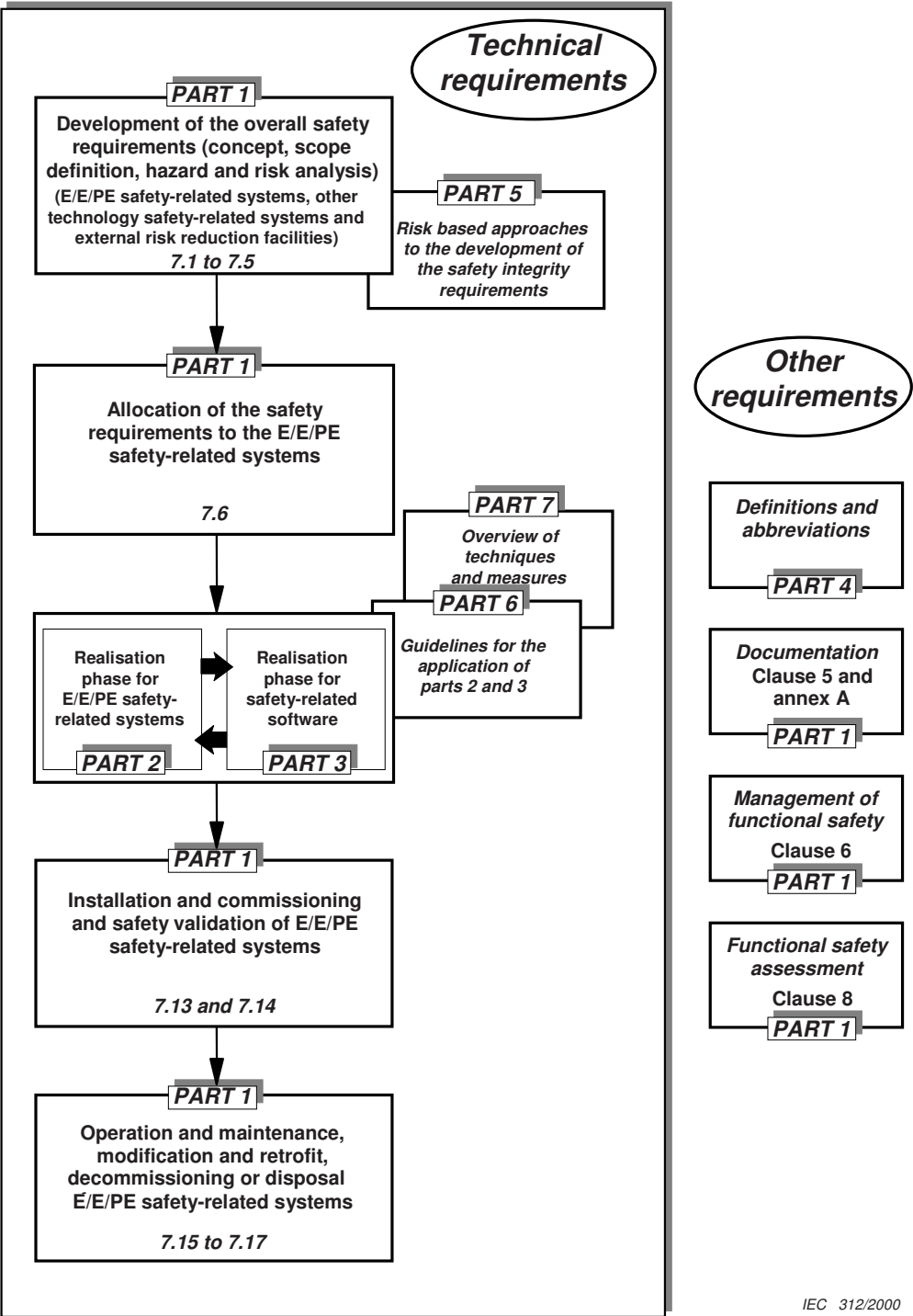


Figure 1 – Overall framework of IEC 61508

2 Normative references

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

IEC 60050(371):1984, *International Electrotechnical Vocabulary – Chapter 371: Telecontrol*

IEC 60300-3-2:1993, *Dependability management – Part 3: Application guide – Section 2: Collection of dependability data from the field*

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 – Basic EMC publication*

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

IEC 61508-3:1998, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 3: Software requirements*

IEC 61508-4:1998, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 4: Definitions and abbreviations*

IEC 61508-5:1998, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 5: Examples of methods for the determination of safety integrity levels*

IEC 61508-6, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 6: Guidelines on the application of parts 2 and 3¹⁾*

IEC 61508-7:2000, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 7: Overview of techniques and measures*

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

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

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

¹⁾ To be published.

3 Definitions and abbreviations

For the purposes of this part of IEC 61508, 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.

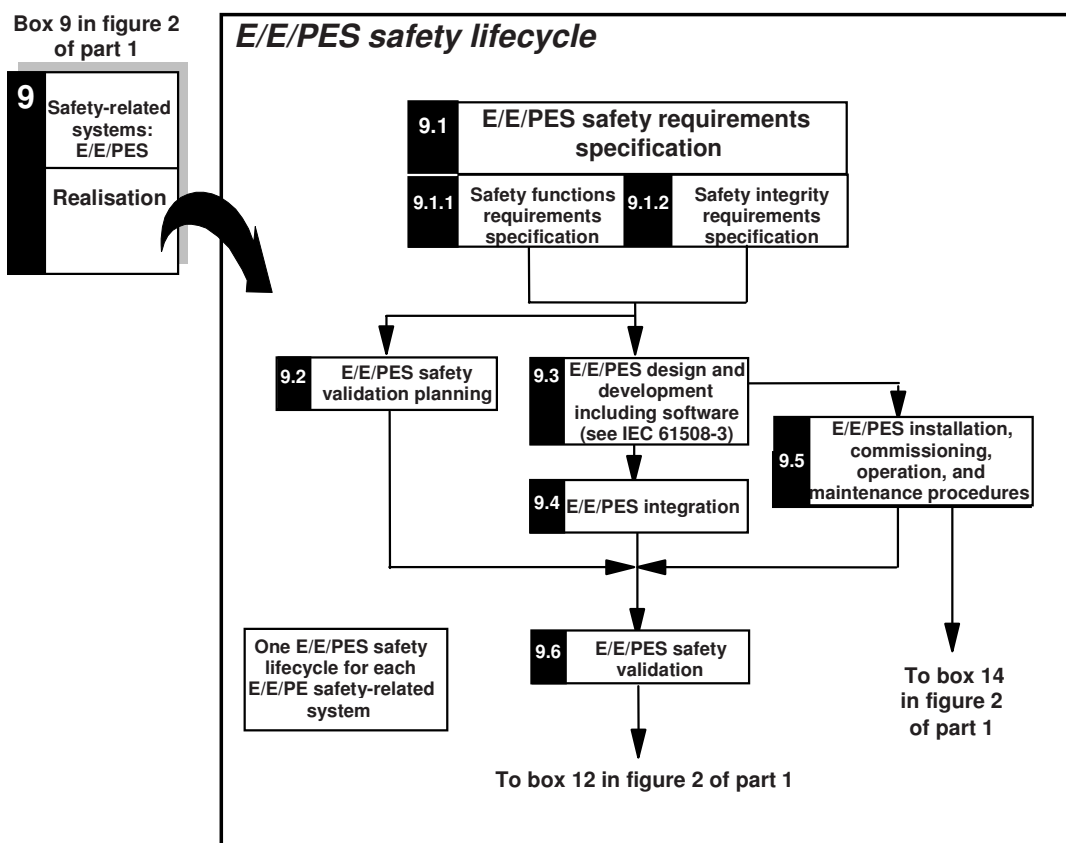
NOTE The relationship and scope for IEC 61508-2 and IEC 61508-3 are shown in figure 3.

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).



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

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

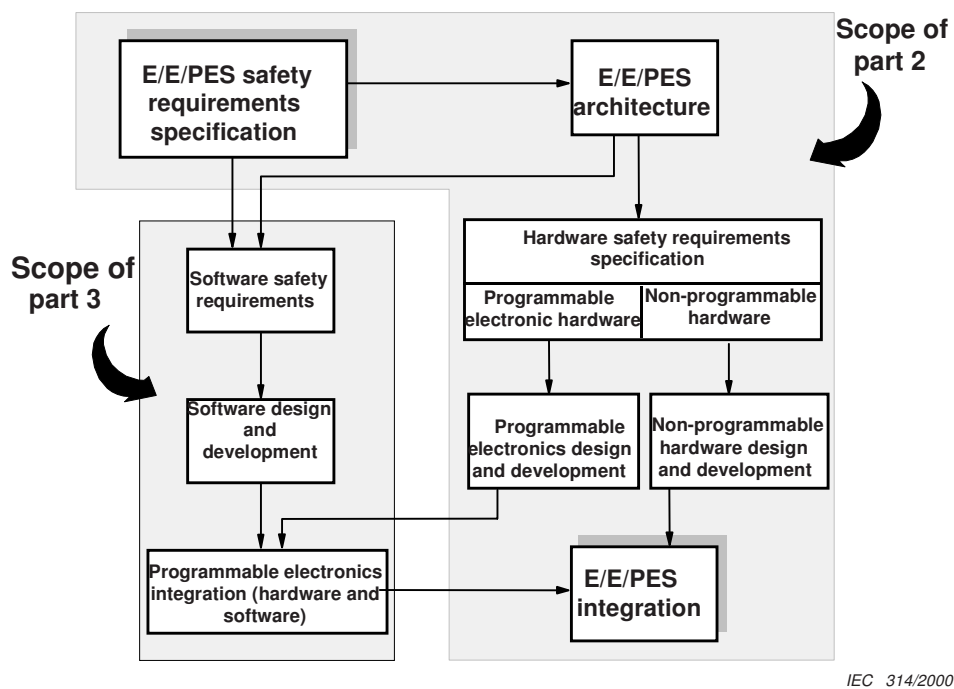


Figure 3 – Relationship and scope for IEC 61508-2 and IEC 61508-3

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

Safety lifecycle phase or activity		Objectives	Scope	Requirements 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, commission in, 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 and consistency with respect to the products and standards provided as input to that phase	E/E/PE safety-related systems	7.9.2	As above – depends on the phase Plan for the verification of the E/E/PE safety-related systems for each phase	As above – depends on the 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 and 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 and 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 IEC 61508-5);
- 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.

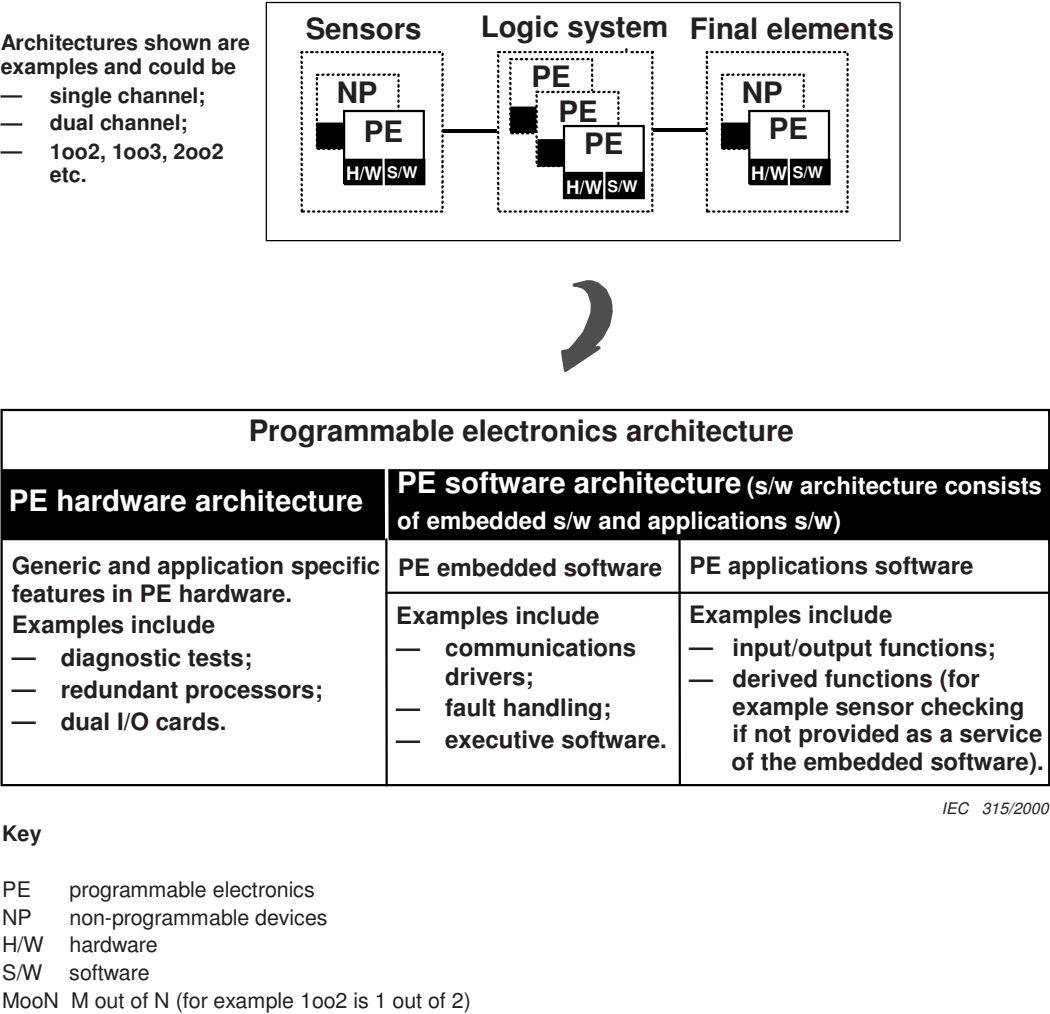


Figure 4 – Relationship between the hardware and software architectures of programmable electronics

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/PE 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/PE 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/PE 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 (see annex C). 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 (see annex C). 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. Subclauses 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 failures plus dangerous 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).